

Antonio Maña
Carsten Rudolph

Developing Ambient Intelligence




- Research Track
- EuroTRUSTAmI Workshops
- Cyber-Security Europe/USA panel debate

Proceedings of the second International
Conference on Ambient Intelligence
Developments (AmI.d'07)



Sponsors



 Springer

Developing Ambient Intelligence

Proceedings of the International
Conference on Ambient Intelligence
Developments (AmI.d'07)

Springer

Paris

Berlin

Heidelberg

New York

Hong Kong

Londres

Milan

Tokyo

Antonio Maña
Carsten Rudolph

Developing Ambient Intelligence

Proceedings of the International
Conference on Ambient Intelligence
Developments (AmI.d'07)

 Springer

Dr. Antonio Maña
Computer Science Department
University of Málaga
E.T.S.I. Informatica (3.2.16)
Campus de Teatinos
29071 Málaga
Spain

Dr. Carsten Rudolph
Fraunhofer Institute for Secure
Information Technology - SIT
Rheinstrasse 75
64295 Darmstadt
Germany

ISBN-13 : 978-2-287-78543-6 Paris Berlin Heidelberg New York

© Springer-Verlag France, Paris 2008

Imprimé en France

Springer-Verlag France est membre du groupe Springer Science + Business Media

Cet ouvrage est soumis au copyright. Tous droits réservés, notamment la reproduction et la représentation, la traduction, la réimpression, l'exposé, la reproduction des illustrations et des tableaux, la transmission par voie d'enregistrement sonore ou visuel, la reproduction par microfilm ou tout autre moyen ainsi que la conservation des banques données. La loi française sur le copyright du 9 septembre 1965 dans la version en vigueur n'autorise une reproduction intégrale ou partielle que dans certains cas, et en principe moyennant les paiements des droits. Toute représentation, reproduction, contrefaçon ou conservation dans une banque de données par quelque procédé que ce soit est sanctionnée par la loi pénale sur le copyright.

L'utilisation dans cet ouvrage de désignations, dénominations commerciales, marques de fabrique, etc., même sans spécification ne signifie pas que ces termes soient libres de la législation sur les marques de fabrique et la protection des marques et qu'ils puissent être utilisés par chacun.

La maison d'édition décline toute responsabilité quant à l'exactitude des indications de dosage et des modes d'emploi. Dans chaque cas il incombe à l'utilisateur de vérifier les informations données par comparaison à la littérature existante.

Maquette de couverture : Jean-François MONTMARCHÉ



Organization

AmId is an international conference organized and implemented by Strategies Telecoms & Multimedia.

General Chair

Javier Lopez University of Malaga, Spain

Steering Committee Chair

Volkmar Lotz SAP Research, France

Program Co-Chairs

Carsten Rudolph Fraunhofer SIT, Germany
Antonio Maña University of Malaga, Spain

Organization Chair

Richard Bricaire Strategies Telecoms and Multimedia, France

Program Committee

Emile Aarts	Eindhoven Univ. of Technology, Netherlands
Julio Abascal	Universidad del País Vasco, Spain
Stefano Campadello	Nokia, Finland
Jorge Cuellar	Siemens, Germany
Sabine Delaitre	JRC Seville, European Commission, Spain
Claudia Eckert	Darmstadt Univ. of Technology, Germany
Eduardo B. Fernandez	Florida Atlantic University
Paolo Giorgini	University of Trento, Italy
Sigrid Guergens	Fraunhofer SIT, Germany
Jan Juerjens	University of Bremen, Germany
Spyros Kokolakis	University of the Aegean, Greece
Jianhua Ma	Hosei University, Japan
Matteo Melideo	Engineering Ingegneria Informatica, Italy
Haris Mouratidis	University of East London, UK
Antonio Muñoz-Gallego	University of Malaga, Spain
David Naccache	Univ. La Sorbonne, France
Pierre Paradinas	CNAM, France
Ted Selker	MIT Media lab, USA
Pedro Soria-Rodríguez	Atos Origin, Spain
George Spanoudakis	City University London, UK
Willy Susilo	University of Wollongong, Australia
Mohammad Zulkernine	Queen's University, Ontario, Canada

Organization Committee

Daniel Serrano

University of Málaga, Spain

Eva Gherdani

STM, France

Lenick Perron

STM, France

Julien Heraud

STM, France

Preface

These proceedings contain the papers selected for presentation at the Second International Conference on Ambient Intelligence Developments (AmI.d) and a report on the panel discussion *Cyber-Security Europe/USA*, held in Sophia-Antipolis, France, during September 17-19, 2007.

At the time of the introduction of the Ambient Intelligence (AmI) concept many scenarios were considered to be visionary or even science fiction. Enabled by current technology, many aspects of these scenarios are slowly but inexorably becoming true. However, we are still facing important challenges that need further investments in research and industrialization. Current software engineering techniques and tools are not prepared to deal with the development of applications for what we could call AmI ecosystems, lacking a fixed architecture, controlled limits and even owners. The comfortable boundaries of static architectures and well-defined limits and owners are not existent in these AmI ecosystems.

In its second year AmI.d again shows the heterogeneity of research challenges related to Ambient Intelligence. Many different disciplines are involved and have to co-ordinate their efforts in resolving the strongly related research issues. We were very pleased that Norbert Streitz accepted to complete the research track by talking about his vision on AmI environments and *disappearing computers*. AmI.d was accompanied by the EuroTRUSTAmI workshops providing a forum for discussion and exchange between more than 28 European projects and platforms. Finally, a panel discussion complemented the program by showing a widened perspective by discussing future issues of cyber-security in the context of international AmI eco-systems.

The research papers included in the AmI.d proceeding are devoted to both theoretical and applied research, cover the most leading-edge research and contain contributions that have been formally reviewed and chosen by a selected International Program Committee. The contributions cover a wide range of AmI topics:

- Design and Development of AmI systems, Software engineering
- Context information
- Security of AmI
- Agents and AmI
- Applications
- AmI usages and adoption

Finally, we would like to acknowledge the fact that many colleagues offered energy and time for the realisation of this second issue AmI.d. In particular, we would like to thank all members of the program committee and also the people of STM for the local organization of the conference. Most importantly, we thank all authors who submitted and presented their work and all attendees for interesting discussions.

October 2007

Antonio Maña
Carsten Rudolph
Program Co-Chairs
AmI.d'07

Table of Contents

Research Track Proceedings	1
Abstracting connection volatility through tagged futures	2
<i>Johan Fabry and Carlos Noguera</i>	
Towards Semantic Resolution of Security in Ambient Environments	13
<i>Mario Hoffmann, Atta Badii, Stephan Engberg, Renjith Nair, Daniel Thiemert, Manuel Matthes, and Julian Schütte</i>	
Modeling Decentralized Information Flow in Ambient Environments	23
<i>Jurriaan van Diggelen, Robbert-Jan Beun, Rogier M. van Eijk, and Peter J. Werkhoven</i>	
Secure Profiles as a Cornerstone in Emerging Ambient Intelligence Scenarios	34
<i>Antonio Muñoz, Daniel Serrano, and Antonio Maña</i>	
Designing for People in Ambient Intelligence Environments	47
<i>Norbert Streitz</i>	
Architecture and Design Patterns for Ambient Intelligence: an Industry Perspective	55
<i>Antonio Kung</i>	
An Ambient Intelligence Based Multi-Agent Architecture	68
<i>Dante I. Tapia, Javier Bajo, and Juan M. Sánchez and Juan M. Corchado</i>	
Management of Large Video Recordings	79
<i>J.L. Patino, E. Corvee, F. Bremond, and M. Thonnat</i>	
XMPP based Health Care Integrated Ambient Systems Middleware	92
<i>Wael Labidi, Jean-Ferdy Susini, Pierre Paradinas, and Michael Setton</i>	
Increasing Interactivity in Agent-based Advanced Pocket-Device Service Application	103
<i>Sameh Abdel-Naby, Paolo Giorgini, and Stefano Fante</i>	
Towards a Model Driven Development of Context-aware Systems for AMI Environments	114
<i>Estefanía Serral, Pedro Valderas, Javier Muñoz, and Vicente Pelechano</i>	

Taking Ownership of Computational Resources	125
<i>Alain Rhelimi</i>	
Bluetooth Indoor Positioning and Ambient Information System	133
<i>Karim Khalil, Hiroshi Mizuno, Ken Sasaki, Hiroshi Hosaka, and Pierre Maret</i>	
XACML as a Security and Dependability Pattern for Access Control in AmI environments	143
<i>Antonio Muñoz, Francisco Sánchez-Cid, Paul El Khoury, and Luca Compagna</i>	
Rationale for defining NCIPs (Neighborhood and Context Interaction Primitives) position paper-	156
<i>Jérémie Albert and Serge Chaumettea</i>	
Agent Oriented AmI Engineering	166
<i>Raïan Ali, Sameh Abdel-Naby, Antonio Maña, Antonio Muñoz, and Paolo Giorgini</i>	
EuroTRUSTAmI workshop : European R&D towards trusted Ambient Intelligence	180
Introduction	181
NESSI	183
Project Serenity	184
Project SMEPP	186
Project Discreet	188
Project EmBounded	192
Project HAGGLE	194
Project GridTrust	196
Project ReSIST	199
Project MINAmI	202
Project MonAMI	205
Project ONE	207
Project RE-Trust	210

Project SENSE	213
Project SENSORIA	216
Project UBISEC&SENS	218
Project WASP	220
Project ESFORS	222
Project PalCom	224
Project R4eGov	226
EPoSS	228
Project Hydra	230
Project BioSecure	232
Project GREDIA	235
Project GridEcon.....	238
Cyber-Security EU/US. Meet the pathfinders of our future	240
<i>Jacques Bus (organizer and moderator), Andy Purdy, Jody Westby,</i>	
<i>Willem Jonker, Michel Riguidel, David Wright, and Charles</i>	
<i>Brookson</i>	
Author Index	252

Research Track Proceedings

Abstracting connection volatility through tagged futures

Johan Fabry and Carlos Noguera

INRIA Futurs - LIFL, ADAM Team
40, avenue Halley,
59655 Villeneuve d'Ascq, France
{johan.fabry|noguera}@lifl.fr

Abstract. The property of connection volatility, fundamental to the ambient intelligence (AmI) domain, makes it hard to develop AmI applications. The underlying reason for this is that the code for this concern is scattered and tangled with the core functionality of the application. In this paper we introduce the abstraction mechanism for connection volatility that we have created, which allows for this concern to be implemented in a non-tangled fashion. The core of our mechanism consists in extending the existing concept of futures with meta-data, i.e. *tags*, to specify values to be used in an offline state. The implementation of our abstraction mechanism, in Java, is called Spoon Graffiti. The meta-data of the futures is described using annotations and the intended behavior is achieved through source-code processing, using the Spoon annotation processor. As a result of using tagged futures and Spoon Graffiti, the specification of offline behavior of an AmI application can be performed in a non-tangled way, which significantly eases development.

1 Introduction

Developing Ambient Intelligence (AmI) software is a non-trivial task. This is because, not only do we need to deal with many of the known issues of distributed systems, e.g., inherent concurrency and network latency, but also we face the fundamental problem of connection volatility. As ambient devices frequently come in and out of range of each other, connections will be constantly established and broken. Connection volatility is therefore a fundamental problem of AmI: whereas in non-AmI programs connections are assumed to be permanent, in AmI the inverse is the norm.

Developing applications that behave correctly in the presence of connection volatility is a difficult task. An important reason for this is that the code for this concern is scattered throughout the application, and tangled with the core functionality of the application. Furthermore, no abstraction mechanisms have yet been developed that provide an adequate amount of support for connection volatility. In this paper we introduce the concept of tagged futures as a valid abstraction mechanism for connection volatility in AmI applications. Tagged futures allow the specification of the offline behavior of the application in a

straightforward and non-tangled manner. Furthermore, our proposal includes support to semi-automatically transition from an online to an offline state, and vice-versa. Again this support is provided at a higher level of abstraction and is not tangled with the core application code.

A number of abstraction mechanisms have previously been developed for connection volatility [9, 4, 3, 8, 7, 1, 10], however, none of these provide adequate support for specifying offline behavior of the application. One such abstraction is the use of futures [6], as proposed in an ambient context by Dedecker et.al. [2]. We can use futures as empty place-holders for return values of network operations. Futures have the important advantage that they do not introduce any tangling of the connection volatility concern in the application. Their downside is however that in a disconnected setting they only allow an application to continue working in a very limited fashion. It is our opinion that the restrictions that are imposed are too strong, as we shall show in Sect. 2.2. We therefore propose to enrich futures, to allow them to be more amply useful. Tagged futures allow metadata, i.e., tags, to be attached to them. This metadata can then specify a mock value to be used during disconnected operations. As we shall show in this paper, the use of such metadata makes futures applicable in a more realistic setting.

2 Future Problems

Futures, also sometimes referred to as promises, essentially are placeholder values for an as yet undetermined object. When the actual value for that object has been determined, the future is automatically *resolved*. Resolving causes the future to transparently become the new object. Futures can be passed around as if they were the resolved value, without this affecting the behavior of the application. It is only when the future itself is accessed, e.g., through a method call or a field access that the behavior of the application differs. Accesses to a future *block* until the future is resolved. When the future is resolved, any blocked accesses are forwarded to resolved value for the future. An important advantage of futures is that, in the code, they are indistinguishable from the objects for which they are place-holders. As a result, this abstraction for connection volatility does not introduce any tangled code.

We can use futures as return values of network operations, allowing the application to continue to function in a disconnected fashion. As long as the future itself is not accessed, the application will function as normal. However, when a future is accessed, the application will block. The application will only continue after the future has resolved, in other words, only after the network link is established, the remote call has been executed and its return value is known.

2.1 The Shopping Application

We will employ a running example to illustrate an important limitation of futures, and show how our proposal can address this limitation. This running example is a shopping list application, a screen shot of which is shown in Fig. 1.

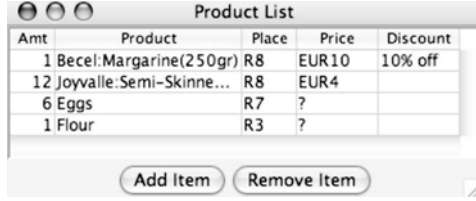


Fig. 1. Screen shot of the shopping application when inside a store.

The list can contain two kinds of products: generic products such as eggs and flour, and specific products that also identify a brand and container size. In Fig. 1, the first two items are specific products, and the last two are generic products. When inside a store, the list contains extra information. This is obtained using a network local to the store itself. The location of the products inside the store is shown, and for specific products their price and discounts, if any, are also displayed.

In a first step, we have implemented the shopping application as a non-Aml distributed system, taking care to have a clean modular decomposition of the application. Figure 2 shows the class diagram of this implementation, where we have omitted impertinent classes. The diagram is fairly self-explanatory. The only classes meriting an extra description are **Shop Product Info** and **Specific Info**: These classes contain the extra information for a given product that is displayed when inside a shop. Whenever the user wishes to add an item, the **Shopping List** firstly creates a **Product** or **Specific Product**, depending on the amount of information given. The shopping list then requests the **Shop** for the extra information for that product, and links this to the **Product** before adding the item to the list.

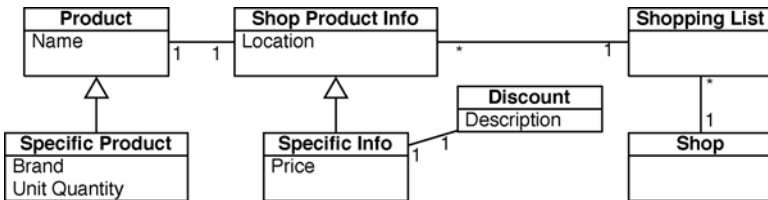


Fig. 2. Diagram of relevant classes of the shopping application

2.2 Features Missing From Futures

When the shopping list application is not connected to the server, using futures as placeholders for the **Shop Product Info** or **Specific Info** allows it to continue

operating despite no such information being available. The future is linked to the **Product** or **Specific Product**, and the item is added to the shopping list. When entering a shop, the shopping list application will connect to a server and the future will be resolved, allowing the extra information to be shown. Consequently, it seems that futures are indeed a suitable abstraction for dealing with disconnected operations in this context.

The above scenario however does not take into account the behavior of the user interface (UI) shown in Fig. 1. Whenever an item is added to the list, the UI should, of course, reflect this. Therefore, after the item is added, the UI refreshes itself, reading out the required values for the different elements in the grid. When disconnected from the server, some of these values will be contained within futures, e.g., the place of an item. As a result these calls will block, blocking the UI and rendering the application unusable until a network connection is established, which resolves the future.

It is clear that the above behavior is not what a user would expect. It should be possible to add and remove products at all time, regardless of whether the application is connected or not. Furthermore, to enable this, the user will be willing to accept some information not to be available in the list, and to be replaced with mock values. For example, when disconnected, place and price of products may be represented by a question mark, and the discount may be empty. It is however essential that, once a connection has been established, such mock values are replaced with the true values as obtained from the server. Vice-versa, whenever the connection is lost, these mock values should be put in place again. This will allow new values to be obtained from a server when a connection is re-established. In our example, this will allow a user to wander from store to store, and always have the extra information for the current store being shown. When entering a store the connection will be re-established with the server for that store, which entails that the futures will resolve to the data for that store.

3 Tagged Futures

It is our intent to allow futures to be useful beyond what is currently possible when faced with connection volatility, as we have discussed above. To achieve this, we propose in this paper to extend futures as follows:

Mock values: can be specified as results of accesses to unresolved futures.

Update mechanism: when the futures are resolved, interested parties are informed and can take appropriate actions.

Invalidation mechanism: reverts a resolved future to its prior form on network disconnects.

The kernel of our proposal lies in adding tags, i.e., metadata to futures. Both the update and invalidate mechanism are a natural consequence of adding this metadata, as we discuss next.

3.1 Adding Metadata to Futures

The main contribution we present in this paper is the concept of adding metadata, as tags, to futures. This will alleviate some of the limitations of futures, therefore less restricting the applications' behavior in a disconnected setting.

Concretely, the first kind of metadata we add is mock values. These mock values are specified by the programmer of the application, in the class for which the future is a stand-in. These mock values will then be returned as a result of an access to the future, i.e., a method call or a field read. Note that we consider specifying such mock values as optional: if no mock value is given, the access will simply block.

As a result of this extension of futures, mock values will now be used by other objects in the system. Whenever futures are resolved, these mock values are no longer required and should also be replaced by the real values. Furthermore, any computation that has been performed using the mock values should be invalidated, and re-executed with the real values. To allow this, we propose the use of an update mechanism in addition to future resolution. This mechanism informs objects that use mock values that the future has been resolved. This allows them to perform any necessary updates, as they see fit.

The above two features provide support for a program to change from a disconnected to a connected state. To provide support for the inverse: changing from a connected to a disconnected state, we propose to use an invalidation mechanism. This mechanism invalidates all objects that are the result of the resolution of a future. As a result, these objects revert to their original future. In analogy to network connection, all computation dependent on these, now invalid, objects is invalid. The above update mechanism will again be triggered, allowing necessary updates to be performed.

3.2 Futures, Passive Futures, Possible Futures, and Future Observers

Conceptually, our introduction of tagged futures adds four new kinds of objects to a distributed system that serve to handle connection volatility. These new kinds of objects are Futures, Passive Futures, Possible Futures and Future Observers.

Futures are placeholders for objects that are unavailable due to the absence of network connections. When the connection is established, futures will automatically resolve to the real value. When the connection is dropped, the real value will automatically revert to the future. Methods and fields of futures may be tagged with mock values, to be returned when these are accessed. If no mock values are given, these accesses block until the future is resolved. In the shopping application, we can use futures for the **Shop Product Info** and **Specific Info** classes. When disconnected, these will return mock values for the location and price of objects, e.g., a question mark.

Passive Futures are a simplified version of futures. Passive futures do not have the ability to resolve to the real value when the network connection is established. Instead, passive futures let some other object assume responsibility for their resolution. The object responsible will usually be another future. We introduce passive futures to allow the resolution of multiple related futures to be handled by one coordinating authority. In the shopping application a passive future can be used for the **Discount**. When disconnected it will return an empty description for the discount. Upon connection, futures for **Specific Info** will handle the resolution of associated **Discount** instances.

Possible Futures are the objects that are substituted by futures or passive futures when the application is offline. In the shopping application, the classes **Shop Product Info**, **Specific Info** and **Discount** therefore are Possible Futures.

Future Observers are objects that may use a mock value of a future. These need to be notified when a future is resolved and also when an object is reverted to a future. This allows them to perform necessary updates. In the shopping application, the shopping list is a future observer. It observes all futures for **Shop Product Info** and **Specific Info** objects, and will refresh the UI after futures are resolved or reverted. As a result, when in a shop the additional information will be shown, and outside of a shop the mock values for this information.

4 Implementing Tagged Futures with Spoon Graffiti

We have chosen to implement our proposal using source-code transformations so that tagged futures have a minimal impact at runtime. The system we created is based on the Spoon transformation engine [5], and is called Spoon Graffiti¹. Spoon allows the transformation of a program by means of successive processing rounds. These are implemented as visitors of a model derived from the program's abstract syntax tree. They are directed by the annotations present on various source code elements (classes, methods, fields, etc). Spoon is seamlessly integrated with the Eclipse IDE. This permits our tool to report errors on the definition of the tags in a transparent way, that is, errors can be presented just as compilation errors. This is specially useful when processing annotations that have Java expressions as arguments, as will be presented in the next section.

Thanks to using source-code transformations, the only overhead which remains at runtime is a class that reifies the online or offline state of the application. This minimal infrastructure is dependent on the distribution mechanism used, which currently is Java RMI. This class can however easily be re-implemented for a different distribution mechanism. The bulk of the behavior of the application, with regard to connection volatility, is implemented outside of this infrastructure, and we discuss it next.

¹ Because the future is tagged.

4.1 Tagged Futures as Annotations

To add support for connection volatility to a distributed application, a developer adds annotations to the code, as well as a number of additional methods. The use of annotations allows this extra behavior to be added without tangling it with the core behavior of the application.

The behavior of Futures and Passive Futures is realized by modifying the code of the classes of Possible Futures. Modifying the classes thus avoids issues regarding object identity, as the Future is the same object as the Possible Future. The downside of this is that, if the Futures are not passive, Possible Future classes need to implement a method for resolution. Similarly, generic behavior is added to classes that contain the annotations for a Future Observer. Methods that perform the actual update of the observer need to be implemented by the developer. We discuss this in more detail following the five types of annotations we have defined, which are shown in Tab. 1.

	Type	Optional Argument	Usage
@Future	Method, Field	An expression	Future, Passive Future
@Connect	Method		Future
@ObservedFuture	Local Variable		Future Observer
@Online	Method	Class	Future Observer
@Offline	Method	Class	Future Observer

Table 1. Defined annotations with their type and corresponding usage

The **@Future** annotation is added to a method or a field, making the class that contains it a possible future class. If no argument is given to the annotation, calls to that method or accesses to that field when the application is offline will block. Otherwise the result of evaluating the argument expression (which is encapsulated in a string literal) is returned. Note that in possible future class, methods and fields that have no such **@Future** annotations are not modified. This is so to support behavior which is unaffected by the presence of a connection.

Possible Futures that also contain the **@Connect** annotation will be replaced by futures that are not passive. The annotation declares the method that is called to resolve the future. The method will be called when a reconnection occurs. It should act as an initializer for the object: assigning to all fields the values it obtains over the network.

Future observers indicate which possible futures they observe using the **@ObservedFuture** annotation, which is given to instance variables of methods. At runtime, all values assigned to these variables will be considered as being observed. Upon network connection, these futures will be resolved by a call to their method annotated with **@Connect**. If a future is observed by multiple observers, this method will only be called once. Also, if a future is not observed, the method will not be called, i.e., it will not be resolved.

Future observers declare their interest in notification of future resolution or reverting to futures by annotating methods with `@Online` respectively `@Offline`. These methods should take one argument, of the type of the superclass of all possible future classes. After a future resolves respectively a possible future reverts, these methods will be called with the just changed object as argument.

5 The Shopping Application Revisited

We now illustrate how tagged futures and our implementation using Spoon Graffiti provides for a usable and non-tangled abstraction of connection volatility. We do this by revisiting the shopping application, of which the modifications are outlined in Fig. 3.

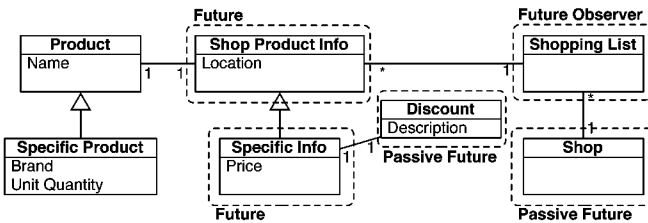


Fig. 3. Offline shopping application, with object kinds defined by the annotations.

We do not treat the entire application here, but instead focus on significant sections. We first discuss the Specific Info and Discount classes, before talking about the Shopping List and the Shop. Below is an excerpt of the code for the Specific Info and Discount classes:

```

public class SpecificInfo extends ShopProductInfo {
    private String price;    private Discount disc;

    @Future("\TBD\")
    public String getPrice() { return price; }
    public String getDiscount() {return disc.reduction_type; }

    @Connect
    public void become(){
        SpecificInfo realSPI = (SpecificInfo)
            Shop.getProductInfo(target_product);
        location = realSPI.location;
        price = realSPI.price; discount = realSPI.discount; }
    [... constructors omitted ...] }
public class Discount {

```

```

@Future("\TBD\")
public String reduction_type;
[... constructors omitted ...] }

```

This code first shows how the `@Future` annotation can be applied to both methods and fields. Second it illustrates a use of a method without a `@Future` annotation tag, to delegate to a `Discount` object, which itself takes care of disconnected operations. A similar case is in `Shop Product Info`, which allows a reference to the product name to be obtained by the shopping list. Third, this code provides an example of how to resolve a future, in the `become()` method. This method obtains a new `Specific Info` from the server, and simply copies over all the relevant data, including the `Discount` object. As a result, futures for `Discount` objects can be passive. We omitted in the listing above the two constructors for each class: one for a normal instantiation used when online, and one for an 'empty' instantiation used when offline.

```

public class ShoppingList implements TableModel {
    public void addProduct(ShopProductInfo prod, Integer amt){
        @ObservedFuture ShopProductInfo p2 = prod;
        products.add(prod); prod_amounts.add(amt);
        this.changed(prod); }

    @Online
    @Offline
    private void changed(ShopProductInfo prod){
        for(TableModelListener listener : tml)
            listener.tableChanged(new TableModelEvent(this)); }
    [ ... fields and table model methods omitted ... ] }
public class Shop {
    @Future("ShopProductInfo.createEmptySPI(prod)")
    public static ShopProductInfo
        getProductInfo(Product prod){
        [... body omitted ...] }
    [... server implementation omitted ...]
}

```

The Shopping List class implements the Java Swing Table Model class, which allows it to be used in a Swing table, as shown in Fig. 1. Adding a product to the list, in the `addProduct` method implies that futures for it are observed, which is declared through the `@ObservedFuture` annotation. Future resolution, reverting to futures, as well as adding and removing products all trigger the `changed()` method. This method simply refreshes the UI.

The Shop is a passive future, that in an offline state returns empty Shop Product Info objects when queried, as indicated by its `@Future` annotation. The convenience method called in the argument of the annotation creates empty Shop Product Info or Specific Info objects. As the Shop itself contains no state that needs to be updated when the connection goes online or offline, it can be

represented by a passive future when offline. Note that by having the Shop itself as a tagged future we do not need any extra mechanism for the creation of futures when the application is offline.

This concludes the revisit of the shopping application. When this application is offline, the extra information for a product will be displayed as TBD. When the application goes online, the extra information will automatically be obtained from the server and displayed. To implement this behavior, no code needed to be added to, or changed in, methods that provide the core functionality of the application. As a result, this implementation shows that tagged futures, as implemented in Spoon Graffiti, are indeed a non-tangled abstraction that provides adequate support for connection volatility.

6 Related Work

Related work can be subdivided in to major categories: distributed languages and distributed middleware.

Using futures as return values of a synchronous call has previously been used in languages such as ABCL/f [9] and Argus [4] (where they are known as promises). However in both these languages accessing a future blocks, which yields the problem we have elaborated in Sect. 2.2. In the AmbientTalk language [1, 2], calls are asynchronous, and a special `when` construct is used to delay execution of a block of code until the future is resolved. Again, as accessing an unresolved future blocks, this yields the problem described in Sect. 2.2. Furthermore, we consider the use of the `when` construct to produce code which is more tangled than our solution.

A significant amount of research has been performed on middleware for mobile networks, however to the best of our knowledge no system has yet been constructed that provides abstractions specifically for connection volatility in an AmI context. The most appropriate middleware solution seems to be Rover [3], as it allows for queuing of a remote message call in conjunction with weak replica management. While this can conceivably be used to implement behavior similar to the used of tagged futures, this would firstly not be encapsulated as one abstraction and secondly be unlikely to be tangled code. Similar to Rover, Coda [7] and XMiddle [10] also provide support for replica management but have no specific abstraction mechanism for connection volatility.

7 Conclusions and Future Work

In this paper we have proposed an extension to futures to provide better support for connection volatility in AmI applications. To the best of our knowledge, this is the first work performed to provide such an abstraction, allowing the specification of offline behavior in a non-tangled way.

Our proposal add tags to futures, specifying mock values to be used when offline, together with an update and invalidation mechanism for these mock values. We have discussed how we have implemented these extensions, and have

shown though an example how they cleanly add support for connection volatility. We believe that tagged futures are an elegant abstraction for connection volatility which will significantly ease development for AmI applications.

Future work consists of exploring other kinds of metadata, e.g., instead of immediately reverting to a future when going offline, specifying a timeout, indicating a time-span in which this data is valid when offline. Furthermore, we consider adding support for writing to futures, so that when going online this data is written to the server. This amounts to replica management and will therefore entail a conflict detection and resolution mechanism, as in Coda [7], Rover [3] or XMiddle [10].

Spoon Graffiti, the full code of the shopping application example, as well as other examples can be obtained from: <http://spoon.gforge.inria.fr>

References

1. J. Dedecker, T. Van Cutsem, S. Mostinckx, T. D'Hondt, and W. De Meuter. Ambient-oriented programming. In *OOPSLA '05: Companion to the 20th annual ACM SIGPLAN conference on Object-oriented programming, systems, languages, and applications*, pages 31–40, New York, NY, USA, 2005. ACM Press.
2. J. Dedecker, T. Van Cutsem, S. Mostinckx, T. D'Hondt, and W. De Meuter. Ambient-oriented programming in ambienttalk. In *ECOOP 2006 - Object-Oriented Programming*, volume 4067 of *LNCS*, pages 230–254. Springer, July 2006.
3. A. Joseph, J. Tauber, and F. Kaashoek. Mobile computing with the rover toolkit. *IEEE Trans. Comput.*, 46(3):337–352, 1997.
4. B. Liskov and L. Shrira. Promises: linguistic support for efficient asynchronous procedure calls in distributed systems. In *PLDI '88: Proceedings of the ACM SIGPLAN 1988 conference on Programming Language design and Implementation*, pages 260–267, New York, NY, USA, 1988. ACM Press.
5. R. Pawlak, C. Noguera, and N. Petitprez. Spoon: Program analysis and transformation in java. Technical Report 5901, INRIA, may 2006.
6. Jr. R. Halstead. Multilisp: a language for concurrent symbolic computation. *ACM Trans. Program. Lang. Syst.*, 7(4):501–538, 1985.
7. M. Satyanarayanan, J. Kistler, P. Kumar, M. Okasaki, Ellen H. Siegel, and David C. Steere. Coda: A highly available file system for a distributed workstation environment. *IEEE Trans. Comput.*, 39(4):447–459, 1990.
8. A. Schill, B. Bellmann, W. Bohmak, and S. Kummel. System support for mobile distributed applications. In *SDNE '95: Proceedings of the 2nd International Workshop on Services in Distributed and Networked Environments*, page 124, Washington, DC, USA, 1995. IEEE Computer Society.
9. K. Taura, S. Matsuoka, and A. Yonezawa. ABCL/f: A future-based polymorphic typed concurrent object-oriented language - its design and implementation. In G. E. Blelloch, K. M. Chandy, and S. Jagannathan, editors, *DIMACS '94 Workshop*, volume 18 of *Specification of Parallel Algorithms of Series in Discrete Mathematics and Theoretical Computer Science*, pages 275 – 291. American Mathematical Society, 1994.
10. S. Zachariadis, L. Capra, C. Mascolo, and W. Emmerich. Xmiddle: information sharing middleware for a mobile environment. In *ICSE '02: Proceedings of the 24th International Conference on Software Engineering*, pages 712–712, New York, NY, USA, 2002. ACM Press.

Towards Semantic Resolution of Security in Ambient Environments

Mario Hoffmann¹, Atta Badii², Stephan Engberg³, Renjith Nair², Daniel Thiemert², Manuel Matthess¹, and Julian Schütte¹

¹ Fraunhofer SIT, GER

² IMSS, University of Reading, UK

³ Priway, DK

Abstract. Driven by new network and middleware technologies such as mobile broadband, near-field communication, and context awareness the so-called ambient lifestyle will foster innovative use cases in different domains. In the EU project Hydra high-level security, trust and privacy concerns such as loss of control, profiling and surveillance are considered at the outset. At the end of this project the Hydra middleware development platform will have been designed so as to enable developers to realise secure ambient scenarios. This paper gives a short introduction to the Hydra project and its approach to ensure security by design. Based on the results of a focus group analysis of the user domain “building automation” typical threats are evaluated and their risks are assessed. Then, specific security requirements with respect to security, privacy, and trust are derived in order to incorporate them into the Hydra Security Meta-Model. How concepts such as context, semantic resolution of security, and virtualisation support the overall Hydra approach will be introduced and illustrated on the basis of a technical building automation scenario.

1 Introduction

A digital revolution is changing our life and work styles powered by an embedded ICT-empowered environment. From washing machines used in our homes over logistics tracking to mobile phones and PDAs on which we depend to communicate and work, they all deploy embedded systems. World Semiconductor Trade statistics show that 98 percent of the programmable digital devices are embedded devices [4]. Whilst the plethora of embedded programmable devices is re-assuring of a competitive, diverse and hopefully enduring creative base of Research and Development in such critical components, it also makes for a heterogeneous array of devices distributed in the ambient environment which cannot communicate with each other due to lack of a common protocol to provide for the much needed seamless integration. Imagine any of your devices being able to interact with any other device so that even a customised PDA with an interface that is familiar to the user can manage devices such as TVs and door locks in a hotel room, a short-distance device can use long-distance capabilities of other

devices and users can manage devices in other domains remotely. Further, every application or service could use all devices in place so that e.g. an application can utilise all available sensors or support devices deployed independently of the application. This depends of course on permissions of the developer and requirements of the user – e.g. users could choose services that respect security and privacy according to a certain policy. Security challenges are hard in homogeneous solutions, but escalate when moving to enable inclusive interoperability. Here we need to depart from traditional thinking based on device identification with significant use of implicit knowledge and manual administration to a model-driven and semantically open security model based on explicit assertions and shared ontologies. For developers to open the digital access to devices and applications, they require a flexible and much more nuanced security model; for users to be able to trust communication between devices, they need new models for user controls and security fault tolerance. Imagine what happens if biometric sensors in people’s homes suddenly turn up to be accessible and controllable by neighbours and criminals, acting as commercial spyware or even political control. The fear of such scenarios significantly reduces the value potential of this embedded networked revolution. The EC co-funded FP6 IST project Hydra (Networked Embedded System Middleware for Heterogeneous Physical Devices in a Distributed Architecture) to support some of the leading companies and research institutes in Europe in attempting to fulfil the vision of such seamless integration in the ambient environment of heterogeneous devices. Hydra aims to develop a middleware layer for building secure, fault-tolerant networked embedded systems where diverse heterogeneous devices co-operate [5]. The emergent world of ambient intelligence and pervasive computing would be closer to realising its full potential if the embedded devices deployed, for example in a home, are able to communicate semantically interoperable with each other and cooperate to fulfil tasks. The Hydra mission is to provide this capability by designing the required middleware facilitating semantic interoperable security.

2 Hydra Challenge

When speaking of interoperability the challenges we are facing are manifold. Starting with the simple issue of having two devices, one being able to use Wifi, the other being able only to use Bluetooth we are confronted with different types of protocols, not only in terms of communication but also in terms of security. In most projects, industrial or research, security is often a neglected area as developers tend to ignore its importance. It is mostly thought to be an add-on which can be implemented later, if at all. This holds several threats as most security leaks can only be closed afterwards with an immense effort. Considering these security leaks from the very beginning is the aim of the Hydra project. Such Security by Design with the main focus on interoperability of security helps to build a powerful tool to enable manufacturers and developers to develop secure applications and devices in an ambient environment. To demonstrate the middleware in various areas the project is primarily focusing on 3 domains: *Home*

Automation, Healthcare and Agriculture. The Security by Design approach itself is focusing on enabling secure interoperability. This means that a developer of embedded applications for ambient environments should not need to take care that the devices his applications uses or communicates with have the same specifications, e.g. same communication protocol or security protocol. If one device interacting with the application uses protocol *A*, and another device interacting with the application uses protocol *B*, then the developer of the application should be able to handle this using the Hydra middleware. This will be achieved by semantic resolution of security, i.e. turning physical capabilities and functionalities into semantically understandable descriptions, making the interaction independent from the specifications of network, devices and applications/services. In the next sections we will present a bird's eye view of our research within the Hydra project to derive the requirements and the approaches which we will use in order to fulfil these requirements. In this way we intend to provide some answers to our common concerns to achieve not just secure interoperability but potentially also cooperativity amongst heterogeneous embedded systems serving us in the emergent ambient environment.

3 Security Requirements Engineering

In the Hydra project the following security requirements specification process (cf. 1) is performed in order to ensure security by design: First, we derive a technical scenario from the building automation user domain scenario. Then, we conduct discussion rounds with focus groups of expert developers who are potential future Hydra middleware users. In the focus group analysis, actors, assets, and roles are identified. Based on the analysis of multilateral communication schemes between those roles we identify high-level threats to Hydra. Following the concept of "security by design" we derive the overall protection goals that have to be taken into account for the design of the Hydra middleware platform. The results of the focus group analysis in combination with the state-of-the-art are the basis for the risk analysis. Here, the identified threats and potential (threat) actors are analysed and described. Probability, impact and effects of successfully performed attacks are assessed and used as input to calculate the risk of a threat. From that point it is then possible to estimate how serious actors should take a threat. Finally, the process results in derived and prioritised security and trust requirements based on the results of the risk analysis.

A. Technical Scenario The technical scenario used in our approach is built on the vision scenario for the user domain "Building Automation". Since the vision scenario is not very detailed in terms of technical aspects the technical scenario adds this information. The aim of the technical scenario is to give the members of the focus group a better and more detailed starting point for their technical interpretations to elicit requirements for the security and trust within the Hydra project.

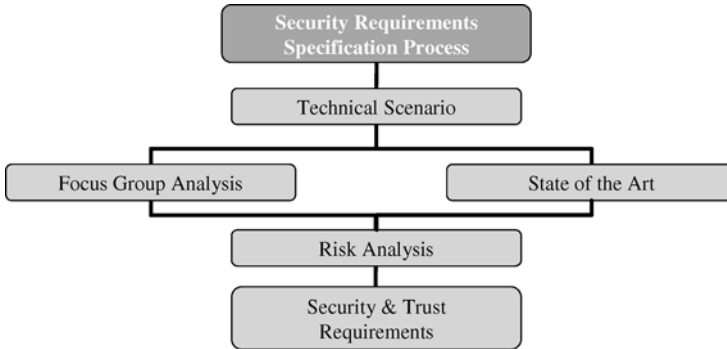


Fig. 1. Security Requirements Specification Process

B. Results of Focus Group Analysis The technical scenario is the starting point of focus group analysis. Here, an initial threat analysis of the technical implications identifies assets to protect such as billing information, user preferences and profiles, as well as communication data, actors such as building operators, service agents and occupants, and roles such as network operators, content providers and end-user. The analysis of multilateral communication schemes between such roles derives the main protection goals that the developers would expect to be met taking advantage of the future Hydra middleware platform. These comprise: (1) Confidentiality, (2) Integrity, (3) Authenticity, (4) Authorisation, (5) Availability, (6) Non-repudiation, and (7) Privacy.

C. Results of Risk Analysis On the basis of these protection goals the risk analysis defines eight steps as part of a Hydra specific user-centric framework for risks analyses and evaluation. This comprises a pattern-based description of assets, (threat) actors, and threats as well as the assessment of attacks, their impact, their probability, and security implications. The highest risks in our analysis according to the usage scenario are expected to affect user data and identity, where identity comprises both user identities as well as device identities.

D. Security and Trust Requirements The derivation of the security and trust requirements based on the previous results conclude the security analysis. The requirements are prioritised according to their classification into the categories mandatory, desirable and optional requirements. With respect to the risk analysis the most important requirements concern securing confidential information, e.g. private data during transactions, and empowering the user to control both his individual context and the disclosure of personal information to the immediate vicinity as well as to authorised (virtual) parties.

E. Hydra Synthesis The more personalised information has to be collected, linked and analysed by ambient systems in order to serve users according to

their individual context, the more the specific protection goals have to be balanced between actors in those scenarios. More than 80% of the security and trust requirements have been classified “mandatory” to be fulfilled by the Hydra security model. Most important requirements aim at (1) securing confidential information, (2) authentication mechanisms, (3) context-aware access control, (4) context and semantic reasoning, (5) interoperability of (security) communication protocols, and (6) distributed trust models. In order to fulfil these requirements we propose a security meta-model with the following key characteristics: “be interoperable with existing security models”, “be extendable”, “allow developers to semantically define security requirements”, “allow developers to virtualise end-users, services, and devices”, and “simplify implementation”. The concepts needed to realise the Hydra Security Meta-Model, i.e., (1) context security, (2) semantic security resolution, and (3) virtualisation, will be introduced in detail in the next section.

4 Hydra Security Approach

In this section, the main concepts of Hydra’s security capabilities are presented and the approach to the Hydra Security Meta-Model is outlined.

4.1 Context

One of the main concepts of Hydra is the notion of context. By context, we understand any information that can be used to describe the situation of an entity, whereas the information is observer-specific, i.e. there is no global context [8]. The processing of context is structured in four layers: *Context Sensing*, *Context Awareness*, *Situational Awareness* and *Reasoning*. At the first two layers, raw data, e.g. from sensor nodes is collected and processed in a way that allows defining a structured representation of context. At the next layer, the awareness of the situation the entity currently behaves in is created by linking the contexts of other entities nearby. Reasoning finally is the process of deducing possible consequences of the current situation.

Although higher layers of context processing are application-specific and cannot be part a middleware, the idea of context will play a major role in Hydra. On the one hand, context data will be a part of the integrated security model, e.g. by supporting Attribute-Based Access Control (ABAC) mechanisms [1, 2]. On the other hand, Hydra aims to enable the development of ambient environments by providing context data along with processing operations and tools for context-aware applications while reducing the security problems which may be introduced by the concept of context:

Context contains a lot of sensitive data (e.g. location or interests of a user) and thereby raises the risk of privacy violations. Especially due to uncontrolled linkage of different contexts, it would become impossible for an user to keep his personal data under control. Thus, it is critical to provide only as much context information as needed to an application or a service. Vice versa, every entity

may be a data source for other context sensing entities and thereby could unintentionally reveal information about itself. Hydra will address these problems by providing concepts which help limiting the amount of information that is gathered and exposed across different contexts while still allowing to link contexts in order to generate situational awareness. One of these concepts is virtualisation which will be described in the next section.

4.2 Virtualisation

As interconnection increases and users and devices behave in different contexts, perimeter security tends to fail. Moreover, a number of security problems and functional requirements arises and needs to be addressed by appropriate mechanisms:

At first, it must be possible to avoid the tracking of users and devices across different contexts. Hence, information leakage from one context to another must be prevented. Further, an entity might need different context-specific representations. An example would be a home automation system which provides a different interface and different functionalities, depending on whether it is used by a technician or by a normal user, whether it is in maintenance mode or in normal operation mode. It may be required as well to apply mechanisms to legacy devices which do not have the capabilities to provide these mechanisms by themselves.

Hydra uses the concept of virtualisation to address these issues. By virtualisation, we understand the process of creating a logical representation of an entity. As the logical representation is an entity in itself, it is feasible to nest and combine virtualisations and by that way e.g. create a single logical representation of multiple different entities. As virtualisation refers to generic entities, not only hardware devices can be virtualised but also applications, users and their identities.

Thus, Hydra proposes to apply virtualisation mechanisms to different entities: *Virtual devices* or *proxies* act as logical representations of devices. By defining a proxy for a physical device, it is thus possible to integrate non-Hydra-enabled devices into a Hydra-enabled network and to enable further high-level concepts like semantic description of device capabilities or resolution of security. In addition, physical devices can be combined to virtual devices which are tailored to the application – e.g. it is possible to define a “virtual” global light switch that controls all lights within a building. Virtual devices will also allow representing a device with a reduced set of functionality – either to reduce complexity for the user or in terms of access control⁴.

Virtual identities are an important aspect, as well. They allow a user to define different identities for different contexts. Through virtual identities it is possible to recognise a user within a certain context while not being able to identify

⁴ This will of course only prevent accesses to the device going through the proxy. Controlling direct physical access to a device is out of scope of a middleware such as Hydra.

the same user in a different context. Thus, virtual identities help preserving the user's privacy by avoiding the linkage of identities across context boundaries which would otherwise lead to accumulated private information about a user. Another advantage is that virtual identities help a user not to disclose more information about himself than required. For example, if a service agent enters a house in order to carry out a maintenance task, he can identify himself as a delegate of the service company instead of providing personal information about himself. It is also conceivable to extend the concept of virtual identities to *virtual users* in form of personal agents, performing tasks (semi-) autonomously on behalf of the actual user.

Further virtualisation techniques are possible; however, the above described mechanisms will make up the main part of Hydra's virtualisation design.

4.3 Semantic Resolution of Security

Interoperability of heterogeneous devices and applications also requires security to be resolved at a semantic level. This is to ensure translation between heterogeneous devices, to delegate security decisions from applications to the middleware layer and to ensure adaptability according to the specific context. While the Hydra middleware will not enforce a specific security model on devices or applications, it is nonetheless responsible for ensuring interoperability in even sensitive applications. The goal is the middleware to be an abstraction layer between the security models and protocols supported by devices and applications and the specification of security requirements made by the developer. Thus, a model-driven approach is needed which allows the representation of security requirements, policies and capabilities at a semantic level and translates these specifications to a concrete environment. One approach would therefore be the usage of ontologies for the semantic representation of protection goals, access rules, security capabilities as proposed in [6] and [3]. However, Hydra itself will not provide ontologies, but rather define the requirements and interfaces to integrate such.

4.4 Security Boundaries

The interface between Hydra and non-Hydra defines the security boundary. The security parameters of all entities within the security boundary can be represented in a semantic way and thus be controlled by Hydra (but don't have to). Entities that are outside the security boundary cannot be controlled by the middleware and thus their security parameters are not subject to the rules specified within Hydra. The security boundary is flexible and depends primarily on developer and user choices about the extend to which devices and applications will be part of the Hydra environment. In this way, as a facilitator rather than a guarantor of security, Hydra provides for security-aware design and development by enabling developers of embedded systems and to include security and privacy aspects in their applications.

4.5 Towards a Security Meta-Model

In heterogeneous environments, one impediment to interoperability are the differences between security protocols, identity schemes, authentication mechanisms, etc. In order to overcome this drawback, Hydra will make use of a Security Meta-Model which will mainly comprise of the above described concepts context, virtualisation, flexible security boundaries and semantic resolution of security. This model will be a meta-model, i.e. it will be a “model of models”, abstracting from concrete security mechanisms to semantic descriptions. Developers will have the opportunity to define security requirements at a semantic level and leave the mapping from semantic specification to concrete security mechanisms to the middleware. So, although Hydra is a middleware and thus can neither make context-based decisions by itself, nor enforce security, it will provide developers with concepts which allow creating context-aware, yet secure applications in heterogeneous environments.

5 A Usage Scenario

In order to illustrate the necessity and benefits of the Hydra Security Meta-Model, we implement a demonstrator scenario (cf. Fig. 2). The demonstrator is based on the technical building automation scenario used as the starting point of the security analysis in section 3. In this scenario, a service agent sent by a service provider needs physical access to a faulty heating system of a resident who is currently not at home. The steps 1 to 4 in Fig. 2 focus on the security challenges and how these will be resolved through the realisation of specific parts of the Hydra Security Meta-Model: The scenario starts with a critical malfunction in the heating system that has been detected by a device specific Hydra proxy in step 1. In current home and office automation systems Hydra proxies serve as virtual representations of legacy devices in the Hydra network as defined in our virtualisation concept in section 4.2. On the one hand they take into account device specifics by semantic description of device capabilities while on the other hand they take advantage of the Hydra security mechanisms by semantic resolution of security for example. Future devices are envisioned to be Hydra-enabled so that they can run Hydra middleware by themselves. Once the heating system’s Hydra proxy has sensed the malfunction and changed its status the Hydra based building automation system (HBAS) is aware due to the fact that the contexts have been linked a priori. Therefore, changes to the context of the Hydra proxy are known to the HBAS. The HBAS then reasons taking into account further information like season or temperature to determine the criticality of the error and sends an error message to the resident. The HBAS request includes the error protocol and recommends calling a service provider to fix the problem.

In step 2 the resident receives the authentic request from his HBAS and decides to follow the recommendation. He digitally signs the error protocol and sends it – including a context restricted authorisation token – to a service provider of his choice. The authorisation token will be used in step 3 which

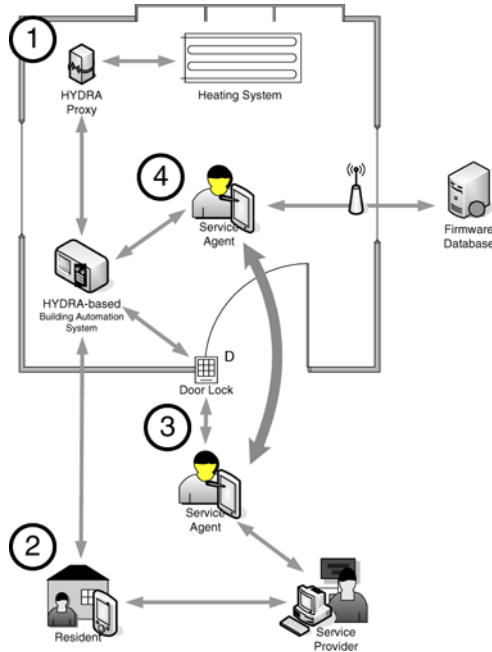


Fig. 2. Demonstrator Scenario

describes the situation in front of the resident's house. In this step, three different objects perform context sensing: the mobile device of a service agent, the door lock and the HBAS. The service agent presents the authorisation token stored on a Hydra-enabled PDA to the door. The door forwards the token which has been additionally signed by the service provider to the HBAS that proves it valid and trusted. Thus, the service agent is now allowed to enter the house and gets access to the HBAS in the final step. Note that the HBAS does not ask for the service agent's identity – the double-signed authorisation token (by the resident and the service provider) is sufficient to guarantee liability. In the final step – step 4 – the service agent gets context restricted access to the Internet in order to download the latest version of the heating system's firmware update. After fixing some configuration settings and installing the update of the firmware the heating system works smoothly inside of its specification again. In addition to the authorisation process based on trusted credentials and virtualisation, the demonstrator will be improved by two steps: Firstly, semantic resolution of security will add trusted authentication in the Hydra network (even to non Hydra devices by using Hydra proxies as mentioned above). Secondly, the rather simple Role-Based Access Control (RBAC) above will be enhanced to Attribute-Based Access Control (ABAC) mechanisms (e.g., XACML [7]) to support more dynamic and unforeseen scenarios. The demonstrator will be shown at CeBit fair 2008.

6 Summary and Outlook

In this paper we have presented the approach to security, privacy and trust in ambient environments supported by a context-aware middleware. We have presented our process of gathering the requirements for a middleware for heterogeneous networked embedded systems in the Hydra project. Furthermore, we have introduced our approach to meet those requirements which is based on semantic resolution of security, virtualisation, and context, forming a security meta-model. Further research in the project will be focused on applying different technologies of virtualisation on different types of entities, e.g. users, devices or applications. Further, we plan to investigate how different security models can be represented semantically based on ontologies in order to realise interoperability. Such ontologies will also be used to realise semantic models of devices and applications to enable semantic interoperability. The concept of context to support security will be detailed in terms of representation of context information. The final outcome will then be the security meta-model, in addition to a software development kit and an integrated development environment, which will enable developers to involve security aspects from the initial stages of embedded application development.

References

1. Ernesto Damiani, Sabrina De Capitani di Vimercati, and Pierangela Samarati. New paradigms for access control in open environments. In *Proc. of the 5th IEEE International Symposium on Signal Processing and Information*, Dec. 2005.
2. S. di Vimercati, P. Samarati, and S. Jajodia. Policies, models, and languages for access control. In *Proc. of the Workshop on Databases in Networked Information Systems*, March 2005.
3. S. Dritsas, L. Gymnopoulos, M. Karyda, T. Balopoulos, S. Kokolakis, C. Lambri-noudakis, and S. Katsikas. A knowledge-based approach to security requirements for e-health applications. *Electronic Journal for E-Commerce Tools and Applications*, 2006.
4. FAST GmbH for the European Commission. Study of worldwide trends and R&D programs in embedded systems in view of maximizing the impact of a technology platform in the area, Nov 2005.
5. HYDRA. Networked embedded system middleware for heterogeneous physical devices in a distributed architecture. <http://www.hydra.eu.com>, Jul 2007. contract number: IST-2005-034891, duration: 07/2006-06/2010.
6. Naval Research Lab. NRL Security Ontology, Jul 2007. <http://chacs.nrl.navy.mil/projects/4SEA/ontology.html>.
7. OASIS. eXtensible Access Control Markup Language (XACML) Version 2.0. <http://www.oasis-open.org/committees/xacml>, 2004.
8. Bill Schilit, Norman Adams, and Roy Want. Context-aware computing applications. In *IEEE Workshop on Mobile Computing Systems and Applications*, Santa Cruz, CA, US, 1994.

Modeling Decentralized Information Flow in Ambient Environments

Jurriaan van Diggelen, Robbert-Jan Beun, Rogier M. van Eijk, and Peter J. Werkhoven

Institute of Information and Computing Sciences
Utrecht University, the Netherlands
{jurriaan,rj,rogier}@cs.uu.nl; peter.werkhoven@tno.nl

Abstract. This paper proposes a decentralized approach for modeling information flow in ambient environments. We study how query and notification mechanisms can be used to reduce the amount of information exchanged between agents. We will propose qualitative criteria which state whether querying a concept is appropriate given the logical structure of an agent's knowledge base. Furthermore, we will propose quantitative criteria which state which concept is most likely to be most informative, given an agent's information needs and its experience with past events.

1 Introduction

Effective and efficient information sharing is of fundamental importance for ambient intelligence. On the one hand, sufficient information should be exchanged between sensors, devices and users to maximally employ the potential use of the information present in the system. On the other hand, when vast amounts of data are available, information overload becomes a serious issue. Therefore, only the relevant information must be communicated. The problem of information sharing is complicated as the different components in the system typically represent their information at different levels of abstraction. For example, a sensor may deal with low-level information about *Temperature*, whereas an inference system used for crisis management may deal with high-level concepts such as *Fire* and *Emergency*. Another complication is the openness of the system, i.e. new devices may enter and leave the system at any time. This means that the different devices should be capable of organizing their communication networks themselves.

Many approaches that aim at guiding the information flow in ambient environments adopt a centralized approach [4, 9]. One central component is assumed which collects all information and provides access to this information to all other components. Although this approach imposes a clear organization on the information flow, it also raises a number of problems. Firstly, the system becomes brittle as the functioning of the whole system is dependent on one component. Secondly, the central distributor must be able to deal with the heterogeneities of all other components in the system. This makes it very difficult to design this

component, particularly because it is not known beforehand which components will constitute the system.

Therefore, we adopt a decentralized approach by treating every component in a uniform way, i.e. as a fully autonomous agent. In this way, the problem of modeling the information flow no longer needs to be addressed as a whole (as in the centralized approach), but is split up in smaller problems which are handled by the individual agents. Every agent must have sufficient communicative skills to satisfy its information needs in an environment with heterogeneous agents that represent information at different levels of abstraction. Furthermore, the agent's communicative behavior should be minimal such that as few messages as possible are exchanged between them. This is needed to prevent information overload of the agent itself and of the agents around it.

In this paper we will provide a conceptual framework in which information needs and different levels of abstraction can be clearly represented. We also discuss two communication mechanisms, i.e. query and notification requests. We investigate which queries or notification requests can best be posed to reduce the amount of exchanged messages to a minimum.

Our approach to these two issues is as follows. An agent's knowledge base is specified as a multi-context system [6], i.e. it contains multiple contexts that are related by mappings that specify translations between them. A context consists of a set of concepts regarded relevant by an agent for performing one of its tasks. These may be a concepts like *User-Location* and *User-Identity*, which contain important contextual information for a user interface agent [10]. Also, these may be concepts like *Fire* and *Emergency* which are relevant to a crisis management agent, or *Temperature* which is relevant to a temperature sensor. The agent's information needs can be precisely represented using contexts. For example, if the information needs are defined as the context that contains *Fire*, we assume that the agent desires to know whether *Fire* is true or not, at each time instance.

Typically, two agents have some contexts in common and some contexts that differ. The agents can only communicate information that is represented in a common context. This ensures that the language used by the sending agent is understood by the receiving agent. Because the agents may view their world at a different level of abstraction, information may also be represented in a non-common context. In this case, the sending agent must translate the non-common representation to a common representation to become understood by the receiving agent. Thus, the agents must be able to translate between different contexts fluently.

The central question addressed in this paper is which concepts in one context are best to query or request for notification to resolve the information needs stated in another context. We will first approach this issue by formulating several qualitative criteria. In this way, the agent can use the logical structure of its knowledge base to decide whether querying a concept is appropriate. Because the agent bases its decision on prior knowledge, these criteria are applicable from the moment the agent joins the system. We will then approach the issue by formulating several quantitative criteria. This enables the agent to use its past

experience to decide which concepts are most relevant among those concepts satisfying the qualitative criteria. Because the agent bases this decision on past experience, these criteria only become applicable after the agent has been in the system for some time.

The paper is organized as follows. In Section 2, we introduce the conceptual framework. In Section 3, we discuss the qualitative criteria for selecting the best concept to query or to be notified about. Section 4 discusses the quantitative criteria. Section 5 presents a conclusion and indicates directions for further research.

2 Framework

An agent's knowledge base is represented using description logic [2]. A description logic knowledge base consists of a TBox and an ABox. The TBox stores concepts and their definitions (like an ontology), and the ABox stores sentences constructed using these concepts. The TBox represents general knowledge about a problem domain, which is not subject to changes. The ABox represents problem-specific knowledge that is subject to occasional or even continuous change [2].

Because time plays an important role in our framework, we assume that the domain of discourse is specified as a set of time instances. This means that a concept is interpreted as a set of time instances to which the concept applies. For example, if the concept *Fire* is interpreted as $\{t3, t5\}$, it means that there was fire at time instances $t3$ and $t5$. We use a special variable `NOW` to denote the current time instance. This can be implemented by adopting one central time reference for all agents which instantiates the agents' `NOW` variables with the current time.

We adopt the description logic $\mathcal{ALC}(\mathcal{D})$ [1] as a concept language. Without going into the formal semantics, we will briefly discuss its constructs. Concepts are composed using atomic concepts and concept constructors, i.e. \sqcap (conjunction), \sqcup (disjunction), \neg (negation). For example, the concept *Cloudy* \sqcap \neg *Rainy* refers to the concept *Cloudy* and not *Rainy*. Furthermore, the language contains constructs for reasoning with numbers. For example, the construct $\geq_{50}(\textit{Temperature})$ refers to the concept that Temperature is greater than or equal to 50 degrees.

The TBox is specified as a number of inclusion axioms of the form $c \sqsubseteq d$, meaning that the interpretation of c is a subset of the interpretation of d , i.e. all instances of c are also instances of d . For example, the TBox axiom *Cloudy* \sqsubseteq \neg *Rainy* means that all time instances at which it was *Cloudy* are time instances at which it was not *Rainy*. The ABox is specified as a number of membership assertions of the form $c(t)$ meaning that t is an instance of c . For example the ABox assertion *Rainy*($t4$) means that it is rainy at time instance $t4$. For $c(t)$ we will sometimes simply write that c is true at time instance t . For $\neg c(t)$, we will sometimes write that c is false at time t .

Different contexts are implemented by prefixing the atomic concept names with a context identifier (similar to [3]). For example, if the concepts *Rainy*

and *Cloudy* are all defined within context *C1*, a TBox axiom that relates these concepts may be $C1:Cloudy \sqsubseteq \neg C1:Rainy$. TBox axioms may also be used to define relations between concepts in different contexts. In this case, they are called context mappings (also known as bridge rules [6]).

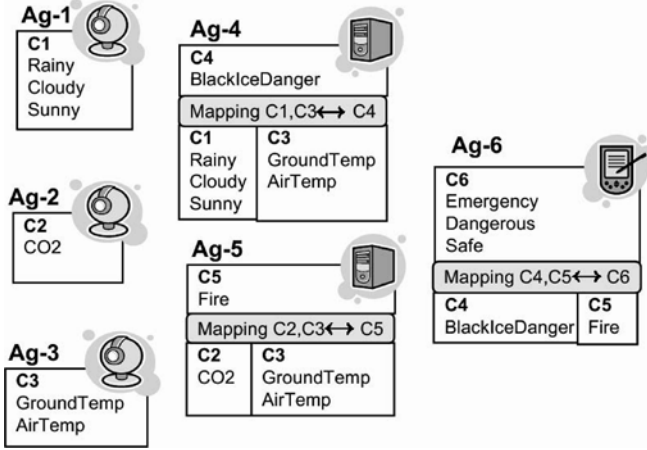


Fig. 1. Example Agents

Example 1.

Figure 1 illustrates six example agents. The agents' TBoxes are subdivided in different contexts which are mapped using context mappings. The TBoxes of Ag-4, Ag-5 and Ag-6 are specified below:

Ag-4

$C1:Cloudy \sqsubseteq \neg C1:Rainy$

$C1:Rainy \sqcap \leq_0(C3:GroundTemp) \sqsubseteq C4:BlackIceDanger$

$C1:Sunny \sqsubseteq \neg C4:BlackIceDanger$

Ag-5

$\geq_{50}(C3:AirTemp) \sqcap \geq_{10}(C2:CO2) \sqsubseteq C5:Fire$

Ag-6

$C4:BlackIceDanger \sqsubseteq C6:Dangerous$

$C5:Fire \sqsubseteq C6:Emergency$

As illustrated in this example, different agents represent their information at different levels of abstraction. They also occupy different roles in the system. The agents Ag-1, Ag-2 and Ag-3 represent low level information and perform the role of a sensor, i.e. they acquire information by sensing their environment. The agent Ag-4 is capable of processing the information produced by the sensors Ag-1 and Ag-3 (using the shared contexts C1 and C3). Likewise, Ag-5 is capable of processing the information produced by the sensors Ag-2 and Ag-3. They

interpret this sensor information in terms of a higher context (C4 for Ag-4 and C5 for Ag-5). These agents perform the role of an *aggregator* [5], i.e. they acquire information from multiple sensors and derive the consequences in terms of a higher level context. The agent Ag-5 can process the information produced by the aggregators and raises the level of abstraction in order to present it to the user, i.e. it functions as an *interpreter* [5]. One may think of Ag-6 as a PDA which, for instance, shows a green light when it is safe, a red light when it is dangerous, and a red light flashing in case of an emergency.

A description logic TBox provides proper means to model an agent's information needs [12] because it is based on an *open world assumption* [2]. This means that when a concept assertion $c(t)$ is absent in the ABox, neither $c(t)$, nor $\neg c(t)$ will be derived, i.e. the truth value remains unknown. Because the information needs apply to the current time instance NOW, we can say that the information needs on c are only fulfilled if either $c(\text{NOW})$ or $\neg c(\text{NOW})$ can be derived. In this case, we say that the agent knows-whether c . This is defined as follows.

Definition 1. *Know-whether*

An agent knows-whether c , iff $KB \models c(\text{NOW})$ or $KB \models \neg c(\text{NOW})$

In the above definition $KB \models$ means *it follows from the knowledge base that*. We assume that every agent has its information needs specified as a set of concepts. For example, suppose that Ag-6 has the information need *Emergency*, *Dangerous* and *Safe*. This means that it wishes to know-whether *Emergency*, *Dangerous* and *Safe*. Because the current time instance NOW increases once in a while, an agent that knows-whether a concept is true at one moment, may no longer do so after some time has passed. This causes a continuous information need for the agent.

A sensor can sense the value of a concept from its environment in order to meet its information needs. Other agents must communicate with other agents for this purpose. For example, for Ag-6 to know-whether *C6:Dangerous* is true, it may query *C4:BlackIceDanger* from Ag-4. This raises an information need for Ag-4, namely *C4:BlackIceDanger*. Subsequently, Ag-4 may query C1-concepts from Ag-1 and C3-concepts from Ag-3. In turn, this raises information needs by Ag-1 and Ag-3. Because these agents are sensors, they sense these values from the environment in order to answer the query.

Fundamental to this process is that, through the chain of queries from end user to sensor, high-level concepts are translated into lower-level concepts that can eventually be observed by sensors. To realize this reduction in information abstraction, an agent must adequately use its context mappings to translate between different contexts. The next section discusses this in further depth.

3 Qualitative criteria

Given the conceptual framework introduced in the previous section, we will regard the following question: given that an agent desires to know whether c in context C_i , which concepts d in C_j are informative?

A first class of concepts that can be readily qualified as informative contains those concepts whose membership either implies or excludes membership of concept $C_i : c$. Suppose that $C_j : d$ is such a concept. If the agent knew that $d(\text{NOW})$, the agent would know either $c(\text{NOW})$ or $\neg c(\text{NOW})$. In other words, the agent knows-whether c . Formally, this condition between $C_j : d$ and $C_i : c$ can be specified as follows: either $d \sqsubseteq c$, or $d \sqsubseteq \neg c$.

Sometimes, membership of a concept can only be decided by posing multiple queries to different agents, a process known as *query dissemination* [7]. In Example 1, *Fire* is such a concept as it must be decided using *CO2* from context C2 and *AirTemp* from context C3. Consequently, for Ag-5 to know whether *Fire*, it must query Ag-2 for *CO2* and Ag-3 for *AirTemp*. Because neither *CO2* nor *AirTemp* directly causes the agent to know-whether *Fire*, the condition discussed earlier must be generalized.

A concept d is called informative for concept c if d can be regarded as part of what must be known to exclude or conclude membership of concept c . Formally, this is defined as follows.

Definition 2. Informative

Concept $d \in C_j$ is informative for concept $c \in C_i$ iff there exists d' for which

- $(KB \models d \sqcap d' \sqsubseteq c \text{ or } KB \models d \sqcap d' \sqsubseteq \neg c)$, and
- $(KB \models d' \not\sqsubseteq c \text{ and } KB \models d' \not\sqsubseteq \neg c)$

This definition states that a concept d is informative for concept c , if two conditions hold. The first condition states that, together with some other concept d' which stems from any context, d and d' must imply c or $\neg c$. The second condition states that membership of d' alone does not imply c or $\neg c$. Hence, the information about d is really necessary for the conclusion. Note that, when concept d by itself is sufficient to imply c or $\neg c$, then d also qualifies as informative. This can be easily shown by taking for concept d' , the concept \top (which is defined as a superconcept of all other concepts).

The idea of querying informative concepts is similar to backward chaining in expert systems [11]. To know the truth-value of a consequent, all truth-values of the conjuncts in the antecedent must be known. We would call all these conjuncts informative.

An example of the previously defined notions is given below.

Example 2. Suppose that Ag-4 in Example 1 has information need *BlackIceDanger*. We can derive the following.

- $C1:\text{Sunny}$ is informative
- $\neg C1:\text{Sunny}$ is not informative
- $C1:\text{Rainy}$ is informative
- $\leq_0(C3:\text{GroundTemp})$ is informative
- $\geq_{50}(C3:\text{AirTemp})$ is not informative
- $C1:\text{Cloudy}$ is not informative

3.1 Query and Notification requests

We can now state the qualitative criteria for querying a concept. These criteria state which concepts in one context are potentially useful to query for an agent that wishes to know whether a concept in another context is true.

An agent that queries a concept d does not know whether the answer will provide information that d or that $\neg d$. Therefore, if only one of the concepts d or $\neg d$ is informative, a query on concept d is appropriate. This is specified as follows.

Specification 1 *Query: Qualitative criteria*

An agent may query concept $C_j : d$ to know whether $C_i : c$ iff

- *d is informative for c or $\neg d$ is informative for c , and*
- *the agent does not know whether d .*

Note that querying a concept d to know whether c , *might* enable the agent know-whether c , but need not necessarily do so. For example, $C1:Sunny$ is informative for $C4:BlackIceDanger$ but $\neg C1:Sunny$ is not. When the answer to a query on $Sunny$ is "no", the agent does still not know whether $BlackIceDanger$.

Besides posing queries, a common interaction mechanism in ambient environments is a request for notification [9]. By requesting notification of a certain concept, an agent gets notified whenever that concept becomes true. The issue when it is best to query or request for notification will be addressed in Section 4.1. Here, we will be concerned with the issue which concepts are best to request for notification.

Contrary to queries, an agent that requests notification of concept d , only gets an answer when d is the case, and not when $\neg d$ is the case. When the agent did not receive any information about d , it assumes that $\neg d$ is the case. Because notification requests are intended to reduce the information exchange, the agent should anticipate on *not* receiving a message. Therefore, the negation of the concept about which it will be notified must be informative. This is formalized as follows.

Specification 2 *Request for notification: Qualitative criteria*

An agent may request for notification of $C_j : d$ to know whether $C_i : c$ iff

- *$\neg d$ is informative for c*

The criteria specified in 1 and 2 are rather loose, i.e. they do not exclude any concept that could potentially be useful to query or request for notification. Therefore, several options are left open for the agent. In Example 2, the non-informative concepts $C3:Airtemp$ and $C1:Cloudy$ are ruled out. The concepts $C1:Sunny$, $C1:Rainy$ and $C3:Groundtemp$ are all left as possible options to query. Using the logical structure of the knowledge base, it is not possible to decide which of these options is best.

For example, if the answer to a query on $Sunny$ is likely to return that $Sunny$ holds, this is a good query, as it immediately enables the agent to know whether $BlackIceDanger$. However, if a query on $Sunny$ is likely to return that $\neg Sunny$

holds, it may be better to query *C1:Rainy* and *C3:GroundTemp* instead. Such a decision must be based on an expectation of the answer. These quantitative issues are discussed in the following section.

4 Quantitative criteria

To take into account what a likely answer to a query will be, we will use the notion of *information gain* [8]. An agent profits most when it queries a concept with the highest information gain.

Before we will discuss information gain, we will discuss an underlying measure from information theory, i.e. *information entropy*. We will apply this measure to characterize the degree of which the truth value of a concept differs over time. A concept that is true at all time instances has entropy 0, i.e. it is maximally pure. Likewise, a concept which is false in all time instances has entropy 0. A concept that is true for half of the time instances, and false for the other half of the time instances has entropy 1, i.e. it is maximally impure. Before we give a formal definition, we introduce the following terminology:

- Δ is the domain of discourse, i.e. the set of time instances which have passed.
- $\Delta^c = \{t \in \Delta \mid \text{KB} \models c(t)\}$ (the set of time instances at which c was true)
- $\Delta^{\neg c} = \{t \in \Delta \mid \text{KB} \models \neg c(t)\}$ (the set of time instances at which c was false)

Information entropy can now be formalized as follows.

Definition 3. *Entropy*

Entropy(KB, Δ , c) = $-p \log_2 p - n \log_2 n$, where

- $p = \frac{\#\Delta^c}{\#\Delta}$ (the proportion of time instances at which c was true)
- $n = \frac{\#\Delta^{\neg c}}{\#\Delta}$ (the proportion of time instances at which c was false)

In the above definition, # is used to denote the number of instances in a set.

Example 3. This example demonstrates how information entropy can be calculated using an agent’s ABox. The table below shows the ABox of Ag-4, after eight time instances have passed. It shows which concepts are true (t) and which are false (f) at which time instances.

The entropy of Sunny can be calculated as follows.

$$\text{Entropy}(\text{KB}, \{t1..t8\}, \text{sunny}) = -\frac{1}{8} \log_2 \frac{1}{8} - \frac{7}{8} \log_2 \frac{7}{8} = 0.543.$$

The entropy of BlackIceDanger is calculated as

$$\text{Entropy}(\text{KB}, \{t1..t8\}, \text{BlackIceDanger}) = -\frac{3}{8} \log_2 \frac{3}{8} - \frac{5}{8} \log_2 \frac{5}{8} = 0.954.$$

This indicates that the concept Sunny differs less over time than the concept BlackIceDanger.

Information gain is formally defined as the expected reduction in entropy after the truth value of a concept is known.

	Sunny	Rainy	$\leq_0(\text{GroundTemp})$	BlackIceDanger
t1	f	t	f	f
t2	f	t	t	t
t3	f	f	f	f
t4	f	t	t	t
t5	t	f	f	f
t6	f	f	t	f
t7	f	t	t	t
t8	f	t	f	f

Fig. 2. The ABox of Ag-4 after 8 time instances

Definition 4. *Information Gain*

$$\text{Gain}(KB, \Delta, c', c) = \text{Entropy}(KB, \Delta, c') - \frac{\#\Delta^c}{\#\Delta} \text{Entropy}(KB, \Delta^c, c') - \frac{\#\Delta^{-c}}{\#\Delta} \text{Entropy}(KB, \Delta^{-c}, c')$$

Example 4. Suppose that Ag-4 wishes to know whether BlackIceDanger. The information gain of Sunny can be calculated as follows. $\text{Gain}(KB, \{t1..t8\}, \text{BlackIceDanger}, \text{Sunny}) = \text{Entropy}(KB, \{t1..t8\}, \text{BlackIceDanger}) - \frac{1}{8} \text{Entropy}(KB, \{t5\}, \text{BlackIceDanger}) - \frac{7}{8} \text{Entropy}(KB, \{t1, t2, t3, t4, t6, t7, t8\}, \text{BlackIceDanger}) = 0.954 - \frac{1}{8} \cdot 0 - \frac{7}{8} \cdot 0.985 = 0.092$. In a similar way, it can be calculated that the information gain of Rainy is 0.348, and that the information gain of $\leq_0(\text{GroundTemp})$ is 0.584.

4.1 Query and Notification requests

To know whether a concept in context C_i is true, it is best to query a concept in C_j with the highest information gain. This idea corresponds to ID3, an algorithm for making a decision tree with as few checks as possible [8]. However, contrary to a decision tree, we only use the information gain for efficiency. The final outcome is based on the logical rules, and not on the set of training examples. For example, a query on *Sunny* is regarded as not very efficient, because it has a relatively low information gain. The best concept to query is *Groundtemp*, with the highest information gain. This idea is specified below.

Specification 3 *Query: Quantitative criteria*

Let CQ be the set of concepts that meet the qualitative criteria of querying to know whether $C_i : c$. The best concept to query is concept $d \in CQ$ for which $\text{Gain}(KB, \Delta, c, d)$ is maximal.

We will now describe the quantitative criteria for deciding whether to query or to request for notification. This decision is based on the expected answer. When the entropy among the answers is low, many queries will return the same answer. In this case, it is better to request for notification as this will reduce the information exchange. When the entropy among the answers is high, a request for notification does not substantially reduce the information flow. In this case queries are preferred. This is specified below.

Specification 4 *Query or Notify: Quantitative criteria*

Let c be a concept that matches the qualitative criteria for query and notify. If entropy of c is low and $\#\Delta^{-c} > \#\Delta^c$ then request for notification on c , else query c .

For example, a request for notification on *Sunny* is preferred over a query because *Sunny* has relatively low entropy. For *GroundTemp*, a query would be preferred.

5 Conclusion and Future Research

In this paper, we have presented a decentralized approach for modeling information flow in ambient environments. In particular, we have investigated the use of queries and requests for notifications in multi-context systems. We have identified qualitative criteria, based on backtracking techniques, and quantitative criteria, based on entropy measures, for translating between different contexts. These criteria are useful to minimize the information flow between agents.

We plan to perform simulation experiments to experimentally explore the information flows that occur when every agent uses the proposed communication mechanism. Furthermore, we plan to extend this line of research by modeling more complex information needs which are based on the task models of agents. We believe that the approach presented here provides a solid basis to study the more complex interaction mechanisms that are required to deal with this scenario. Finally, we aim at studying the quality of decisions when the agents have not completely satisfied their information needs. This requires us to extend the model to take the decision making process into account.

References

1. F. Baader and P. Hanschke. A scheme for integrating concrete domains into concept languages. In *Proceedings of the 12th International Joint Conference on Artificial Intelligence, IJCAI-91*, pages 452–457, Sydney (Australia), 1991.
2. Franz Baader, Diego Calvanese, Deborah McGuinness, Daniele Nardi, and Peter Patel-Schneider, editors. *The description logic handbook: Theory, implementation and applications*. Cambridge University Press, 2003.
3. Paolo Bouquet, Fausto Giunchiglia, Frank van Harmelen, Luciano Serafini, and Heiner Stuckenschmidt. C-OWL: Contextualizing ontologies. In *Proceedings of the Second International Semantic Web Conference, LNCS2870*, pages 164–179. Springer Verlag, 2003.
4. Harry Chen, Tim Finin, and Anupam Joshi. An ontology for context-aware pervasive computing environments. *Knowledge Engineering Review*, 18(3):197–207, 2003.
5. A. Dey, D. Salber, and G. Abowd. A conceptual framework and a toolkit for supporting the rapid prototyping of context-aware applications. *Human-Computer Interaction*, 16, 2001.
6. E. Giunchiglia, P. Traverso, and F. Giunchiglia. Multi-context systems as a specification framework for complex reasoning systems. *Formal Specification of Complex Reasoning Systems*, pages 45–72, 1993.

7. Samuel R. Madden, Michael J. Franklin, Joseph M. Hellerstein, and Wei Hong. Tinydb: an acquisitional query processing system for sensor networks. *ACM Trans. Database Syst.*, 30(1):122–173, 2005.
8. Tom M. Mitchell. *Machine Learning*. McGraw-Hill, 1997.
9. Anand Ranganathan and Roy H. Campbell. An infrastructure for context-awareness based on first order logic. *Personal Ubiquitous Computing*, 7(6):353–364, 2003.
10. Bill Schilit and M. Theimer. Disseminating active map information to mobile hosts. *IEEE Network*, 8(5):22–32, 1994.
11. Mark Stefik. *Introduction to knowledge systems*. Morgan Kaufmann Publishers, 1995.
12. J. van Diggelen, R.J. Beun, Frank Dignum, R.M. van Eijk, and J.-J.Ch. Meyer. ANEMONE: An effective minimal ontology negotiation environment. In Peter Stone and Gerhard Weiss, editors, *Proceedings of AAMAS'06*, pages 899–906. ACM, 2006.

Secure Profiles as a Cornerstone in Emerging Ambient Intelligence Scenarios*

Antonio Muñoz, Daniel Serrano, and Antonio Maña

Computer Science Department. University of Malaga.
{amunoz,serrano,amg}@lcc.uma.es

Abstract. Due to the nature of ubiquitous environments there is a strong relation between them and auto-configurable systems. In ubiquitous computing environments, devices interact with the context performing an auto-configuration of system settings. The main idea presented in this paper is the use of profiles as an important key to provide auto-configurability for mobile environments, especially in ubiquitous environments and Ambient Intelligence scenarios. This work is mainly focused on security settings. We define a profile as a repository of structured data representing present and past states of an entity. Ubiquitous entities use profiles to convey their properties to other entities. Our vision of a profile does not include its use by the application as information storage for internal use. Finally, we propose the use of smartcards as a mean to provide security for ubiquitous services. Smartcards can store user information, invoke services and process temporary service results. For these reasons, and as aforementioned, we consider smartcards as a suitable vehicle to provide ubiquitous services. Users on ubiquitous scenarios should be able to access services from any place using their smartcards. By this way it is possible not require complex computing mobile devices, like PDAs.

1 Introduction

Personalization and ubiquity are key properties for on-line services, but the development of these systems presents new challenges because of the complexity of the required architectures. Specifically, the current infrastructures for the development of personalized, ubiquitous services are not flexible enough to accommodate the configuration requirements of the various application domains. These restrictions come, in part, because current architectures have been designed for less dynamic applications, where configuration is static. Current applications need highly configurable infrastructures, this is the reason why auto-configurable systems are becoming more important, and the increasing number of these implanted systems proves that assertion. A strong relation exists between auto-configurable systems and ubiquitous environments due to underlying nature of these environments, in which a device interacts with the context performing an

* Work partially supported by E.U. through projects SERENITY (IST-027587) and GREDIA (IST-034363) and by Junta de Castilla la Mancha through MISTICO-MECHANICS project (PBC06-0082)

auto-configuration of system settings. Most of ambient intelligence scenarios can be proposed to show this fact. A typical ambient intelligence scenario, where a user travels from a source point A to a destination point B, while he is using different Internet connections depending on the wireless net available at every moment. In this situation the user device will auto-configure depending on the available connection, note that not all wireless nets may have the same access configuration. One of the key aspects of ubiquity is that all auto-configuration operations are performed without user interaction, and moreover, for the user there is a unique and continuous connection. We propose the use of profiles as solution for these kinds of scenarios.

The main idea presented in this paper is the use of profiles as an important key to provide auto configurability for mobile environments and especially in ubiquitous environments. This work is mainly focused on security settings; however this is applicable to any kind of automatic setting configuration, such as desktop look-and-fell settings, peripheral device configuration settings, etc. We define a profile as a repository of structured data representing present and past states of an entity. Profiles are normally used to convey the properties of an entity to other entities, not being intended as information storage for internal use by the entity itself. In this paper, firstly, we propose the use of smartcards as a mean to provide ubiquitous services. Smartcards have been traditionally used to authenticate users. However, current smartcards can perform more functions than those traditional ones. Though limited in speed and space, chips contain microprocessors, ROM and memory, and run their own COS (Chip Operating System) over which various applications may be executed. Hence, with this computing power, it is possible using Smartcards as mobile access points to services. Moreover, Smartcards can store user information, invoke services and process temporary service results. For these reasons, and as aforementioned, we consider Smartcards as a suitable vehicle to provide ubiquitous services. Users on ubiquitous scenarios should be able to access services from any place using their Smartcards, this way make possible not require complex computing mobile devices, like PDAs. Secondly we look at using Trusted Computing Module as a mean to provide a secure environment for agent execution in ubiquitous scenarios. Next sections detail how this task is performed, and why it is essential to provide a trusted environment for agents. We highlight the intrinsic auto-configurability characteristic of multiagent systems and we exploit it together with profiles. With these ideas in mind, we have structured the paper as follows. After of this introduction, section 2 overviews some related works. Section 3 shows a scenario that helps to overview the use of profiles from user point of view. Section 4, sketches how mobile agents are very suitable to provide an auto-configurable system, specially combined with profiles. Section 5 presents the necessity of secure profiling. This is based on the two scenarios; these scenarios are introduced in section 3 and section 4. Finally, section 6 presents conclusions and proposes some ongoing work.

2 Background and Related Work

Business-to-Customer services as well as other types of applications, i.e information systems have the increasing necessity of both ubiquity and auto-configuration properties. In literature we have some examples such as [1] [2] [3] [4]. It is not a secret that the development of a ubiquitous, personalized and customized system is complex, especially due to the adaptation to the end-user device, what requires the integration of very different methodologies addressing the assessment of the user's preferences and the generation of a customized user interface. Some authors describe profiling as 'the process of inferring a set of characteristics (typically behavioural) about an individual person or collective entity and then treating that person or entity (or other persons or entities) in the light of these characteristics' [5]. Based on this definition Pearson describes a method for user self-profiling engaged in e-commerce by which customers can have greater control over their related profiles and this is achieved using trusted agents [6]. However, for the profile concept that we propose is totally different, since we understand a profile as a repository of structured data, giving a representation of current and past status about an entity. Following this approach, the real value of profiles depends on the accuracy of the information they provided. Every profile (and its components) must be uniquely identifiable and its structure is not static because it evolves as the profile entity interacts with other entities in the system. This approach is the most appropriate one to solve problems that emerge when profiles are used to perform auto configuration of security settings in information systems. These problems arise when we have to manage these profiles; that is, for this type of storage object we need to deal with properties as mobility, security and availability. In a previous work [7], we discussed about secure profiling storage, describing a profile classification and scrutinizing the security level of each of them.

In this work, our aim is to focus on the provision of auto configuration, what includes personalization and customization procedures. Regarding the processing and description of profiles, we found several possibilities. RDF [8] provides a way to define a generic data model so facilitating a multi purpose mechanism to describe resources. Another approach, CC/PP [9] consists of a framework for the management of information about devices capabilities and user preferences. This framework, based on the RDF approach, is very useful to perform content customization. UAProf [10] provides a solution to define specific vocabulary concerning device information. Also, FIPA [11] defines device ontologies for the communication of devices. Other works, like [12], focus more specifically on profiles, helping in the description of issues that arise when multiple user profiles are merged. In this sense, the work [13] discusses about management of profiles using Smartcards in such a way that users are provided with a consistent and continuous preferred environment anywhere and anytime.

There are other more practical solutions, like [14], that handle the information coming from the user actions while he is browsing the Internet. The information obtained is used to construct a transient navigation profile which might be useful to help the user in the future. As final example of profiles pro-

cessing usability and management, we can find a very interesting approach [15] where Bayesian networks are used as a tool for creating profiles of visitors in a museum in order to customize the information they receive during their tours. Multiagent paradigm can help in order to provide systems auto configurability. Agent concept is code together with an execution state, which can be executed on agent servers (agencies) [16]. Multiagent systems are now being considered a promising architectural approach for building Internet-based applications, ubiquitous applications and especially those oriented to auto-configuration tasks. A collaborative agent must be able to handle situations in which security conflicts arise and must be capable of negotiating with other agents in order to reach an agreement. Security plays an important role in the development of multiagent systems and is considered to be one of the main issues which should be dealt with in order for agent technology to be widely used outside the research community. Several mechanisms for secure agent execution have been proposed in existing literature, but none of them presents a complete solution. Focusing on security, convenience and practical applicability, more extensive reviews of the state of the art in software protection can be found in [17] [18].

As the introduction mentions, one of our proposal is based on a Trusted Computing Module (TPM) [19]. TPMs appear as part of Trusted Platform architectures. Basically Trusted Platform technology provides evidence about the integrity of a platform to both platform owner and third parties. A Public Key Infrastructure (PKI) is needed to take full advantage of Trusted Platform properties, but certain properties (such as platform data protection) are available without it. A Trusted Platform also provides a mechanism to associate one platform to multiple identities. This feature is particularly in order to create ambient intelligence and ubiquitous environments.

3 Secure User Profiles in An Ambient Intelligence Scenario

A ubiquitous environment literally means an environment in which computing is in everywhere. This section begins with the description of a scenario. This scenario is about nowadays users' interactions and how a token could be used in this scenario in order to store profiles.

Our user usually wakes up early in the morning to go to his job, while he is walking towards the closest train subway station, he powers on his PDA. His device starts the user session through B3G technology. At the starting of the session some user information is requested, these data are located in a profile. The profile includes sensible user information, such as user name, date of birth and even bank account number. However, non-critical information is stored as preferences and desktop configuration parameters. The first steps of the session start include the load of the profile, in order to perform two main tasks, firstly starting session and later on an auto-configuration procedure.

Fifteen minutes later, the user is in the subway where B3G coverage is very poor. But there is a wireless network available inside of the wagon. User PDA

has not wireless technology, but the user has his tablet-PC equipped with wifi connection. The user wants to keep on his session started, so he moves his profile token from his PDA to the tablet-PC, by doing this the same session is running. During his travel by train he had time to arrange his agenda and he was able to read his personalized news, thanks to the ubiquitous environment he was saving time. After thirty minutes by train, the user arrives to the offices, and he uses the internal LAN to connect to the Internet, the same sessions is still alive. After eight hours, our man finishes his working day and he comes back at home. While he is watching the TV he decides to check his tasks for the following day, so he uses his token on home desktop computer, and once again his session is working. Due to the change of device that user does, in each step, an auto configuration process is carried out by using profiling techniques. Additionally, different kind of networks are involved in this scenario, as some of them should be unsecured, our profiles must be securely managed. In order to clarify using profiles to perform an auto configuration of security settings, we present the concept of network profile. A network profile contains information regarding the physical characteristics of the networking technology used (e.g., wifi, 3G), the features of this network (e.g., cost, mobility, management), and the current status of the network (e.g., number of hosts, bandwidth). Each network has an associated network profile, which covers both the physical link (wireless or wired) between the provider and the customer, and how to use the network. In resume, profiles must be stored

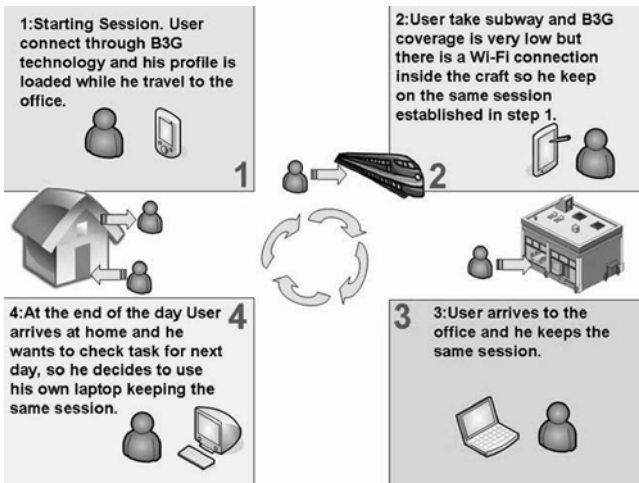


Fig. 1. Example of Ambient Intelligence scenario

securely. In order to clarify why, we provide the following example. During his session, the user reviews his bank account through the Bank web site. Third parties could try to steal critical information related to his account. This fact represents an important drawback, and is the most important reason for secure

profiling. Additionally, it is important to highlight how profile information is used to perform system auto-configuration tasks, and how the configuration should be applied for preferences and for security configuration (firewalls, key management, access control, etc.).

4 Auto Configurable Multiagent System

The new mobile agent paradigm uses networks to carry objects (data and procedures) that can be executed special hosts called agencies. This section introduces a scenario where a client orchestrates the work of a server by sending to the server an agent whose procedure makes all of the required requests when it is executed. For instance, deleting the old files requires moving just one agent between computers. All of the orchestration, including the analysis of which files are old enough to be deleted, is done 'on-site' at the server. One of the main advantages of mobile agents is performance, while two computers in connected require ongoing communication for ongoing interactions, two computers in a mobile agent network can interact without communication, once the agent has reached the server. Another important advantage of mobile agents is automation. A user can use an agent to carry out a long and complex sequence of tasks and then send the agent to the server. This model is improve by fact that an agent can travel to many servers performing several tasks in each of them. The user need be connected to the network only long enough to send the agent and maybe for a later return of it. Mobile agent networks enable users to automate tasks that today they must perform interactively such auto configuration tasks.

Several approaches in this direction exist in literature. One of the most relevant is Seta2000 [20], that consists on an infrastructure for the development of recommender systems that support personalized interactions with their users, providing access from different types of devices (e.g., desktop computers and mobile phones). The Seta2000 infrastructure is based on a multiagent architecture, this infrastructure has been proved by developing two prototypes: SeTA is an adaptive Web store personalizing the recommendation and presentation of products in the Web. In [21] authors defend the idea that networks can be made more flexible and useful embedding code mobility deep into their infrastructures. A proof is that active networking researching are building systems consisting of highly configurable routers and smart packets. In [22] a toolkit to carry out Agent-based telematic services and telecom applications is described. This fact demonstrates auto configurability appeal behind multiagent systems.

With this scenario we propose taking advantage of multiagent systems properties to perform auto configuration tasks. But as in the previous scenario security is critical in profile managing, so mobile agents must be executed securely. In that case, we introduce agent profiles. We propose to use profiles in order to provide a secure execution environment for agents, focused on defending mobile agents against agencies, as well as against another agents running. Agent profiles will help in the security auto configuration tasks that agents do in agencies. Additionally these profiles have some desirable side effects, for instance they offer

the possibility of providing a monitor interface. Using agent profiles agents can be described by meaning of a software profile, in which all needed requirements to execute a concrete agent are stored. But there is more information that is needed to execute securely an agent, because is important to take into account contextual information. With this in mind we define a new concept composing all this data, its the agent profile: Agent profile consists on a composition of software profile and context information in order to gather all needed information to secure execution of an agent.

5 Towards Secure Profiles

This section starts proposing a solution for secure section 3 and 4 scenarios. First scenario could make use of a smartcard as a way to provide a secure execution environment. The user wants to take advantage of a ubiquitous environment, for this purpose we need a trusted computing and tamperproof resistant device, and an important feature is that should be portable. A Smartcard provides the ability to perform cryptographic tasks. In second scenario, as secure device we propose a TPM which provides a secure execution environment for agents, focusing on providing this secured environment agencies have to be trusted by agents executed and for this purpose we need some security characteristics such as a method to perform a remote attestation process, additionally to cryptographic primitives and a trusted root of execution. Because of these requirements we propose to use TPM for this task. This scenario needs a trusted computing and tamperproof resistant device too.

5.1 Secure Profiles Scenario

As aforementioned, in a previous work [7] we presented the reasons why Smartcards are one of the most suitable devices (and probably the most) to store profiles in these scenarios. This statement is based on their security properties and their mobility features. However, even most advanced smartcards have several technical restrictions. Main ones are due to the small amount of free memory available. Anyhow, Smartcards present important features, such as the fact that the data they contain can be protected against unauthorized access and tampering. Access to data can only be performed supervised by the operating system and the secure logic system, confidential data written onto the card is protected from unauthorized external access.

Because it is hard to get the data from a smartcard without authorization, and because it fits well in a pocket, a smartcard is uniquely appropriate for secure and convenient data storage. Without permission of the card holder, data can not be captured or modified, so can further enhance the data privacy of a user: in our particular case, profile information. As aforementioned, the space restriction is an important drawback because profiling techniques loose part of its potentiality. This problem is increased if we store profiles using XML format, as most of actual approaches propose. In general, we can apply two solutions:

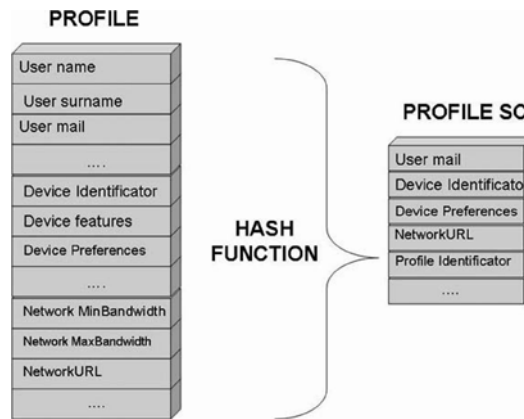


Fig. 2. Hashing profiles in a smartcard

(i) to reduce the size of profiles by storing inside only the most critical fields or, alternatively (ii) to apply any technology leaning to reduce the profile size, such as VCard or ASN.1 [23] formats. One additional problem arises because of the small amount of memory available. Additionally, some free memory is necessary to store applets (at least one) inside the Smartcard in order to run a secure procedure based on split code execution between two different processors. A part will run in the device processor and the other part inside the smartcard. By this way we provide a more secure design, considering a smartcard as a trustworthy device capable to implement a secure software execution scheme [24]. Another alternative to avoid the memory space restrictions consists of splitting profile information in two sets of fields. One set of fields that are more used (or more relevant) will be stored inside the Smartcard, called the Smartcard profile. The rest of fields will be stored in a remote database, and is called the database profile. A hash value of all fields of the profile is added to the smartcard profile in order to preserve a link between profiles, as shown in figure 2. It is important to mention that, for this purpose, we use two pair of cryptographic keys. A secure protocol is used to retrieve the fields stored in the remote database. This task will be performed using a public key cryptosystem fixed by the Smartcard Provider. The protocol that we propose is composed of different phases. In the following, each step of the protocol is explained with more detail.

1. Request of the profile identifier. This step is performed by the device application after a previous testing process that checks which are the profile fields needed. The profile identifier is a hash value calculated using any hash algorithm. For simplicity, we assume that MD5 [25] is the hash algorithm used,.

Table 1. Protocol used to retrieve profiles from remote databases.

1. T -> S: Request IdM5
2. S -> T: Epub PDB (IdMD5, IdSC)
3. T -> PD: Epub PDB(IdMD5,IdSC)
4. PD : IdMD5, IdSC, PD ?T: E Kpub SC(Profile)
5. T -> S: E Kpub SC(Profile)
6. S: Profile checking process
7. S -> T: Profile field1, Profile field2,

2. Sending Profile Identifier. This operation is performed by the smartcard applet. This applet is a JavaCard applet. The profile identifier will be sent encrypted using the Profile Database public key additionally to the smartcard Identifier.
3. The device application is a java applet which is running in the user's computer. This application sends a request of profile information to the Profile Database. The request is done by mean of the profile identifier, which is encrypted in such a way that only the Profile Database manager will be able to get it in clear-text.
4. The Profile Database application processes the request. This application will send the full profile. The profile is encrypted by using Smartcard public key so that only the Smartcard owner is able to decrypt its content. This means that several steps are carried out. Firstly, decryption of the identifier request is done, in order to get IdMD5 and IdSC in clear-text. Next, the profile is encrypted with the public key of the Smartcard, and is subsequently sent to the device application.
5. The device application sends a request for confirmation of profile to the Smartcard application. This task can only be performed by the smartcard because no other one has the private key to decrypt the profile. Thus, the encrypted text EKpubSC(Profile) is sent from the device to the Smartcard.
6. Inside the Smartcard, the JavaCard applet will perform a validation and decryption process of the profile information.
7. The last step consists of performing the authorisation and sending the profile data fields in clear-text that the device application requested for its use. Thus, profile-field1, profile-field2 ... are sent from the Smartcard to the device.

5.2 Secure Profiles to Achieve a Secure Agent Environment

Agents are autonomous, that is they act on behalf of the user on the contrary to conventional programs which depend on user interaction to be executed. Agents contain some level of intelligence, from fixed rules to learning engines that allow them to adapt to changes in the environment, and agents have some extra

information related with their execution state. This data should be considered critical and must be securely managed.

Additionally, it is important to take into account several aspects such as agents do not only act reactively, but also proactively (agents have social ability). All these characteristics have an important impact on the possible security solutions. Some partial approaches have been presented in literature.

Concerning the problem known as malicious host problem [26], which consists of mobile agents that must protect themselves against hosts trying to tamper maliciously with either the code or the data carried by incoming agents, the solution is presented in terms of sanctuaries. A sanctuary consists on a site where a mobile agent can be executed and for this purpose a secure infrastructure for mobile agents and to exam main limits of such infrastructure are built. This kind of protection is focused on protect these programs against a possible malicious server without taking into account the opposite case, mobile agent containing some pieces of malicious code. Additionally, we found some alternatives such as Proof-Carrying Code (PCC) which enables a computer system to determine that an agent, by an automatic way and with certainty, provided by another system is safe to install and execute. But this type of alternatives has several drawbacks. The most important is that generally we have no protection against a malicious server which may change agent code. We propose to use profiles to carry out the agent identification and authorization processes. For this purpose we mix two different kinds of information on the profiles. We have software profiles, in order to keep some minimum conditions that a software component must fulfil in a concrete context, and then we have a context profile. In order to check that this profile fulfils its specification a secure and trusted component is needed. It is proved that a full secure solution only can be achieved by a two co-processors. This is one of the reasons to use a TPM, additionally and as previously was mentioned, the TPM is a tamper-resistant cryptographic device. A TPM can be viewed as a normal open computer platform that has been modified to maintain privacy by providing a set of basic functionalities. This ensures that the data will be released only on that platform and in circumstances determined by the user.

Protection profiles deal with many aspects of security properties, such as audit, cryptographic support, communications, component extensibility, data protection, protection, privacy, secure management, trusted path and channels, etc. TCG introduces two Protection Profiles. One describes the TPM; the other describes the attachment of the TPM to the platform and the properties of the platform that are necessarily to properly support the TPM. We propose two different Agent Profiles. One describes agent software properties and the other describes contextual properties to perform its execution procedure. Attestation is the process of vouching for the accuracy of information. Attestation can be understood along several dimensions, attestation by the TPM, attestation to the platform, attestation of the platform and authentication of the platform. Concretely in our scenario we use attestation to the platform as an operation that provides proof that a platform can be trusted to report integrity measurements;

performed using the set or subset of the credentials associated with the platform. In this scenario we propose to perform this attestation between two different TPM each one installed into a host where each agency runs. For this task we have to take into account that both platforms are physically separated, for this reason we need one of main important characteristics provided by Trusted Computing Module, it is the remote attestation feature.

Attestation enables an agent in a host to authenticate itself to remote agents and hosts. Attestation authenticates who built the platform hardware and the software started at each layer of agent software stack, starting from the firmware.

More potential point of this scheme is based on its underlying simplicity, because the protocol used is very short and fast. Additionally this scheme allows a further scalability because when agent will finish its execution in destination agency and this will travel to a new agency, destination agency will become the new source agency and the new destination agency will play the role of destination agency in presented scheme.

6 Conclusions and Ongoing Work

The growing use of smartcards is reflected in current European population. The massive use of smartcards as of cellular phones clearly shows this fact. At the same time, it seems very clear that user profiles will be demanded by more and more future applications and services. At this moment, Smartcards are the most suitable devices to store profiles for users. Although Smartcards have several limitations such as memory restrictions, these restrictions are being tackled by technological progress according to the Moore's law. In the meanwhile, some solutions are needed. In this paper we have presented several solutions to avoid these storage limitations.

As an open issue in this field, we believe that a more detailed classification of different security levels is needed. This is an on-going work where we are identifying more levels than the three proposed in this paper. A comparative analysis of different types of Smartcards in the market should be performed to evaluate time, available memory, price, etc.

Another issue is the use of the Trusted Computing Platform in order to provide different security levels, that is, to take into account different security levels in execution. As well as we are currently working on the improvement of security in multiagent systems by means of using Trusted Platform Modules (TPMs) [27], smartcards and a combination of them.

References

1. Resnick, P. and Varian, H., Eds. 1997. Commun. ACM: Special Issue on Recommender Systems 46.
2. Riecken, D., Ed. 2000. Commun. ACM: Special Issue on Personalization 43.
3. Maybury, M., Ed. 2000. Commun. ACM: Special Issue on News on Demand 43.

4. Maybury, M. and Brusilovsky, P., Eds. 2002. *Commun. ACM: The Adaptive Web* 45.
5. Bygrave, L. 'Electronic Agents and Privacy: A Cyberspace Odyssey 2001', *International Journal of Law and Information Technology*, vol 9, no 3, p 280, Oxford University Press, 2001.
6. Pearson, S. 'Trusted Agents that Enhance User Privacy by Self-Profiling'. AAMAS Workshop, 'Special track on privacy' Bologna, Italy, 15th July 2002.
7. A. Muoz, J. A. Onieva, J. Lopez, 'On Secure Profiling', 1st International Workshop on Secure Ubiquitous Networks (SUN'05), pp.214-218 (within DEXA'03 Workshops), IEEE Press, August 2005
8. W3C, 'Resource Description Framework (RDF): Concepts and Abstract Syntax', www.w3.org. February 2004..
9. W3C, 'CC/PP: Structure and Vocabularies 1.0' www.w3.org, January 2004. <http://www.ubiq.com/hypertext/weiser/SciAmDraft3.html>
10. Wireless Application Protocol Forum, 'Wireless Application Group User Agent Profile Specification', Nov. 1999
11. Foundation for Intelligent Physical Agents, 'FIPA Device Ontology Specification', www.fipa.org, December 2002.
12. B.Dalem, M.Rauterber, 'Multiple User Profile Merging (MUPE): key challenges for environment awareness', EUSA 2004, LNCS 3295, pp 196-206, 2004.
13. W. Mueller, J.Wang, 'Javacard-enabled Smart Cards for Collaborative Engineering Environments', *Proceedings of E-College workshop on challenges in Collaborative Engineering (CCE 2003)*, Poznan, Poland, April (2003), pp 76-83.
14. E.H. Chi, 'Transient User Profiling', *Proceeding of the workshop on User Profiling*, Vienna, Austria 2004
15. F. Sparacino, 'Sto(ry)chastics: a Bayesian Network Architecture for User Modelling and Computational Storytelling for Interactive Spaces', *proceedings of Ubicomp, the fifth international conference on ubiquitous computing 2003*, Seattle, WA, USA.
16. Berkovits S, Guttman J, Swarup V. 'Authentication for Mobile Agents'. In *Mobile Agents and Security* volume 1419, pages 114-136. Springer-Verlag 1998.
17. Maa, A. *Proteccion de Software Basada en Tarjetas Inteligentes*. PhD Thesis. University of Mlaga. 2003.
18. Hachez, G. *A Comparative Study of Software Protection Tools Suited for E-Commerce with Contributions to Software Watermarking and Smart Cards*. PhD Thesis. Universite Catholique de Louvain. 2003. http://www.dice.ucl.ac.be/hachezthesis_gael_hachez.pdf
19. Pearson, S. 'Trusted Computing Platforms: TCPA Technology in Context'. Published by Prentice-Hall PTR, Hewlett-Packard Company, 2003.
20. Liliana Ardissono, Anna Goy, Giovanna Petrone, Marino Signan. *A multi-agent infrastructure or developing personalized web-based systems*. February 2005, *ACM Transactions on Internet Technology (TOIT)*, Volume 5 Issue 1.
21. Kwindla Hultman Kramer, Nelson Minar, Pattie Maes, 'Special features: Tutorial: mobile software agents for dynamic routing April 1999 *ACM SIGMOBILE Mobile Computing and Communications Review*, Volume 3 Issue 2
22. Stefan Fricke, Karsten Bsufka, Jan Keiser, Torge Schmidt, Ralf Sessler, Sahin Albayrak. *Agent-based telematic services and telecom applications*, April 2001. *Communications of the ACM*, Volume 44 Issue 4.
23. B. Kaliski. 'A Laymans Guide to a Subset to ASN1, BER and DER', June 1991.
24. A. Maa, J. Lpez, J. Ortega, E. Pimentel, J.M. Troya, 'A Framework for Secure Execution of Software'. *International Journal of Information Security*, Volume 2, Issue 4, pp.99-112, Springer, November 2004.

25. R. Rivest, 'The MD5 Message-Digest Algorithm', Request for Comments 1321, April 1992
26. Chess David M. Security issues in mobile code systems. In *Mobile Agents and Security*, volume 1419, pages 1-14. Springer Verlag, 1998.
27. Antonio Maa, Antonio Muñoz, Daniel Serrano. Towards Secure Agent Computing for Ubiquitous Computing and Ambient Intelligence'. The 4th International Conference on Ubiquitous Intelligence and Computing (UIC'07), Hong Kong, China, July 11-13, 2007. (To appear)

Designing for People in Ambient Intelligence Environments

Norbert Streitz

Fraunhofer IPSI, Darmstadt, Germany
streitz@ipsi.fraunhofer.de

Abstract. In this keynote paper, I present selected visions of ambient intelligence and the disappearing computer and comment on the resulting challenges for designing interaction in future smart environments. Our approach starts out with putting the human at the centre of our design considerations and is based on exploiting the affordances of real objects by augmenting their physical properties with the potential of computer-based support. Combining the best of both worlds requires an integration of real and virtual worlds resulting in hybrid worlds. In this approach, the computer "disappears" and is almost "invisible" but its functionality is ubiquitously available and provides new forms of interacting with information. This approach can be summarized by the notion that "the world around us is the interface to information" and is the basis for ambient computing environments. The general comments are illustrated with an example taken from work in the EU-funded "Disappearing Computer" initiative, especially on ambient displays and mobile devices in the "Ambient Agoras" project.

1 Introduction

"It seems like a paradox but it will soon become reality: The rate at which computers disappear will be matched by the rate at which information technology will increasingly permeate our environment and our lives". This statement by Streitz & Nixon (2005) illustrates how computers are increasingly becoming an important part of our day-to-day activities and will determine a wide range of physical and social contexts of our future life. The availability and ubiquity of computers is the first step we are currently witnessing. It is to be followed by the integration of information, communication and sensing technology into everyday objects resulting in "smart artefacts" and making the computer disappear at the same time.

There are a number of related visions known as Ubiquitous/ Pervasive/ Proactive/ Ambient Computing, the Disappearing Computer, Calm Technology, Ambient Intelligence, Smart Objects, Smart Environments, etc. All of them share some basic assumptions and predictions about how these future environments are supposed to be constituted, make themselves available for interaction and "behave" in an intelligent and smart way.

1.1 The Disappearing Computer

The notion of the 'disappearing computer' is an implication of Weiser's (1991) statement 'The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it.' Weiser argues for the development of a 'calm technology' by moving technology into the background while the functionality is available in a ubiquitous fashion. In this approach, the computer "disappears" and is almost "invisible" but its functionality is ubiquitously available and provides new forms of interacting with information. We took this as a starting point for our approach and argue in the following way (see also Streitz, 2001; Streitz et al., 2001).

Computers became primary objects of our attention resulting also in a research area called 'human-computer interaction.' Today, however, we must ask: Are we actually interested in interacting with computers? Isn't our real goal rather to interact with information, to communicate and to collaborate with people? Shouldn't the computer move into the background and disappear?

This "disappearance" can take different forms and we distinguish between: physical and mental disappearance (Streitz, 2001). Physical disappearance refers to the miniaturization of devices and their integration in everyday artefacts as, for example, clothes. In the case of mental disappearance, the artefacts can still be large but they are not perceived as computers because people discern them as, e.g., interactive walls or interactive tables. This leads us to the core issue and questions: How can we design human-information interaction and support human-human communication and cooperation by exploiting the affordances of existing objects in our environment? And, in doing so, how do we exploit the potential of computer-based support augmenting these activities?

1.2 Ambient Intelligence

Ambient Intelligence (AmI) represents a vision of the (not too far) future where "intelligent" or "smart" environments react in an attentive, adaptive, and active (sometimes even proactive) way to the presence and activities of humans and objects in order to provide intelligent/smart services to the inhabitants of these environments. The underlying approach is based on the integration of sensing capabilities, processing power, reasoning mechanisms, networking facilities, applications and services, digital content, and actuating capabilities to be distributed in the surrounding environment. While there are a number of different technologies involved, the goal of ambient intelligence and smart environments is also to hide their presence from the users by having the computer "disappear" from the users' perception and providing them with implicit, unobtrusive interaction paradigms. People and their social situation ranging from individuals to groups, be them work groups, families or friends and their corresponding environments (office buildings, homes, public spaces, etc) are in the centre of the design considerations.

The focus of this presentation is on the resulting challenges for designing interaction in future smart environments. Our approach is based on exploiting

the affordances of real objects by augmenting their physical properties with the potential of computer-based enrichment. Combining the best of both worlds requires an integration of real and virtual worlds resulting in hybrid worlds (Streitz et al., 1998).

2 Smart Environments

The availability of information technology for multiple activities is one important step but it is not sufficient for achieving the objectives indicated above. It is to be followed by the integration of information, communication and sensing technology into everyday objects of our environment in order to create what is called “Smart Environments”. Their constituents are smart artefacts that result from augmenting the standard functionality of artefacts thus enabling new quality of interaction and “behaviour”(of artefacts). Without entering into the philosophical discussion of when it is justified to call an artefact ‘smart’ or what we consider “smart” or “intelligent” behaviour in general, the following distinction turns out to be useful (Streitz et al., 2005):

2.1 System-Oriented, Importunate Smartness

An environment is “smart” if it enables certain self-directed (re)actions of individual artefacts (or by the environment in case of an ensemble of artefacts) based on previously and continuously collected information. For example, a space or a place can be “smart” by having and exploiting knowledge about which people and artefacts are currently situated within its area, who and what was there before, when and how long, and what kind of activities took place. In this version of “smartness”, the space would be active, (in many cases even proactive) and in control of the situation by making decisions on what to do next and actually take action and execute them automatically (without a human in the loop). For example, in a smart home, we have access control to the house and other functions like heating, closing windows and blinds are being done automatically. Some of these actions could be importunate. Take the almost classic example of a smart refrigerator in a home analyzing consumption patterns of the inhabitants and autonomously ordering depleting food. While we might appreciate that the fridge makes suggestions on recipes that are based on the food currently available (that would be still on the supportive side), we might get very upset in case it is autonomously ordering food that we will not consume for reasons beyond its knowledge, such as a sudden vacation, sickness, or a temporal change in taste.

2.2 People-Oriented, Empowering Smartness

The above view can be contrasted by another perspective where the empowering function is in the foreground and which can be summarized as “smart spaces make people smarter”. This is achieved by keeping “the human in the loop” thus empowering people to make informed decisions and take actions as mature and

responsible people who are in control. In this case, the environment will also collect data about what is going on and aggregates the data but provides and communicates the resulting information - hopefully in an intuitive way so that ordinary people can comprehend it easily - for guidance and subsequent actions determined by the people. In this case, a smart space might also make suggestions based on the information collected but the people are still in the loop and in control of what to do next. Here, the place supports smart, intelligent behaviour of the people present (or in remote interaction scenarios people being away “on the road” but connected to the space). This view can be summarized as ‘smart spaces make people smarter’.

Of course, these two points of view will often not exist in their pure distinct forms. They rather represent the end points of a dimension where we can position weighted combinations of both somewhere in between. What kind of combination will be realized is different for different cases and depends very much on the application domain. It is also obvious that in some cases it might be useful that a system is not asking for user’s feedback and confirmation for every single step in an action chain because this would result in an information overload. The challenge is to find the right balance. The position we like to propagate here is that the overall design rationale should be guided and informed by the objective of having the human in the loop and in control as much as possible and feasible.

2.3 Interaction Design

Having different kinds of technology available is one aspect of developing smart environments. Designing the interaction with the different smart artefacts constituting these environments is another challenge. As one might expect, there are dependencies between both design and development strands of having the computer “disappear” and making the artefacts “smart”.

As computers disappear from the scene, become invisible, and disappear from the perception of the users (Streitz, 2001; Russel et al., 2005), a new set of issues is created concerning the interaction with computers embedded in everyday objects resulting in smart artefacts: How can people interact with invisible devices? How can we design implicit interaction for sensor-based interfaces and at the same time provide for a migration path from explicit to implicit interfaces? How can we design for transparency and coherent experiences? One way of tackling these problems is described in the following examples. Our approach is mainly characterized by returning to the real world as the starting point for design and trying to exploit the affordances that real-world objects provide.

3 The Disappearing Computer Initiative

“The Disappearing Computer” (DC) was an EU-funded proactive research initiative of the Future and Emerging Technologies (FET) section of the Information Society Technologies (IST) research program. The goal of the DC-initiative was “to explore how everyday life can be supported and enhanced through the use

of collections of interacting smart artefacts”. Together, these artefacts will form new people-friendly environments in which the “computer-as-we-know-it” has no role. There were three main objectives:

- Developing new tools and methods for the embedding of computation in everyday objects in order to create smart artefacts.
- Investigating how new functionality and new use can emerge from collections of interacting artefacts.
- Ensuring that people’s experience of these environments is both coherent and engaging in space and time.

These objectives were addressed via a cluster of 17 related projects under the umbrella theme of the DC-initiative. The cluster was complemented by a variety of support activities provided by the DC-Network and coordinated by the DC Steering Group, an elected representation of all projects. For more details please visit the DC-website [www.disappearing-computer.net].

4 Ambient Agoras

The “Ambient Agoras” project [www.ambient-agoras.org] was one of the projects of the “Disappearing Computer” initiative introduced above. Its overall goal was to augment the architectural envelope in order to create a social architectural space (Streitz et al., 2003; Streitz et al., 2007) supporting collaboration, informal communication, and social awareness. Ambient Agoras aimed at providing situated services, place-relevant information, and feeling of the place (“genius loci”) to users, enabling them to communicate for help, guidance, work, or fun in order to improve collaboration and the quality of life in future office environments. The guiding metaphor for our work was the Greek “agora” (market place). In line with this, we investigated how to turn everyday places into social marketplaces of ideas and information where people can meet and interact. Ambient Agoras addressed the office environment as an integrated organization located in a physical environment and having particular information needs both at the collective level of the organization and at the personal level of the worker. Although the application domain was office work, it became obvious during the project that a number of results can be transferred to similar communication situations in other application domains as well, e.g., public spaces and distributed networked home environments. This is due to the fact that we addressed rather generic issues of informal communication, awareness and social cohesion in distributed groups residing in remote sites.

For the “Ambient Agoras” environment, we coupled several interaction design objectives (disappearance and ubiquity of computing devices) with sensing technologies (active and passive RFID, WLAN-based positioning), smart artefacts (walls, tables, mobile devices, ambient displays) and investigated the functionality of two or more artefacts working together and privacy as a horizontal dimension. In particular, we addressed the following three major issues:

- Support of informal communication in organizations, locally and between remote sites.
- Role and potential of ambient displays in future work environments.
- Combination of more or less static artefacts integrated in the architectural environment with mobile devices carried by people.

4.1 Ambient Displays and Mobile Smart Artefacts

In line with our general approach, we decided that a calm and ambient technology is being used to support the informal social encounters and communication processes within a cooperative corporate building (Streitz et al., 2003). Ambient displays are examples of this approach.

The Hello.Wall is our version of an ambient display that was developed for the Ambient Agoras environment (Streitz et al. 2003; Streitz et al, 2007). It is a large (1.8 m wide and 2 m high) compound artefact with integrated light cells and sensing technology. Communication of information is facilitated via dynamically changing light patterns. The Hello.Wall artefact is controlled by a computer somewhere hidden in the background using a special driver interface. The design of the system is general and allows taking a range of parameters as input and mapping them on a wide range of output patterns.

In our setting, the Hello.Wall provides awareness and notifications to people passing by or watching it. Different light patterns correspond to different types of information, e.g., presence and mood of people. It is interesting to note that the use of abstract patterns allows distinguishing between public and private or personal information. While the meaning of public patterns is known to everybody and can therefore easily be interpreted, the meaning of personal patterns is only accessible to those who are initiated. Another interesting observation is that it not only communicates information but at the same time its appearance has also an effect on the atmosphere of a place and thus influences the mood of the social body around it.

The Hello.Wall is complemented by a mechanism where it can “borrow” the display of other artefacts, in order to communicate additional information. This enables users to access information complementing the Hello.Wall. We call the corresponding mobile devices “ViewPorts”. The ViewPort is a WLAN-equipped PDA-like handheld device based on commercially available components but integrated in and mapped to a new form factor. In addition, we integrated RFID readers and transponders. Thus, the ViewPort can sense other artefacts and can be sensed itself.

4.2 Connecting Remote Teams

One major application for the Ambient Agoras environment was the “Connecting-Remote-Teams” scenario (Röcker et al., 2004; Streitz et al, 2007). It addressed the issue of extending awareness information and facilitating informal communication from within a corporate building to the connection of distributed teams working at remote sites. Besides opportunistic chance encounters in the hallway,

people sojourning in lounge areas having a coffee or tea are especially accessible for informal communication. While people's availability and current mood for a conversation are easily detectable in a face-to-face situation, it is very difficult to identify opportunities for similar encounters in a remote-sites setting.

We evaluated the this scenario in a Living Lab experiment with our project partners using two sites, one at Electricité de France (EDF) in France (Paris) and one at Fraunhofer in Germany (Darmstadt). For more details of the setting and an extended description of the notion of affordances for smart artefacts see Streitz et al (2007).

5 Conclusions

The work reported demonstrates our approach on the role of information and communication technology in future smart environments for which the notion of the "disappearing computer" is of central importance. While in our previous work - not reported here - of developing the Roomware components (Streitz et al 1998, 2001), the focus was on supporting especially the productivity-related processes of team work and group meetings, the Ambient Agoras environment focussed on informal communication and social awareness. We combined two corresponding design goals: First, to develop a smart environment that supports selected social processes as, e.g., awareness, informal communication, and coordination of team work in local and distributed collaboration settings. Second, the implementation corresponds to and is compatible with the nature and characteristics of the processes addressed by following the objectives of developing a calm technology. Computers move into the background and are not considered or perceived anymore to be computers or computer-related devices. This is achieved by designing smart artefacts that exploit the affordances of everyday artefacts (Streitz et al. 2007).

6 Acknowledgements

The work reported in this article was supported by the European Commission as part of the "Disappearing Computer" initiative ("Ambient Agoras" project, contract IST-2000-25134). Thanks are due to our partners in different projects as well as to the members and students of the Fraunhofer IPSI research division AMBIENTE [www.ipsi.fraunhofer.de/ambiente] for their substantial contributions in realizing the different components and environments.

References

1. Röcker, C., Prante, T., Streitz, N., van Alphen, D. (2004). Using Ambient Displays and Smart Artefacts to Support Community Interaction in Distributed Teams. Proceedings of OZCHI-2004 Conference (Nov. 2004, University of Wollongong, Australia.)

2. Russell, D., Streitz, N., Winograd, T. (2005). Building Disappearing Computers. *Communications of the ACM*, Vol. 48 (3), March 2005. pp. 42-48.
3. Streitz, N. (2001). Augmented Reality and the Disappearing Computer. In: Smith, M., Salvendy, G., Harris, D., Koubek, R. (Eds.), *Cognitive Engineering, Intelligent Agents and Virtual Reality*. Lawrence Erlbaum, 2001. pp. 738-742.
4. Streitz, N., Geißler, J., Holmer, T. (1998). Roomware for Cooperative Buildings: Integrated Design of Architectural Spaces and Information Spaces. In: Streitz, N. Konomi, S., Burkhardt, H. (Eds.): *Cooperative Buildings - Integrating Information, Organization, and Architecture*. (CoBuild '98, Darmstadt, Germany) Springer LNCS Vol. 1370, 1998. pp. 4-21.
5. Streitz, N., Kameas, A., Mavrommati, I. (Eds.) (2007). *The Disappearing Computer*. Springer "State-of-the-Art" Survey, LNCS 4500.
6. Streitz, N., Nixon, P. (2005). The Disappearing Computer. *Communications of the ACM*, Special Issue. Vol. 48 (3), March 2005. pp. 33-35.
7. Streitz, N., Prante, T., Rückert, C., van Alphen, D., Magerkurth, C., Stenzel, R., Plewe, D. (2003). Ambient Displays and Mobile Devices for the Creation of Social Architectural Spaces: Supporting Informal Communication and Social Awareness in Organizations. In: O'Hara, K., Perry, M., Churchill, E., Russell, D. (Eds.), *Public and Situated Displays: Social and Interactional Aspects of Shared Display Technologies*. Kluwer, pp. 387-409.
8. Streitz, N., Prante, T., Rückert, C., van Alphen, D., Stenzel, R., Magerkurth, C., Lahlou, S., Nosulenko, V., Jegou, F., Sonder, F., Plewe, D. (2007). Smart Artefacts as Affordances for Awareness in Distributed Teams. In: N. Streitz, A. Kameas, I. Mavrommati (Eds.), *The Disappearing Computer*. Springer LNCS 4500, 2007. pp. 3-29.
9. Streitz, N., Rückert, C., Prante, T., van Alphen, D., Stenzel, R., Magerkurth, C. (2005). Designing Smart Artefacts for Smart Environments. *IEEE Computer*, March 2005. pp. 41-49.
10. Streitz, N., Tandler, P., Müller-Tomfelde, C., Konomi, S. (2001). Roomware: Towards the Next Generation of Human-Computer Interaction based on an Integrated Design of Real and Virtual Worlds. In: J. Carroll (Ed.), *Human-Computer Interaction in the New Millennium*. Addison-Wesley, 2001. pp. 553-57.
11. Weiser, M. (1991). The computer for the 21st Century. *Scientific American*. September 1991, pp. 66-75.

Architecture and Design Patterns for Ambient Intelligence: an Industry Perspective

Antonio Kung

Trialog, 25 rue du Gnral Foy, 75008, Paris, France.

`Antonio.kung@trialog.com`

Abstract. This paper provides an industry view on ambient intelligent systems, in particular on design stumbling blocks that could delay the advent of such systems. We first list a number of important architecture principles for ambient intelligent systems. We show that many of such principles are not well taken into account through a number of pattern examples related to seamless connectivity, trusted computing and application deployment. From an industry standpoint, these examples highlight a mismatch between the envisioned infrastructure and business stakeholders organizations. From an architecture and design pattern standpoint, they illustrate difficulties in creating suitable patterns, either when several patterns must be merged into one, or when an existing pattern must be deconstructed into several patterns. A number of recommendations are finally provided.

1 Introduction

Ubiquitous computing [1] refers to the integration of computers in the environment to serve people in their everyday lives. Ambient Intelligence (AmI) is another term used in [2] to highlight “a vision of people surrounded by intelligent intuitive interfaces that are embedded in all kinds of objects and an environment that is capable of recognizing and responding to the presence of different individuals in an invisible way”. Ambient intelligence systems involve computing elements that are embedded, context-aware, personalized, adaptive, and anticipatory. The expected computing evolution [3], is shown in figure 1. To make it happen, it is widely agreed that a number of key technologies are needed: unobtrusive hardware, seamless communication, dynamic distributed networks, human-centric computer interfaces and dependable trusted systems.

However the deployment of such technologies is made difficult at the industry level by two factors. First, the high fragmentation of embedded systems applications as well as specific needs have led to a flurry of sector specific communication standards (e.g. IEEE 802 covers Wifi, ZigBee [16], and car to car communication). Secondly, the increasing complexity of embedded systems applications have led to equally complex supply chains involving different business stakeholders focusing on different subsystems (e.g. processors, ASIC, operating system, middleware, application component) and different integration levels.

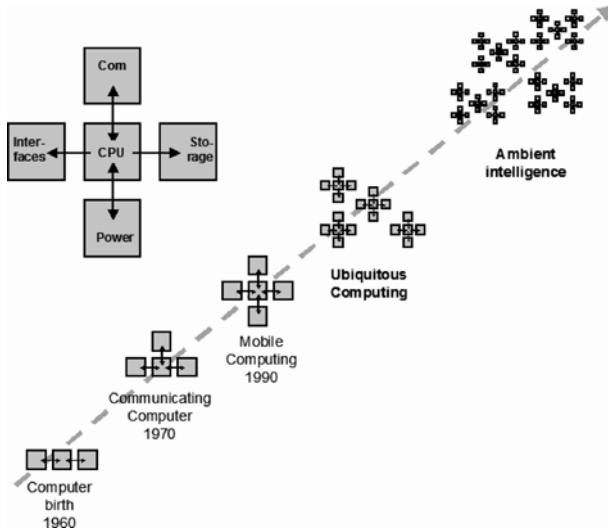


Fig. 1. Computer Evolution towards Ambient Intelligence

This paper takes an architecture and design pattern viewpoint to describe industry oriented issues. It first identifies a number of important architecture principles for ambient intelligent systems. It then describes a number of patterns that will help meet those principles in the area of seamless connectivity, trusted computing, and application deployment. An industry perspective is then taken to show that these patterns are not well supported. Gaps are identified: individual patterns are not widely available, and the combination or deconstruction of patterns is not straightforward. Finally, a number of recommendations are provided. This paper combines the findings of a number of IST projects: TEAHA [17], MonAMI [18], HIJA [11], and Sevecom [19]. The support of the European Commission is acknowledged.

2 Architecture Principles for Ambient Intelligence

There are a number of architecture principles which guide the building of ambient intelligent systems. We list five of them here.

The technology independence principle ensures that application components are independent of the underlying technology components. For instance, a data management component in charge of collecting data related to a given context should be independent of the sensing technology and of the communication technology. The rationale is to allow the deployment of application components on top of the wide variety of underlying technologies that can be available.

The stakeholder asset protection principle ensures that computing assets owned and manipulated on behalf of a stakeholder are properly isolated and protected. For instance, diagnosis data collected by a household appliance manager must not be accessible by other applications. Similarly, patient monitoring data collected by a health application must also be protected. Two types of stakeholders could be involved at the same horizontal level when multiple applications run in parallel (e.g. to serve different persons in the same environment) or at a vertical level when a single application involves different stakeholders (e.g. a payment company and services providers). The rationale is that stakeholders expect to get the same level of protection whether their applications run isolated or in parallel to other applications.

The computing resource guarantee principle ensures that resources such as CPU time, memory space, storage space, and computer battery are properly allocated and guaranteed for a given application. The rationale is that applications expect to enjoy the same level of quality of service whether they run isolated or in parallel to other applications.

The stakeholder separation of concern principle ensures that a system is structured into subsystems which can be assigned to clearly identified stakeholders. For instance device drivers and applications are subsystems which are typically developed by different stakeholders (e.g. peripheral manufacturers versus application developers). Separation of concern can take place at different levels, at the application level (e.g. when some open interfaces are desirable), or at a computing level (e.g. when functional and non functional aspects must be separated). The rationale for separation of concern is to create system structures that ease the creation of new applications because many other subsystems can be reused.

Finally, the identity protection principle ensures that stakeholders identities are properly secured and protected against privacy issues. For instance, identities used in payments applications should be authenticated, or application and system data should not be exploited by third parties to identify and track a given person. The rationale for identity protection is to ensure the right level of trust and data protection.

The next sections will elaborate on the consequences of the listed architecture principles in terms of design patterns.

3 Patterns for Ambient Intelligent Systems

Patterns [4] are widely used today to specify architecture and design aspects. They refer to templates describing a solution to solve a commonly occurring problem. Patterns are a convenient way to describe the features which are needed to meet the above principles. The following sections list a number of patterns that could be used in ambient intelligent systems. All the patterns are in general well known so the purpose of this section is to relate them to the building of ambient systems from an industry perspective.

3.1 Seamless Connectivity

Seamless connectivity enables communications between systems independently of the underlying communication technology. It is therefore the feature which is initially desired to meet the technology independence principle. We now describe six patterns, Service discovery, Proxy-based communication, Secure communication, Policy-based communication, Stakeholder ontology administration and Pseudonym-based communication which were contributed by the IST projects TEAHA [8], [9] (the first five patterns) and SeVeCom [12], [13] (the last pattern).

Service discovery is a protocol pattern which enables the dynamic discovery of available services in an environment (e.g. a PDA discovers a printer). Comparisons of existing service discovery protocols show that they are very similar [5]. Two approaches are used. The first is registry based, i.e. a server is used to store information on services available. The second is peer-to-peer based, i.e. peers searching for a service directly interact with peers providing a service.

Proxy-based communication is a pattern which enables communication between heterogeneous systems (e.g. a ZigBee device communicates with an UPnP [21] digital TV). Assuming that A and B use communication technologies X and Y respectively, communication between A and B is achieved by introducing a proxy element. The proxy supports both X and Y communication protocols. It interacts with A and B on behalf of the other party by mapping X protocol to Y and vice versa. This pattern often involves an additional element which can be conveniently located in a gateway (e.g. an OSGi gateway [20]).

Secure communication is a protocol pattern which enables trusted communication between peers (e.g. privacy protection should take place when a remote e-health application in a hospital monitors and collects data from patients staying at home). In this pattern A and B exchange credentials to authenticate each other and agree on session keys. The key agreement procedure is based on the Diffie-Hellman protocol [6], [7]. This pattern is often called the ping-pong pattern because two messages are sufficient to implement the protocol.

Policy-based communication ensures that only authorized communication can take place between two devices (e.g. safety regulations do not allow remote systems to switch on an oven). This pattern actually extends the proxy-based pattern. The proxy not only ensures communication between peers using different communication technologies, it also enforces communication policies, i.e. it guarantees that only authorized peers can interact.

Stakeholder ontology administration ensures that information needed to define and standardize applications communication payloads is properly updated and configured according to stakeholders requirements. We use the term ontology to refer to the set of concepts which are needed for systems to exchange information, i.e. to achieve semantic interoperability. For instance, "start washing machine" involves two concepts, "start" and "washing machine". The need for updating and configuring ontology data arises when systems evolve at different paces or when specific variations are needed. For instance, industry stakeholders for household appliances in Europe have started an initiative for the definition of the first generation of communicating household appliances [25]. They have

to cope with two market issues, first the specifics of multi-brand markets (e.g. the ontology used for a given type of brand could be richer), and secondly the support of generations of devices (e.g. a refrigerator can be used during decades. During this time span several generations of ontologies might have been defined). The pattern is integrated in the system which manages the interface between software applications and the underlying communication technology. It involves a stakeholder separation capability (e.g. ontologies from different industry sectors are handled separately), and two administration features, an ontology discovery and selection capability (e.g. when a new household appliance of brand A is installed, the most suitable ontology will be searched for) and an ontology repository management system. In TEAHA an implementation was made using an OSGi framework. Separation was achieved by having separate Java bundles called business cluster plug-ins. Administration was achieved by representing ontologies as bundles and by using OSGi bundle administration capability with discovery based on the OSGi network bundle search capability.

Pseudonym-based communication ensures that the identities of stakeholders involved in an application payload are not revealed to unknown external observers (e.g. it should not be possible to figure out which patient is being monitored in an e-health application). This pattern involves two features, a pseudonym management system, and a control capability of the underlying communication technology identities (e.g. changing a pseudonym must also involve changing underlying physical communication addresses).

Proxy-based communication contributes to technology independence. Secure communication, policy-based communication, and pseudonym-based communication contribute to the stakeholder asset protection architecture principle. All the listed patterns contribute to stakeholder separation of concern. Finally, the pseudonym-based communication contributes to identity protection. From an industry perspective, we believe that the collective effect of combining such patterns is what it will take to produce ambient systems with genuine seamless inter-working capabilities.

3.2 Trusted Computing

Trusted computing enables individual applications to benefit from asset protection capabilities (e.g. confidential application data is not accessible by everyone). From a system point of view, it allows multiple independent applications to run on the same platform. It is therefore the feature which is initially needed to meet the stakeholder asset protection principle. We now describe two patterns for trusted computing, security module support, and computing resource QoS. These patterns were contributed by the IST projects TEAHA and HIJA [11], [10] respectively.

Security module support ensures that sensitive assets (e.g. data, secret keys, credentials) are manipulated in a computing platform by an isolated subsystem with tamper resistance or tamper detection capability. TPM [23] or smart cards are well-known implementations of this pattern.

Computing resource Quality of Service (QoS) ensures that individual applications running on a platform are allocated and guaranteed computing resources (e.g. CPU time, memory resource, battery power, communication bandwidth). From a security point of view, it ensures that denial of service events cannot occur (e.g. an individual application using too much CPU prevents another application from running). From a dependability point of view it ensures that the right level of QoS is provided by the execution platform. This pattern involves two features: an application admission system and application resource allocation system. The admission system checks whether a new application can run in terms of resource. The resource allocation system assigns resources to applications. It could be through static schemes (e.g. partitioning) or through dynamic schemes (e.g. scheduling).

Security module support contributes to the technology independence, stakeholder separation of concern and stakeholder asset protection principles. Computing resource QoS contributes to the computing resource protection principle. From an industry perspective, the combination of both patterns is important to achieve trusted computing for ambient systems.

3.3 Application Deployment

Application deployment enables the execution of individual applications in new environments. It provides the dynamic capabilities needed by ambient systems applications. An underlying infrastructure with suitable technology for dynamic operation of software components is required, thus implying architecture and design patterns which meet the stakeholder separation of concern principle. We describe two patterns for application deployment: platform independence support, and service delivery. Note that the stakeholder ontology administration pattern described in the seamless connectivity section could have also been included in this section, as ontology information is application specific.

Platform independence support is a well known pattern that allows for software subsystems to run anywhere independently of the underlying executing platform. The most popular approaches are Java and C#. This pattern involves an agreement on an platform independent representation (e.g. byte code for Java, Common Intermediate Language for C#), and a virtual machine with downloading capabilities (e.g. JVM for Java and CLI for C#).

Service delivery enables services or applications to be dynamically provided. This pattern is supported by OSGi [20] in a configuration where application components called bundles can be downloaded and executed on a gateway system (e.g. in a home or in a car). The OSGi pattern involves features for managing the installation and operations of such components. It relies on the use of a specific middleware framework which runs on top of an underlying virtual machine. A more holistic and visionary pattern is defined in TAHI [24]. This pattern models a service according to the service supply chain. Four blocks of stakeholders are defined: (1) the content management block which involves the content creator, content provider and content aggregator stakeholders, (2) the service management block which involves the service creator, the service operator, and the ser-

vice aggregator stakeholders, (3) the network management block which involves the network operator and the service provider stakeholders, and finally (4) the premises infrastructure block which involves the surveyor, installer, system manager, maintenance, subscriber and beneficiary stakeholders. Each stakeholder in the supply chain in a service implementation is "represented" by a layer made up of two types of entities, the Remote Service Objects (RSO) and the Pervasive Service Agents (PSA). RSOs represent the capabilities of each layer. PSAs represent the requirements needed by the overall service. They include dynamic entities in charge of checking RSOs status and negotiating capability.

Platform independence support contributes to the technology independence principle. Service delivery contributes to the stakeholder separation of concern principles.

4 Gaps

All the patterns described in the previous section are useful if not critical to ambient systems. We wish now to provide an industry viewpoint on why the integration of these patterns is not straightforward, in other words why there are gaps between the ambient intelligence vision and existing technologies. There are currently no available overall architecture and design patterns that would describe the architecture of ambient systems at a sufficiently detailed and complete level because today's systems are much more specialized and involve many different value chains (i.e. many stakeholders). This was not the case for past computing systems. Even though they were not specified with patterns, it is straightforward to identify commonly used patterns¹. For instance, mainframes in the sixties and seventies, or mini computers in the eighties were all based on the time sharing and virtual memory operating system pattern. This pattern ensures that CPU and memory resource are properly allocated using time sharing and paging protocols. It also protected memory through page access rights. The entire pattern assumed features that were available at the hardware and operating system levels so that it could meet both the computing resource guarantee and the stakeholder asset protection principles (stakeholders being application users).

We now describe gaps which illustrates the difficulties in integrating patterns and technologies, or in deconstructing patterns and technologies.

4.1 Combining Patterns and Technologies

Many combinations of patterns will prove difficult to implement. The examples below show that a pattern can be too specialized and not well understood for straightforward integration, or that a pattern need agreements between stakeholders which are not easy to achieve.

¹ From a high level standpoint, one can also argue that Figure 1 describes five architecture patterns

The combination of proxy-based communication with service discovery implies proxies that must be able to map different service discovery protocols (e.g. the UPnP service discovery or the EHS [22] service discovery), or to map communication networks which are statically organized. Combining the same pattern with secure communication implies proxies that must be able to map different security mechanisms. These combinations are challenging because they involve industry stakeholders with different cultures/needs or expertise (e.g. those using static network technologies versus those using dynamic network technologies, or security expertise and protocol expertise).

The combination of service discovery with secure communication implies that the service discovery protocol also involves credential exchange. Combining it with policy-based communication implies a service discovery protocol which supports policy configuration exchange. To our knowledge no mainstream technologies and implementations today support these combinations well. Our interpretation is that this would require expertise on both protocol and security technologies.

The combination of computing resource QoS with security module support requires agreement and convergence between dependability and security specialists in the industry. This is not currently the case in the industry even though the convergence need is well identified [1], [15]. The combination of computing resource QoS with platform independence requires an agreement between virtual machine developers and platform developers. The conventional view is that virtual machines provide their own resource management, using services of the underlying platform resource management system. But the portability requirement of virtual machines is a conflicting business priority. It has leads to implementations that do not use potential platform resource management capability (e.g. virtual machines will not take advantage of some OS resource partitioning capability). [10] describes a similar type of problem involving conflicts between OSGi framework developers and Java virtual machine developers. Again for business portability reasons, OSGi framework implementations will be based on mainstream virtual machines which do not support resource management for independent applications. This is inconsistent with the OSGi framework objective to run multiple applications.

The implementation of the pseudonym-based communication pattern could also be difficult if not impossible. This is because an integration with all underlying communication technologies is needed. The pseudonym change process must be able to control and modify the underlying communication technologies identities. Therefore an agreement with communication technology developers, and possibly a modification of the underlying communication technology standard are needed

4.2 Deconstructing Patterns and Technologies

The deconstruction of patterns and technologies is also difficult. By deconstruction we mean the dismantling into smaller building blocks. Issues are not entirely technical. The examples below show that an understanding of supply chains and

of their evolution (i.e. how much should we deconstruct) is needed. They also show that agreements between industry stakeholders with possibly conflicting interests are needed.

Service delivery implies a service supply ecosystem which must match the categories of industry stakeholders that will contribute to the delivery of services. This means that interfaces must be made available between stakeholders (e.g. between a service operator and a network operator). TAHI with some contribution from TEAHA defined up to 14 categories of stakeholders. MonAMI [18] is investigating a deconstruction process that would allow cost effective development of e-inclusion services (e.g. service for elderly and handicapped people) out of existing mainstream services. For instance a multimedia chat service could be deconstructed in such a way that by replacing some part of its implementation, we could come up with a chat service that can be used by handicapped people). The issue is therefore not only to identify how to deconstruct but also to convince stakeholders to agree on resulting specific interfaces.

Pseudonym-based communication, already presented as a combination issue, can also be viewed as a deconstruction issue. If the developer of the pseudonym system and the developer of the communication protocol are different, then there is a deconstruction issue. First, there must be an agreement on a suitable interface for identity management so that the pseudonym manager can make request involving dynamic modification of underlying protocol identifiers (e.g. a MAC address). Secondly, developers of communication technologies must deconstruct their implementation accordingly in order to make this interface available.

Likewise, the combination of computing resource QoS with platform independence can also be presented as a deconstruction issue. The underlying platform implementation should be deconstructed in such a way that an interface with an underlying resource management subsystem is available.

4.3 Secure Service Discovery as an Example of Combination

Combining patterns often does not raise really difficult technical challenges. On the other hand, it involves multi-disciplinary work that is not easily available in industry organizations. This section describes how service discovery was combined with secure communication in the TEAHA project. This work required specialized expertise on service discovery protocols and on security protocols. In the rest of the section we use the following notation to denote a message sent by A to B with payload X and Y:

$$\{A- > B, X, Y\} \quad (1)$$

Secure communication allows for the establishment of a secure communication session. It involves two messages between A and B (a ping-pong exchange) before a secure payload can be exchanged. A->B, credential, key info, B->A, creden-

tial,key info, A->B or B->A, secure payload

$$\begin{aligned} & \{A- > B, credential, keyinfo\}, \\ & \{B- > A, credential, keyinfo\}, \\ & \{A- > B \text{ or } B- > A, securepayload\} \end{aligned} \quad (2)$$

Service discovery can be combined with the above pattern as follows. In the case of peer-to-peer discovery, we have two possibilities, (1) a client C searches for a service and then a server S accepts the request, and (2) S advertises its service and then C subscribes to the service.

$$\{C, search\}, \{S- > C, accept\}, \{C- > S \text{ or } S- > C, payload\} \quad (3)$$

$$\{S, advertise\}, \{C- > S, subscribe\}, \{C- > S \text{ or } S- > C, payload\} \quad (4)$$

The integration of secure communication is achieved by combining the search or advertisement exchange with the ping-pong exchange.

$$\begin{aligned} & \{C, servicesearch, credential, keyinfo\}, \\ & \{S- > C, accept, credential, keyinfo\}, \\ & \{C- > S \text{ or } S- > C, securepayload\} \end{aligned} \quad (5)$$

$$\begin{aligned} & \{S, advertise/credential, keyinfo\}, \\ & \{C- > S, subscribe, credential, keyinfo\}, \\ & \{C- > S \text{ or } S- > C, securepayload\} \end{aligned} \quad (6)$$

The case of registry discovery involves two phases, registry discovery (i.e. a client C discovers a registry server R) and then service discovery (i.e. a client C establishes communication with a server S). Registry discovery also involves either a search exchange or an advertisement exchange.

$$\begin{aligned} & \{C, registrysearch\}, \{R- > C, ack\}, \\ & \{C- > R, servicesearch\}, \{R- > C, S\}, \\ & \{C- > S, subscribe\}, \{S- > C, ack\} \\ & \{C- > S \text{ or } S- > C, payload\} \end{aligned} \quad (7)$$

$$\begin{aligned} & \{R, advertise\}, \{C- > R, subscribe\}, \\ & \{C- > R, servicesearch\}, \{R- > C, S\}, \\ & \{C- > S, subscribe\}, \{S- > C, ack\} \\ & \{C- > S \text{ or } S- > C, payload\} \end{aligned} \quad (8)$$

The integration of secure communication is achieved by combining the ping-pong exchange twice, the first time to establish secure communication with the registry and the second time to establish secure communication with the server.

$$\begin{aligned}
 & \{C, registrysearch, credential, keyinfo\}, \\
 & \{R \rightarrow C, ack, credential, keyinfo\}, \\
 \{C \rightarrow R, secureservicesearch\}, \{R \rightarrow C, secureS\}, \\
 & \{C \rightarrow S, subscribe, credential, keyinfo\}, \\
 & \{S \rightarrow C, ack, credential, keyinfo\} \\
 & \{C \rightarrow S \text{ or } S \rightarrow C, securepayload\}
 \end{aligned} \tag{9}$$

$$\begin{aligned}
 & \{R, advertise, credential, keyinfo\}, \\
 & \{C \rightarrow R, subscribe, credential, keyinfo\}, \\
 \{C \rightarrow R, secureservicesearch\}, \{R \rightarrow C, secureS\}, \\
 & \{C \rightarrow S, subscribe, credential, keyinfo\}, \\
 & \{S \rightarrow C, ack, credential, keyinfo\} \\
 & \{C \rightarrow S \text{ or } S \rightarrow C, securepayload\}
 \end{aligned} \tag{10}$$

5 Conclusion

In this paper we elaborated on the gap between the ambient intelligent system vision and business stakeholders' expectations. By taking a stakeholder viewpoint, we were able to identify some key architecture principles that are either neglected, or not well taken into account, such as the stakeholder asset protection principle. We also listed a number of architecture and design patterns that meet the architecture principles. We showed that many of these patterns are not straightforward to implement, to integrate with other patterns or to deconstruct. This is due to a mismatch between pattern implementations and stakeholder business interests and responsibilities. In particular, patterns can involve expertise and know-how from several categories of stakeholders (e.g. security technology vs. communication technology developers) which are difficult to combine. Furthermore, some patterns owned by a category of stakeholders need to be deconstructed so that other stakeholders can integrate their own pattern (e.g. platform developers need to deconstruct their implementation in such a way that computing resource management can be shared).

We have two suggestions to deal with this gap. The first focuses on stakeholder needs. We propose to work on a code of practice that would help systems designers and technology developers anticipate industry needs from the start. The second focuses on the ambient intelligent vision. We call for the creation of specific multi-disciplinary initiative to discuss and prioritize architecture principles and patterns. Ideally, this could be similar to the community work that led

to the OSI standard. The difference is that the participation of many different categories of stakeholders would be needed².

It can be argued that we did not cover other ambient intelligent challenges (e.g. ad-hoc networks) which could lead to disruptive solutions. One could also argue that the growing pervasiveness of computing systems will create the market and shape the industry accordingly. We claim that we need first to define sound architecture principles and patterns, and secondly to understand better the industry value chain operation so that we can make ambient intelligence happen faster.

References

1. Weiser, M.: The Computer for the Twenty-First Century. *Scientific American*, pp. 94-10, September 1991.
2. Information Society Technology Advisory Group (ISTAG) Scenarios for Ambient Intelligence in 2010, <ftp://ftp.cordis.lu/pub/ist/docs/istagscenarios2010.pdf>.
3. Waldner, J-B.: Nano-informatique et intelligence ambiante : inventer l'ordinateur du XXIe siècle. Paris : Herms Science, 2007, ISBN 978-274-621-5160.
4. Gamma, E., Helm, R., Johnson, R., Vlissides, J.: *Design Patterns: Elements of Reusable Object-Oriented Software*. Addison-Wesley, ISBN 0-201-63361-2, 1994.
5. Sundramoorthy, V.: *At Home in Service Discovery*. PhD thesis, University of Twente, ISBN 90-365-2392-3, 2006.
6. Diffie, W., Hellman, M.E.: Multi-user cryptographic techniques. *Proceedings of AFIPS National Computer Conference*, 199-112, 1976.
7. Diffie, W., van Oorschot, P.C., Wiener M.J.: Authentication and authenticated key exchanges. *Designs, Codes and Cryptography*, 2 (1992), 107125.
8. Scholten, J., van Dijk, H.W., De Cock, D., Preneel, B. Kung, A., d'Hooge, M.: *Secure Service Discovery in Home Networks*. 2006 IEEE International Conference on Consumer Electronics, 8-12 Jan 2006, Las Vegas, Nevada, USA. pp. 115-116. IEEE. ISBN 0-7803-9459-3.
9. Van Dijk, H., Scholten, H., Tobalina, A., Garcia, V., Milanini, S., Kung, A.: *Open Home Networks: The TEAHA Approach*. Sixth International Conference on Networking ICN '07, April 2007, IEEE Computer Society.
10. Kung, A., Hunt, J., Gauthier, L., Richard-Foy, M.: *Issues in Building an ANRTS Platform*. Fourth International Workshop on Java Technologies for Real-time and Embedded Systems - JTRES 2006, ACM International Conference Proceeding Series; Vol. 177, pp. 144-151, ISBN:1-59593-544-4.
11. Kung, A., Hansen, S.: *ANRTS Platforms*. Fourth International Workshop on Java Technologies for Real-time and Embedded Systems - JTRES 2006, ACM International Conference Proceeding Series; Vol. 177, pp. 117-124, ISBN:1-59593-544-4.
12. Papadimitratos, P., Buttyan, L., Hubaux, J-P., Kargl, F., Kung, A., Raya, M.: *Architecture for Secure and Private Vehicular Communications*. Seventh International Conference on ITS Telecommunications, June 2007.

² The need for multidisciplinary work also justifies collaborative projects which are set up by the IST European program or national programs. The findings of this paper would not have been possible without such projects

13. Raya, M., Papadimitratos, P., Hubaux, J-P.: Securing Vehicular Communications. IEEE Wireless Communications Magazine, Special Issue on Inter-Vehicular Communications, vol. 13, num. 5 (October 2006), p. 8-15.
14. Stoneburner, G.: Toward a Unified Security/Safety Model. IEEE Computer, vol. 39, num. 8 (August 2006), p.96-97.
15. Avizienis, A., Laprie, J-C., Randell, B., Landwehr, C.: Basic Concepts and Taxonomy of Dependable and Secure Computing, IEEE Transactions on Dependable and Secure Computing, vol. 1, num.1, January-March 2004, p.11-34.
16. www.zigbee.org viewed on July 2007.
17. www.teaha.org viewed on July 2007.
18. www.monami.info viewed on July 2007.
19. www.sevecom.org viewed on July 2007.
20. www.osgi.org viewed on July 2007.
21. www.upnp.org viewed on July 2007.
22. www.ehsa.org and www.konnex.org viewed on July 2007.
23. www.trustedcomputinggroup.org viewed on July 2007.
24. www.theapplicationhome.com viewed on July 2007.
25. www.ceed.eu and www.ceed.eu/IFEDE//easnet.dll/ExecReq/WPShowItem?eas:dat_im=010113 viewed on July 2007.

An Ambient Intelligence Based Multi-Agent Architecture

Dante I. Tapia, Javier Bajo, and Juan M. Sánchez and Juan M. Corchado

Departamento Informática y Automática, Universidad de Salamanca.
Plaza de la Merced s/n, 37008, Salamanca, Spain
{dantetapia, jbajope, elwiwo, corchado}@usal.es

Abstract. This paper presents an Ambient Intelligence based distributed architecture that uses intelligent agents with reasoning and planning mechanisms. The agents have the ability to obtain automatic and real-time information about the context using a set of technologies, such as radio frequency identification, wireless networks and wireless control devices. The architecture presented can be implemented on a wide diversity of dynamic environments to manage tasks and services.

1 Introduction

Agents and multi-agent systems (MAS) have become increasingly relevant for developing distributed and dynamic open systems, as well as the use of context aware technologies that supply those systems information about the environment.

This paper is focused on describing the main characteristics of an Ambient Intelligence based distributed architecture that integrates Case-Based Reasoning (CBR) and Case-Based Planning (CBP) as reasoning mechanisms into deliberative BDI (Believe, Desire, Intention) agents, as a way to implement adaptive systems on dynamic environments.

A CBR-BDI agent [4] uses Case-Based Reasoning as a reasoning mechanism, which allows it to learn from initial knowledge, interact autonomously with the environment, users and other agents, and have a large capacity for adaptation to the needs of its surroundings. CBP-BDI agents are CBR-BDI agents specialized in generating plans. BDI agents can be implemented by using different tools, such as Jadex [14]. Jadex agents deal with the concepts of beliefs, goals and plans, which are java objects that can be created and handled within the agent at execution time.

The architecture presented is founded on Ambient Intelligence (AmI) environments, characterized by their ubiquity, transparency and intelligence. Ambient Intelligence proposes a new way to interact between people and technology. This last one is adapted to individuals and their context, showing a vision where people are surrounded by intelligent interfaces merged in daily life objects [8]. AmI creates computing-capable environments with intelligent communication and processing, serving people by means of a simple, natural, and effortless

human-system interaction [16]. AmI also arouse the development of intelligent and intuitive systems and interfaces, capable to recognize and respond to users' necessities in a ubiquitous way [7], considering people in the centre of the development [17], and creating technologically complex environments in medical, domestic, academic, etc. fields [20]. Agents on this perspective must be able to respond to events, take the initiative according to their goals, communicate with other agents, interact with users, and make use of past experiences to find the best plans to achieve goals.

The agents in this work employ radio frequency identification (RFID), wireless networks, and automation devices to supply automatic and real-time information about the environment, allowing users to interact with their surroundings and controlling physical services (i.e. heating, lights, switches, etc.).

Next, the main characteristics of the architecture are explained, describing the technologies, agents and reasoning and planning mechanisms that integrate it.

2 Technologies for Context Awareness

This architecture is founded on Ambient Intelligence (AmI) to develop multi-agent systems over dynamic scenarios, thus the importance to use technologies that allow the agents to have information about the environment and react upon it. AmI provides an effective way to create self-adaptive systems to context and users necessities. The vision of AmI assumes seamless, unobtrusive, and often invisible but controllable interactions between humans and technology. AmI provides new possibilities for solving a wide scope of problems. It also proposes a new way to interact between people and technology, where this last one is adapted to individuals and their context, showing a vision where people are surrounded by intelligent interfaces merged in daily life objects [8], creating computing-capable environments with intelligent communication and processing, serving people by means of a simple, natural and effortless human-system interaction [16]. With the appearance of AmI-based systems, one of the most benefited segments of population will be the elderly and people with disabilities, improving important aspects of their life, especially health care [8].

Radio Frequency Identification (RFID) is a wireless communication technology used to identify and receive information about humans, animals and objects on the move. An RFID system contains basically four components: tags, readers, antennas and software. Tags with no power system integrated (i.e. batteries) are called passive tags or "transponders", these are much smaller and cheaper than active tags (power system included), but have shorter read range. The transponder is placed on the object itself (i.e. bracelet). As this object moves into the reader's capture area, the reader is activated and begins signalling via electromagnetic waves (radio frequency). The transponder subsequently transmits its unique ID information number to the reader, which transmit it to an end device or central computer where information is processed and delivered. Information is not restricted to the object identification, thus it can include detailed

information concerning the object itself or its location. Mainly used in industrial/manufacturing, transportation and distribution, there are other growing sectors, including health care [18]. Configuration presented in this paper comprise of transponders mounted on bracelets worn on people's wrist or ankle, readers installed over protected zones, with an adjustable capture range up to 2 meters, and a workstation where all the information is processed and stored.

Wireless LAN's (Local Area Network), also known as Wi-Fi (Wireless Fidelity) networks, increase the mobility, flexibility and efficiency of the users, allowing programs, data and resources to be available no matter the physical location [19]. These networks can be used to replace or as an extension of wired LANs. Wi-Fi networks reduce infrastructure and installation costs. Also provide more mobility and flexibility, allowing people to stay connected as they roam among covered areas, increasing resources efficiency [11]. New handheld devices make easy to use new interaction techniques; for instance, guidance or location systems [6, 15]. The architecture presented in this paper incorporates "lightweight" agents that can reside in mobile devices, such as cellular phones, PDA's, etc. [2], and therefore support wireless communication.

Automation devices are successfully applied on schools, hospitals, homes, etc. [13]. There is a broad diversity of automation technologies, one of them is ZigBee, a low cost, low power consumption, two-way, wireless communication standard, developed by the ZigBee Alliance [21]. It is based on IEEE 802.15.4 protocol, and operates at 868/915MHz & 2.4GHz frequency spectrum. ZigBee is designed to be embedded in consumer electronics, home and building automation, industrial controls, PC peripherals, medical sensor applications, toys and games, and is intended for home, building and industrial automation purposes, addressing the needs of monitoring, control and sensory network applications [21]. ZigBee allows star, tree or mesh topologies. As shown on Figure 1, devices can be configured to act as: network coordinator (control all devices); router/repeater (send/receive/resend data to/from coordinator or end devices); or end device (send/receive data to/from coordinator).

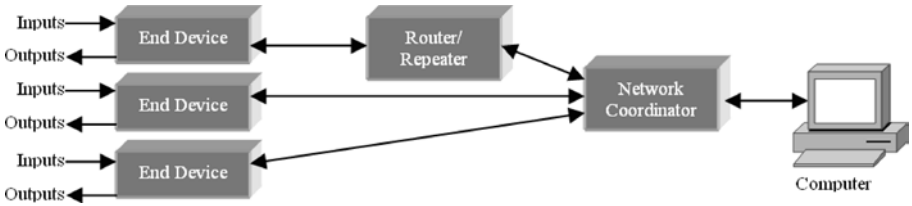


Fig. 1. ZigBee devices' configuration

Information, collected through the set of technologies described before, is processed by deliberative BDI agents with reasoning and planning mechanisms, providing the intelligence and flexibility to develop Ambient Intelligence based

systems with self-adaptive capabilities to changes in the environment and user necessities. Next, the integration of reasoning and planning mechanisms into deliberative BDI agents is described.

3 Agents with Reasoning and Planning Capabilities

Agents in this development are based on the BDI (Belief, Desire, Intention) deliberative architecture model [3], where the agents' internal structure and capabilities are based on mental aptitudes, using beliefs, desires and intentions. Implementation of CBR (Case-Based Reasoning) systems [1] as a deliberative mechanism within deliberative BDI agents, facilitates learning and adaptation, and provides a greater degree of autonomy than pure BDI architecture. CBR use past experiences to solve new problems [12], adapting solutions that have been used to solve similar problems in the past, and learn from each new experience. To merge a CBR motor into a deliberative BDI agent, as seen on Figure 2, it is necessary to represent the cases used in CBR by means of beliefs, desires and intentions, and then implement a CBR cycle to process them, resulting in a deliberative CBR-BDI agent.

The primary notion when working with CBR is the concept of "case", which is described as a past experience composed of three elements: an initial state or problem description that is represented as a belief; a solution, that provides the sequence of actions carried out in order to solve the problem; and a final state, represented as a set of goals. CBR manages cases (past experiences) to solve new problems. The way cases are managed is known as the CBR cycle, and consists of four sequential phases: retrieve, reuse, revise and retain. The retrieve phase starts when a new problem description is received. Similarity algorithms are applied in order to retrieve, from a cases memory, the cases with a problem description more similar to the current one. Once the most similar cases have been retrieved, the reuse phase begins, adapting the past solutions to obtain a best one for the current case. The revise phase consists of an expert revision of the solution proposed. Finally, the retain phase allows the system to learn from the experiences obtained in the three previous phases, updating continuously the cases memory.

On Figure 3, the basic structure of a CBP-BDI agent can be seen. The reasoning mechanism generates plans using past experiences and planning strategies, so the concept of Case-Based Planning (CBP) is obtained [9]. CBP consists of four sequential stages: retrieve stage to recover the most similar past experiences to the current one; reuse stage to combine the retrieved solutions in order to obtain a new optimal solution; revise stage to evaluate the obtained solution; and retain stage to learn from the new experience. CBP is the idea of planning as remembering [10]. CBP is a specialization of CBR which is a problem solving methodology based on using a library of solutions for similar problems [10]. In CBP, the solution proposed to solve a given problem is a plan, taking into account the plans applied to solve similar problems in the past. The problems and their corresponding plans are stored in a plans memory. Problem description (initial

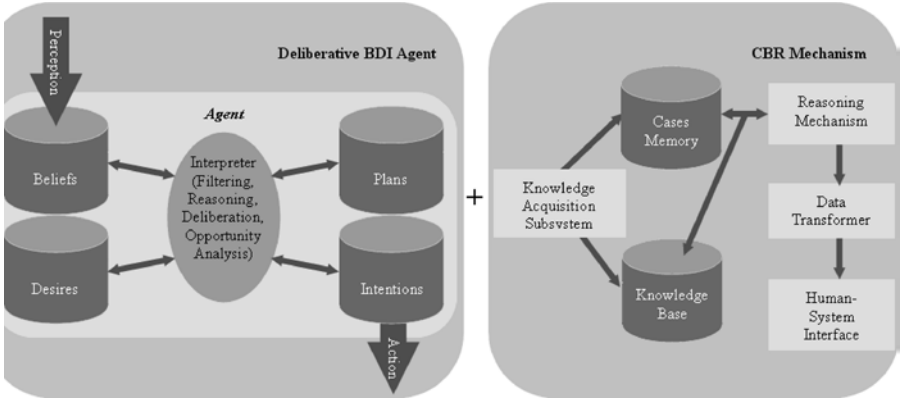


Fig. 2. Basic deliberative BDI agent and CBR mechanisms architectures

state) and solution (situation when final state is achieved) are represented as beliefs, the final state as a goal (or set of goals), and the sequences of actions as plans. The CBP cycle is implemented through goals and plans. When the goal corresponding to one of the stages is triggered, different plans (algorithms) can be executed concurrently to achieve the goal or objective. Each plan can trigger new sub-goals and, consequently, cause the execution of new plans.

Next, an Ambient Intelligence based architecture model is described, with context aware technology and agents with reasoning and planning mechanisms working collectively.

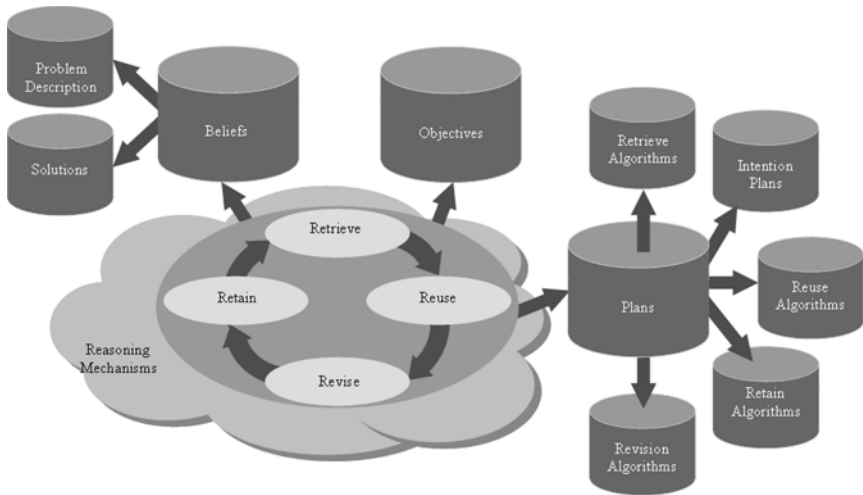


Fig. 3. Deliberative CBP-BDI agent basic structure

4 Architecture Model

Figure 4 illustrate how the reasoning and planning mechanism, and context aware technology are integrated into a generic multi-agent system prototype that can be implemented on diverse dynamic scenarios, for example in geriatric residences [4] with some changes according the users and project necessities.

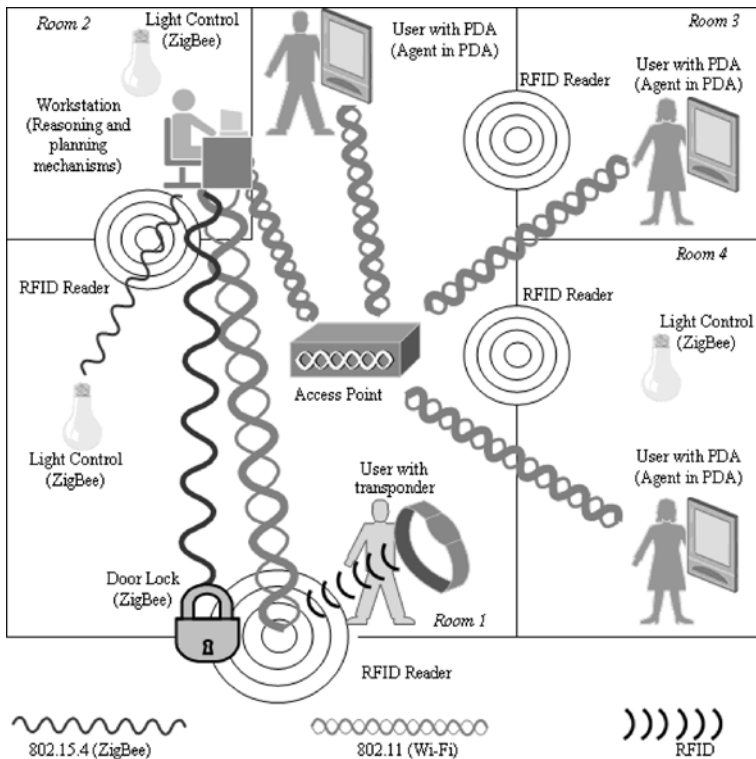


Fig. 4. Architecture applied on an automated environment

Figure 5 shows the technology, the five different deliberative agents in the architecture, and the interaction between all them and users. Each agent has specific roles and capabilities:

- User Agent is a BDI agent that runs on a Workstation. It manages the users' personal data and behaviour (monitoring, location, daily tasks, and anomalies). Beliefs and goals used for each user depend on the plan or plans defined by the super-users. User Agent maintains continuous communication with the rest of the system agents, especially with SuperUser Agent and ScheduleUser Agents, through which the scheduled-users can communicate the result of their assigned tasks. User Agent must ensure that all actions

- indicated by SuperUser Agents are taken out, sending a copy of its base memory (goals and plans) to Manager Agent in order to maintain backups.
- SuperUser Agent is a BDI agent that runs on mobile devices (PDA's). It inserts new tasks into the Manager Agent to be processed by the CBR mechanism. It also communicates with User Agents to impose new tasks and receive periodic reports, and with ScheduleUser Agents to ascertain plans evolution.
 - ScheduleUser Agent is a CBP-BDI planner agent that runs on mobile devices (PDA's). It programmes the scheduled-users daily activities, obtaining dynamic plans depending on tasks needed for each user. It manages scheduled-users profiles (preferences, habits, holidays, etc.), tasks, available time and resources. Each ScheduleUser agent generates personalized plans depending on the scheduled-user profile.
 - Manager Agent is a CBR-BDI Agent that runs on a Workstation. It plays two roles: Security role monitors the users' location and physical building status (temperature, lights, alarms, etc.) through a continuous communication with the Devices Agent; and Manager role which handle databases and tasks assignation. It must provide security for users and ensure tasks assignments efficiency. Tasks assignation is carried out through a CBR mechanism, incorporated within Manager Agent. When a new task assignation needs to be carried out, past experiences, current situation needs and available resources are recalled.
 - Devices Agent is a BDI agent that runs on a Workstation. This agent controls all hardware devices. It monitors users' location (continuously obtaining/updating data from the RFID readers), interact with ZigBee devices to receive information and control physical services (lights, door locks, etc.), and also check the status of the wireless devices connected to the system (PDA's). The information obtained is sent to the Manager Agent to be processed.

The essential hardware used is: Sokymat's Q5 125KHz chip RFID wrist bands and computer interface readers for people monitoring and identification; Silicon Laboratories' C8051 chip-based 2.4GHz development boards for physical services automation (heating, lights, door locks, alarms, etc.); mobile devices (PDA's) for interfaces and users interaction; a Workstation where all the high demanding CPU tasks (planning and reasoning) are processed; and a basic Wi-Fi network for wireless communication between agents (in PDA's and Workstation). All hardware is some way integrated to agents, providing them automatic and real-time information about the environment. The information obtained is processed by the reasoning and planning mechanisms to automate tasks and manage services. The planning mechanism in ScheduleUser Agents is a complex and innovative procedure that is briefly described next.

4.1 Tasks planning

ScheduleUser Agents are autonomous agents that can survive in dynamic environments, with communication capabilities that allow them to be easily inte-

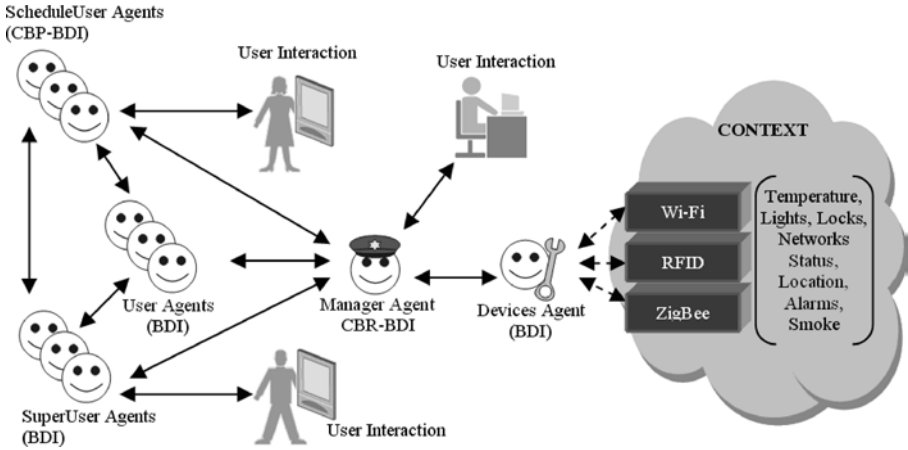


Fig. 5. Architecture applied on an automated environment

grated into a multi-agent system. They can cooperate with other agents to solve problems in execution time and distributed way. The CBP mechanism on each ScheduleUser Agent constructs plans in such a way that a plan is a sequence of tasks that need to be carried out by a user. A task is a java object that contains a set of parameters, as can be seen in Table 1.

Table 1. Tasks description

Task	Data
TaskId	36
TaskType	32
TaskDescript	Description
TaskPriority	3
TaskObjective	0
TaskIncidents	0
UserId	7
UserNecessities	2
MinTime	10 min
MaxTime	60 min
TaskResources	2,4,8

For each task, one or more goals are established, so the whole task is eventually achieved. A problem description is created by the tasks that the scheduled-users must execute, the resources available, and the time assigned. In the retrieve stage, problem descriptions found, within similarity range close to the original problem description, are recovered from the beliefs base. In this case, a toler-

ance of 20% has been permitted. In order to do this, the agent applies different similarity algorithms (cosine, clustering etc.). Once the most similar problem descriptions have been selected, the solutions associated with them are recovered. A solution contains all the plans (sequences of tasks) carried out in order to achieve the objectives of the ScheduleUser Agent for a problem description (assuming that re-planning is possible) in the past, as well as the efficiency of the solution supplied. Solutions are combined in the reuse stage to construct a new plan [4, 9]. The new plan must ensure that the objectives can be accomplished with the resources available in order to carry out the global plan. The user objectives are defined within the planning mechanism. Task resources are defined by an administrator (person) using a Manager Agent GUI. ScheduleUser Agents watch out incidents and interruptions that may occur during re-planning [4]. Furthermore, these agents trust people because revision of plans is made by users. Finally, ScheduleUser agents learn about this new experience. If the plan is at least 90% similar, it is stored in the cases memory.

5 Architecture Model

Deliberative BDI agents with reasoning and planning mechanisms, and the use of technology to perceive the context, create a robust, intelligent and flexible AmI-based architecture that can be implemented in wide variety scenarios, such as hospitals, geriatric residences, schools, homes or any dynamic environment where is a need to manage tasks and automate services.

Although the architecture is currently on development, it is mature enough to demonstrate its capabilities on real scenarios. In fact, a prototype system, based on this architecture, has been successfully applied into a geriatric residence [4], improving security and health care efficiency through monitoring and automating medical staff's work and patients' activities, facilitating the assignation of working shifts and reducing time spent on routine tasks, as seen on Figure 6.

The main characteristic of the architecture presented is the use of CBR and CBP mechanisms merged into deliberative BDI agents that help them to solve problems, adapt to changes in context, and identify new possible solutions, supplying better learning and adaptation than pure BDI model. In addition, RFID, Wi-Fi and ZigBee devices supply the agents with valuable information about the environment, contributing to a ubiquitous, non-invasive, high level interaction among users, system and environment.

However, it is necessary to continue developing and improving the architecture presented, adding new capabilities and integrating more technologies to build more efficient and robust systems to automate services and daily tasks.

Acknowledgments. This work has been partially supported by the MCYT TIC2003-07369-C02-02 and the JCYL-2002-05 project SA104A05. Special thanks to Sokymat by the RFID technology provided and to Telefónica Móviles (Movistar) for the wireless devices donated.

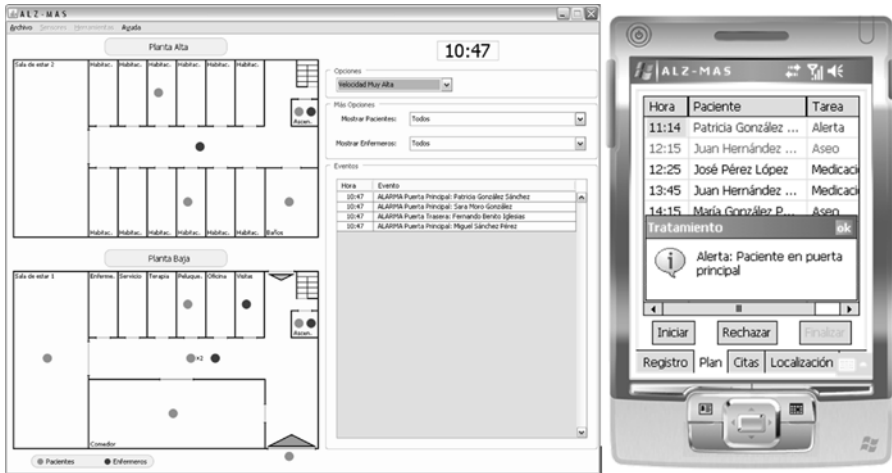


Fig. 6. Architecture applied on an automated environment

References

1. Allen, J.F.: Towards a general theory of action and time. *Artificial Intelligence* Vol. 23 pp. 123-154. (1984)
2. Bohnenberger, T., Jacobs, O., Jameson, A.: DTP meets user requirements: Enhancements and studies of an intelligent shopping guide. *Proceedings of the Third International Conference on Pervasive Computing (PERVASIVE-05)*, Munich, Germany. (2005)
3. Bratman, M.E.: *Intentions, Plans and Practical Reason*. Harvard University Press, Cambridge, M.A. (1987)
4. Corchado, J. M.; Bajo, J.; De Paz, Y.; Tapia, D. I. (2007). *Intelligent Environment for Monitoring Alzheimer Patients, Agent Technology for Health Care*. Decision Support Systems, Elsevier. Amsterdam, Netherlands.
5. Corchado, J.M., Laza, R.: Constructing Deliberative Agents with Case-based Reasoning Technology. *International Journal of Intelligent Systems*. Vol. 18 No.12 1227-1241 (2003)
6. Corchado, J.M., Pavn, J., Corchado, E., Castillo, L.F.: Development of CBR-BDI Agents: A Tourist Guide Application. *7th European Conference on Case-based Reasoning 2004*. LNAI 3155, Springer Verlag. pp. 547-559. (2005)
7. Ducatel, K., Bogdanowicz, M., Scapolo, F., Leijten, J., Burgelman, J.C.: That's what friends are for. *Ambient Intelligence (AmI) and the IS in 2010. Innovations for an e-Society*. Congress Pre-prints, "Innovations for an e-Society. Challenges for Technology Assessment". Berlin, Germany. (2001)
8. Emiliani P.L., Stephanidis, C.: Universal access to ambient intelligence environments: opportunities and challenges for people with disabilities. *IBM Systems Journal*. (2005)
9. Glez-Bedia, M., Corchado, J.M.: A planning strategy based on variational calculus for deliberative agents. *Computing and Information Systems Journal*. Vol.10(1) 2-14. (2002)

10. Hammond, K.: *Case-Base Planning: Viewing Planning as a Memory Task*. Academic Press, New York. (1989)
11. Hewlett-Packard.: *Understanding Wi-Fi*. <http://www.hp.com/rnd/library/pdf/>. (2002)
12. Kolodner J.: *Case-based reasoning*. Morgan Kaufmann (1993).
13. Mainardi, E., Banzi, S., Bonf, M. & Beghelli, S. (2005). A low-cost Home Automation System based on Power-Line Communication Links. 22nd International Symposium on Automation and Robotics in Construction ISARC 2005. September 2005. Ferrara, Italy.
14. Pokahr, A., Braubach L., Lamersdorf, W.: *Jadex: Implementing a BDI-Infrastructure for JADE Agents*, in: EXP - In Search of Innovation (Special Issue on JADE), Vol. 3, 76-85. Telecom Italia Lab, Turin, Italy, September (2003)
15. Poslad, S., Laamanen, H., Malaka, R., Nick, A., Buckle, P., Zipf, A.: *Crumpet: Creation of user- friendly mobile services personalised for tourism*. In Proceedings of 3G. (2001)
16. Richter, K., Hellenschmidt, M.: *Interacting with the Ambience: Multimodal Interaction and Ambient Intelligence*. Position Paper to the W3C Workshop on Multimodal Interaction, 19-20 July. (2004)
17. Schmidt, A.: *Interactive Context-Aware Systems Interacting with Ambient Intelligence*. In G. Riva, F. Vatalaro, F. Davide & M. Alcaiz, *Ambient Intelligence*, IOS Press pp. 159-178. (2005)
18. Sokymat.: *Sokymat*. <http://www.sokymat.com>. (2006)
19. Sun Microsystems. (2000). *Applications for Mobile Information Devices. Helpful Hints for Application Developers and User Interface Designers using the Mobile Information Device Profile*. Sun Microsystems, Inc.
20. Susperregi, L., Maurtua, I., Tubo, C., Prez M.A., Segovia, I., Sierra, B.: *Una arquitectura multiagente para un Laboratorio de Inteligencia Ambiental en Fabricacin. 1er. Taller de Desarrollo de Sistemas Multiagente (DESMA)*. Mlaga, Espaa. (2004)
21. ZigBee Standards Organization.: *ZigBee Specification Document 053474r13*. ZigBee Alliance. (2006)

Management of Large Video Recordings

J.L. Patino, E. Corvee, F. Bremond, and M. Thonnat

INRIA, 2004 route des Lucioles, 06902 Sophia Antipolis (FRANCE)
{jlpatino, Etienne.Corvee, Francois.Bremond,
Monique.Thonnat}@sophia.inria.fr

Abstract. The management and extraction of structured knowledge from large video recordings is at the core of urban/environment planning, resource optimization. We have addressed this issue for the networks of camera deployed in two underground systems in Italy. In this paper we show how meaningful events are detected directly from the streams of video. Later in an off-line analysis we can set this information into an adequate knowledge model representation that will allow us to model behavioral activity and obtain statistics on everyday people activities in metro station. Raw data as well as on-line and off-line metadata are stored in relational databases with spatio-temporal retrieval capabilities and allow the end-user to analyse different video recording periods.

1 Introduction

The management of audio-visual streams acquired for surveillance and safety reasons is an essential point of ambient intelligence applications such as urban/environment planning, resource optimization, disabled/elderly person monitoring. In this work we have addressed the question of management and extraction of structured knowledge from large video recordings recorded over networks of cameras deployed in real sites (European project CARETAKER [1]): two different underground systems, the metro of Torino (GTT) and the metro of Roma (ATAC). Some video interpretation systems have been built in the past with similar applications. PRISMATICA [7] was a video surveillance system tested on-site in Paris and London undergrounds and able to detect overcrowding/congestion; unusual or forbidden directions of motion; intrusion; and stationarity of people. Similarly, ADVISOR [8] was tested in Brussels and Barcelona metro stations and was able to detect fighting between persons, vandalism, person jumping above a barrier, group of people blocking an exit and overcrowding situation. VISOR-BASE [9] was another video interpreting system built to store and interpret video streams from geographically distributed cameras in shopping centers and was aimed at security systems such as cashiers and entrance points monitoring. However, these systems were mainly focused on the real-time recognition of events. Recorded video contains an added value that can only be unlocked by technologies that can effectively exploit the knowledge it contains. The produced audio-visual streams, in addition to surveillance and safety issues, represent a useful source of information if stored and automatically analysed,

in environment planning and resource optimisation for instance. We have thus developed techniques that automatically extract knowledge at two stages. In the first stage, events can be extracted directly from the raw data streams, such as ambient sounds, crowd density estimation, or object trajectories. The second stage of semantic information reflects relationships between tracked objects but also between tracked objects and its environment and is obtained from off-line analysis. While the second layer involves that knowledge that has previously not been modeled but discovered through unsupervised techniques and statistical analysis, the first layer corresponds to that knowledge modelled using ontologies. The ontologies describe the set of all the concepts and relations between concepts shared by the community of a given domain. An ontology is useful for experts of the application domain to use scene understanding systems in an autonomous way, to understand exactly what types of events a particular system can recognise, and for developers desiring to share and reuse activity models dedicated to the recognition of specific events. However, most of the work in ontology is dealing with structure of complex events (linguistic issues not addressing specifically video events) [10]. Several works have also addressed the limitation of standard ontologies to represent time and temporal relationships. For instance, Hobbs [11] has developed a rich ontology dedicated to time reasoning based on Allen temporal algebra [12]. A series of specific workshops sponsored by ARDA have been devoted to building ontologies of video events for video understanding applications [13]. The ontology presented in this work takes into account spatial and temporal constraints for video event recognition and interpretation.

Extracted metadata from both analysis modules, on-line and off-line, will be incorporated in knowledge management systems providing web-base content access and semantic, spatio-temporal, retrieval capabilities. For this purpose we have developed an Agent Software Methodology. The remaining of the paper is structured as follows. In section 2 we present the general architecture of the system. Section 3 introduces the ontology that has been defined for this application. The main concepts and principal results obtained from the on-line analysis are presented in section 4 while those for the off-line analysis are presented in section 5. The conclusions and some perspectives of our work are given in section 6.

2 General Architecture

Figure 1 shows the global architecture mainly composed of two different processing modules, i.e. the real-time on-line analysis subsystem, and the higher-level offline interpretation. For the storage of video streams and the metadata obtained after both, on-line video processing and off-line analysis, three different databases exist: raw database, on-line database, off-line database.

The on-line analysis subsystem takes its input directly from the data acquisition module. Streams of video are acquired at a speed of 25 frames per second. Objects and events of interest, previously defined in the ontology (see next section), are detected on real time and tracking results are written to the on-line

database at a speed of 5 frames per second. Streams of video are directly written to a raw database. The off-line analysis subsystem takes its input principally

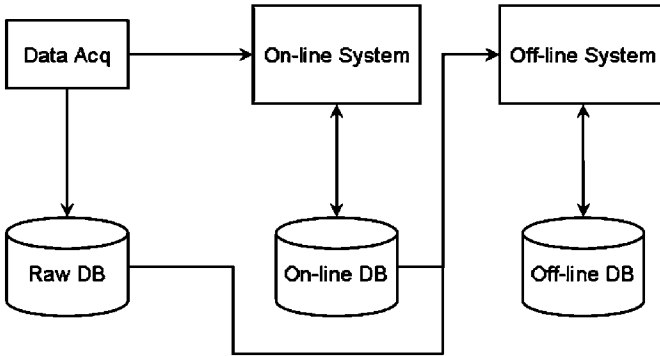


Fig. 1. General architecture

from the on-line database as we are looking to retrieve all stored information related to a period of time that we wish to analyse. This module can also access the raw database in case the user wants to visualize a past event.

In order to allow all modules to communicate between them, we have defined, in agreement with the ontology, an exchange file format based on xml, as it has previously shown that it is an accepted standard that provides a common and understandable representation of the vocabulary, and can help to improve reusability, modularity and interoperability of the applications [2]. Large libraries of xml metadata, linked to the streams of video, are saved in both, on-line and off-line databases. With search tools, it is possible to retrieve a part of a scene, at a certain time, in the whole scene based upon the research criteria given to the search tools. In our case these are based on xml queries. Web-service technology (SOAP, WSDL, UDDI, RSS) is chosen for components and subsystems integration, because it allows reuse of high-performance interoperable components and makes the required distributed processing and communication more straightforward [3].

3 Ontologies

This section presents all the a priori knowledge and structure needed to represent video event knowledge for automatic scene interpretation. Two types of knowledge are modeled. On one side, the multi-user knowledge (safety operators, decision makers), represented by their needs, their use-case scenario definition, and their abilities at providing context description for sensory data. On the other side, the content knowledge is modeled, characterised by a first layer of primitive events that can be extracted from the raw data streams such as objects 3D

dimensions or their trajectories, and a second layer of higher semantic events defined from longer term analysis and from more complex relationships between both primitive events and higher-level events. Both knowledge types are modeled through ontologies.

There are two main types of concepts to be represented: physical objects of the observed scene, including mobile and contextual objects, and video events occurring in the scene. Terminologies describing these objects and events and terms used for scene and video analysis are listed below:

Physical object: a real world object in the scene. There are two types of physical object: physical object of interest (or mobile object) and contextual object.

Physical object of interest: a physical object evolving in the scene whose class (e.g., person, group and crowd) is predefined by end-users and whose motion cannot be foreseen using a priori information.

Contextual object: a physical object attached to the scene. The contextual object is usually static and whenever in motion, its motion can be foreseen using a priori information. For instance, the movements induced by a door, an elevator, the water coming out of a fountain, the leaves of a tree, a chair and a luggage can be foreseen.

Tracked target: corresponds to the detection and tracking of a physical object of interest. A tracked object is characterized in a scene by a unique tracking identifier.

Video event: a generic term to describe any event, action or activity happening in the scene and visually observable by cameras. Video events of interest can be either predefined by end users or learned by the system. Video events are characterized by the involved objects of interest (including contextual objects and zones of interest), their starting and ending time and by the cameras observing them. We distinguish four types of video events i.e. primitive state, composite state, primitive event and composite event which are classified into two categories i.e. state and event defined below:

- A state is a spatio-temporal property of a physical object valid at a given instant or stable on a time interval.
- A primitive state is a state which is directly inferred from visual attributes of physical objects computed by perceptual components.
- A composite state is a combination of states. This is the most complex granularity of states. We call components all the sub-states composing the state and we call constraints all the relations involving its components and its physical objects. For example: “Person p1 is close to machine m and person p2 stays inside zone z”.
- An event is one or several change(s) of state values at two successive time instants or on a time interval.
- A primitive event is a change of primitive state values. Primitive events are more abstract than states but they represent the finest granularity of events. For example: “Person p moves from zone z1 to zone z2”.

- A composite event is a combination of states and events. This is the most complex granularity of events. Usually, the most abstract composite events have a symbolical/Boolean value and are directly linked to the goals of the given application. We call components all the sub-states/events composing the event and we call constraints all the relations involving its components and its physical objects.

Five examples of video events are given below. First, an object of interest “o” (e.g. person, group, crowd) is inside a zone “z” if it’s 3D position on the ground belongs to the polygon defining the zone (i.e. “o IN z” is true). Second, an object of interest “o” classified as a person is detected as close to the vending machine if this person is detected as inside the specified zone “vending_machine_zone” and if the distance between the person and the specified equipment “vending_machine” (i.e. “o DISTANCE eq”) is less than 1.5 meters. Third, is a mobile object “o” is detected as staying inside a zone “z” when the primitive state “inside_zone(o,z)” is being detected successively for at least 30 seconds. Similarly, as fourth event, a mobile object stays at an equipment “eq” when this object is detected successively close to the same equipment “eq” for at least 10 seconds. The final event example corresponds to when a person is considered to be using a vending machine defined by: a mobile object is to be classified as a person and positioned within a distance from the vending machine so that the primitive state “person_close_to_vending_machine” is detected successively for at least 10 seconds.

4 On-line System

The first section depicts the functionalities of the long term tracking algorithm which establish temporal links between mobile objects in order to obtain robust trajectories. The object information are then analyzed by the event detector in the second section which detect simple to more complex events based on the pre-defined ontologies.

4.1 Multiple objects tracking

Tracking several mobile objects evolving in a scene is a difficult task to perform. Motion detectors often fails in detecting accurately moving objects referred to as “mobiles” which induces mistracks of the mobiles. Such errors can be caused by shadows or more importantly by static (when a mobile object is hidden by a background object) or by dynamic (when several mobiles projections onto the image plane overlap) occlusion [14].

The tracking algorithm builds a temporal graph of connected objects over time to cope with the problems encountered during tracking. The detected objects are connected between each pair of successive frames by a frame to frame (F2F) tracker [15]. The links between objects are associated with a weight (i.e. a matching likelihood) computed from three criteria: the similitude between their

semantic classes, 2D dimension differences and 3D distance difference on the ground plane.

The graph of linked objects is analyzed by the tracking algorithm also referred to as the Long Term Tracker which builds paths of each mobiles according to the links established by the F2F tracker. The best path is then taken out as the trajectory of the related mobiles. Examples of tracked objects are shown in figure 2. Three major characters are evolving in this scene: two persons are one group of persons. These mobiles objects were not successively classified in all the frames due to detection errors (discussed above). However, despite the lack of well detected and classified objects, these objects were successively tracked by the long-term tracker algorithm. Tracked mobile object examples are also shown in figure 3, from the Rome underground. It can be seen that object labeled 0 is being successively tracked as a person although it was sometimes mis-classified. This person is shown interacting with the vending machine, standing on the left side of the image. Two other persons were also tracked, person labeled 1 and 3 which are interacting with the gates to access the train platform.



Fig. 2. Tracked objects in the Torino underground station “Diciotto Dicembre”. Images corresponding to a video sequence acquired at 25 fps

4.2 Event detection

The trajectory of each detected object given by the tracking algorithm aims to build a relationship of the objects with the contextual content of the scene. Using pre-defined ontologies and the event examples in section 2, many primitive and composite events were detected related to the detected and tracked mobile objects interacting with the scene and its content.



Fig. 3. Tracked objects in the Roma underground station “Termini” direction “Rebibbia”. The 2 frames are separated by a time interval of approximately 10 seconds

Figure 4 shows two events detected in the 'Diciotto Dicembre' station, namely the "stays_inside" and "stays_at" events respectively. The "stays_inside" event corresponds to a group of persons being consecutively detected inside the "Platform" zone for at least 30 seconds and the "stays_at" event corresponds to a person being detected at gate number 7 for at least 10 seconds. 9 equipments were modeled, i.e. the 9 gates (or validating ticket machine) which allow the user to access the train, and one zone was defined in the scene: the entrance hall where people can evolve before the gates.

Figure 5 shows an example of a person using the vending machine. This person was tracked successfully for at least 10 seconds (see tracking results in figure 3) inside a small zone in front of the vending machine and close enough to it for the event "peson_uses_VM" could be detected (where VM stands for vending machine). The other persons interacting in the scene were not interacting long enough with the contextual objects for any other events to be triggered (or tracks were lost due to detection errors or occlusion ambiguities).



Fig. 4. Two events detected in the "Diciotto Dicembre" station of Torino underground

Currently we are capable of detecting twelve video events. For instance, processing two hours of video from Torino metro we de-tected over 35000 events, being the most common "inside_zone(14486) group_inside_zone(5523), close_to_Gates(5103) stays_at_Gates(3489)".

5 Off-line system

In order to have a clear and compact representation of the human activity evolving on the video and with the aim to achieve environment planning and resource optimisation, we have divided all related information to objects and events detected on the video into three different semantic tables: mobile objects table, events table and contextual objects table. Some structured knowledge representation had been introduced before [4] and [5], but in this contribution we

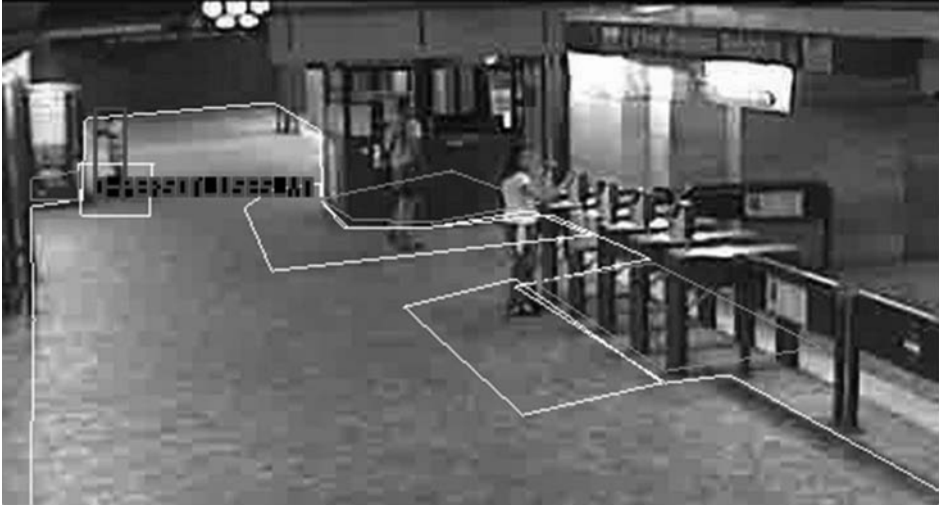


Fig. 5. Event detection in the “Termini” station of the Roma underground

propose a semantic representation which takes also into account interactions between tracked objects in the video and their environment.

Each column in table 7, presented below, contains the fields that we have included for each semantic table. Apart for reordering the information in agreement with our semantic representation, there are a series of new fields we calculate in order to extract new information. With the mobile objects table we are looking to characterize the underground users. Off-line we calculate the shape, significant event and trajectory type of mobile objects. The first field allows us to estimate the number of people in a group or a crowd. The second and third fields gives us behavioral information: what is the most frequent event and what trajectory do people usually take. To describe this last field, we implemented at this point of the processing a hierarchical clustering algorithm [6] to group similar trajectories after a given observation time. The dendrogram, resulting after applying the algorithm, is unique but the final number of clusters in which the data set is to be divided is subjective. In our case, the end-user can interactively choose the final number of clusters.

With the events table, we want to deduce what are the events that normally occur in the underground stations. Both, the mobile objects table and the Events table allows us to generate the contextual objects table, which is a major source of information to the underground manager for safety and resource monitoring and action planning. We have developed a graphical off-line analysis tool where the end users connect to the on-line database as shown in Figure 1 and select a period of recording time, which they want to monitor. Figure 7 shows from this graphical interface the information related to the contextual object VendingMachine2 (From the scene observed in Figure 2). The recording started at 7:09 and lasted 45 min (not shown). In this period 43 persons and 18 groups came to the

Mobile Objects Table	Events Table	Contextual Objects Table
<ul style="list-style-type: none"> - id. The identifier label for the object. - type. The class the object belongs to: Person, Group, Crowd or Luggage. - start. Time the object is first seen. - end. Time the object is last seen. - shape. The label describing the object's shape depending on the object's ratio height/width. - involved_events_id. All occurring Events related to the identified object. - significant_event. The most significant event among all events. This is calculated as the most frequent event related to the mobile object. - trajectory_type. The trajectory pattern characterising the object. 	<ul style="list-style-type: none"> - id. The identifier label for the detected Event. - type. The class where the Event belongs to ('close_to', 'stays_at', ...) - start. First moment on which the Event is detected. - end. Last moment on which the Event is seen. - involved_mobile_object_id. The identifier label of the object involved in that event. - involved_ctx_object_id. The name of the contextual object involved in that event. 	<ul style="list-style-type: none"> - id. The identifier label - type. The class of the object - significant_event. The most significant event among all events but referring to contextual objects. - start; - end. refer to the first and last instant the mobile object interacts with the contextual object - involved_events_id. All occurring Events related to the identified contextual object. - rare_event. This is the rarest event. - event_histogram. Gives the frequency of occurrence of all involved events. - involved_mobile_objects_id. All detected mobile objects interacting with the contextual object of interest. - histogram_mobile_objects. Gives the frequency of appearance for all involved mobile objects. - use_duration. Percentage of occupancy (or use of a contextual object). For instance, the Ticket Machine has a 10% of use over the observation time. - mean_time_of_use. Average time of interactions between the mobile object and the contextual object.

Fig. 6. Tags included in the three different generated semantic tables

Vending machine. Among all related events (shown in the Events Histogram), “group stays at VendingMachine2” was the most rare Event meaning that users do not tend to spend long periods of time while buying a ticket during rush hours. The two last fields give the percentage of use and the mean time of use for the contextual object. For the VendingMachine2, from the 45 min of observation, only 8.8% of the time was in use and the mean time a user spends on the machine is about 23 s. In the foreground of the figure, we have the evolution on the mean time of use and the percentage of use. Every five minutes and for the whole observation time these two parameters are calculated. As seen from these graphs, people tend to spend more time in the machine when their global use is relatively low (off-peak hours). The other VendingMachine also present in the hall indicates a similar users behavior. The mean time spent by a person on the machine was 30 s, and the machine was in use 7.75% of the observation time. The tracking results indicate that the number of persons and group of persons

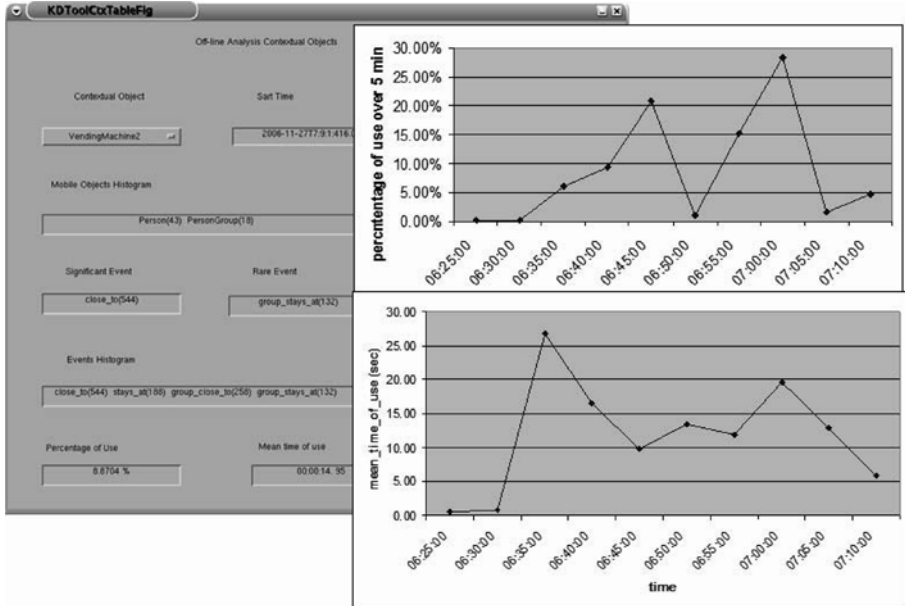


Fig. 7. Statistics calculated for the contextual object VendingMachine2

that came to this machine was of 30 and 10 respectively being also the most rare event associated to this machine 'group stays at VendingMachine1'.

All this information allows the underground manager to optimize the use of the stations. Three xml files are generated, one per each semantic table, and stored in the off-line database, either for further analysis or for subsequent queries.

6 Conclusions

In this paper, we have presented the methodology to manage and extract structured knowledge from large video recordings, which in this application correspond to two different underground network of cameras. From the multi-user knowledge, we have defined a specific ontology that we use to detect primitive events, then from a longer time of analysis, but always on-line, we can deduce more complex or composite events. Overall we are able to detect 12 different kinds of events directly from the streams of video. Off-line, we can further analyze the metadata associated to the detected objects and events of interest. Even if some vision errors still remain, pertinent statistics can be computed. In particular, we have analyzed the interaction between people and contextual objects. Among others, we are able to inform on the number of people on the scene, the percentage of use of the different contextual objects and the time a user spends with them. This is a major source of information for the underground manager

as he can better monitor and plan the resources. All raw data and metadata are stored in separate databases for better management and we have implemented an exchange format based on xml, which also support queries with web service technologies. In the future we plan to extend the ontology to increase the number of types of events we can detect and we will also look to refine the off-line analysis such as subcategories in the undertaken trajectories to give more detailed information to the end-user for better environmental planning. We also plan to develop more advanced tools to better explore the knowledge database using data-mining techniques such as relational analysis.

References

1. Carincotte, C., Desurmont, X., Ravera, B., Bremond, F., Orwell, J., Velastin, S.A., Odobez, J.M., Corbucci, B., Palo, J., Cernocky, J.: Toward generic intelligent knowledge extraction from video and audio: the EU-funded CARETAKER project. In: The IET conference on Imaging for Crime Detection and Prevention (ICDP 2006), London, Great Britain, June 13-14, (2006) 470-476
2. Martinez, A., de la Fuente, P., Dimitriadis Y.: An XML-based representation of collaborative interactions. In: B.Wasson, S. Ludvigsen & U. Hoppe (Eds.): Computer Support for Collaborative Learning: Designing for Change in Networked Learning Environments, (CSCL 2003), Bergen, Norway, (2003) 379-384
3. Lienard, B., Hubaux, A., Carincotte, C., Desurmont, X., Barrie, B.: On the Use of Real-Time Agents in Distributed Video Analysis Systems. In: IS&T/SPIE 19th Annual Symposium on Electronic Imaging, San Jose, California USA, January 28/February 1 2007.
4. Lin, H., Chen, A.L.P.: Motion event derivation and query language for video databases. In: Proceedings of SPIE, Vol. 4315 (2001) 208-218
5. Liu, D., Hughes, C.E.: Deducing Behaviors from Primitive Movement Attributes. In: Defense and Security Symposium, Proceedings of the SPIE, Vol. 5812 (2005) 180-189
6. Kaufman, L., Rousseeuw, J.P.: Finding groups in data, Wiley-Interscience (1990)
7. Velastin, S.A., Boghossian, B.A., Lai Lo, B. P., Sun, J., Vicencio-Silva M.A.: PRISMATICA: Toward Ambient Intelligence in Public Transport Environments. IEEE Trans Syst Man Cy A. 35 (2005) 164-182
8. Cupillard, F., Bremond, F., Thonnat, M.: Video understanding for metro surveillance. In: Proceedings of the IEEE International Conference on Networking, Sensing and Control, special session on Intelligent Transportation Systems (IC-NSC), Taipei, Taiwan (2004)
9. Piater, J., Richetto, S., Crowley, J.: Event based activity analysis in live video using a generic object tracker. In: Freyman, J. (ed.) Proceedings of the 3rd IEEE Workshop on performance evaluation of tracking and surveillance (PETS), Copenhagen, Denmark (2002)
10. Narayanan, S.: KARMA: Knowledge based Actions Representations for Metaphor and Aspect, PhD Dissertation, University of California at Berkeley, CA, USA (1997)
11. Hobbs, J.: A DAML Ontology of Time, <http://www.cs.rochester.edu/~ferguson/-daml/>

12. Allem, J., Ferguson, G.: Actions and Events in Interval Temporal Logic. In: Stock, O. (ed.) *Spatial and Temporal Reasoning*, Kluwer Academic Publishers (1997) 205 - 245
13. Bremond, F., Maillot, N., Thonnat, M., Vu, T.: *Ontologies For Video Event*, Technical report INRIA Sophia Antipolis no. 5189 (2004)
14. Georis, B., Bremond, F., Thonnat, M., Macq, B.: Use of an Evaluation and Diagnosis Method to Improve Tracking Performances. In: *Proceedings of the 3rd IASTED International Conference on Visualization, Imaging and Image Proceeding (VIIP) vol. 2* (2003)
15. Avanzi, A., Bremond, F., Thonnat, M.: Tracking Multiple Individuals for Video Communication. In: *Proceedings of the IEEE International Conference on Image Processing, vol 2* (2001) 379-382

XMPP based Health Care Integrated Ambient Systems Middleware

Wael Labidi¹, Jean-Ferdy Susini²
, Pierre Paradinas², and Michael Setton²

CEDRIC Labs: <<http://cedric.cnam.fr>>

Cyberfab R&D: <<http://cyberfab.net>>

wael@cyberfab.net, jean-ferdinand.susini@cnam.fr,
pierre.paradinas@inria.fr, setton@cyberfab.net

Abstract. Integrated Ambient Systems provides multiple research opportunities for individuals to apply their expertise in various contexts through a Cross Domain Collaborative Information Environment (CD-CIE). In the current context they become more pervasive in a variety of domains, especially online monitoring systems in healthcare where they allow better quality care and reduced overall cost. As standards become available and interoperability speeds up diffusion of biomedical sensor networks, IAS will involve thousands of entities potentially distributed all over the world. Their locations and behaviors may greatly vary through the lifetime of the system and require real-time management. We argue that these constraints need to be handled by an efficient middleware. In this paper, we consider inter-process communication requirements as a basic block to construct large scale IAS. We propose a possible real-time event notification model to perform the loosely coupled interactions required in such large-scale settings. We provide an XMPP based event notification solution with detailed model and working proof.

Key words: Ubiquitous Systems, Ambient Intelligence AmI, u-health, mobile computing, Body Sensor Networks, Real-time Internet, Event Notification Middleware, XMPP.

1 Introduction

Communicating devices are increasingly portable and miniaturized, offering users more mobility and richer services. In this context, ambient intelligence (AmI) provides a new vision of the information society where the emphasis is on user-friendliness, efficient and distributed services support, user-empowerment, and support for human interactions. The synergetic relationship of body sensor networks with AmI has paved the way for Integrated Ambient Systems (IAS), which find applications ranging from military to sports.

The wide variety of scenarios and constraints make difficult the implementation of IAS in real world for large numbers of users. This requires the development of a dedicated and flexible communication infrastructure based on an adequate

interaction scheme. The event notification middleware is receiving increasing attention and is claimed to provide the loosely coupled interaction required in such large scale and real-time settings.

This work proposes an eXtensible Messaging and Presence Protocol (XMPP) based event notification middleware for real-time and large scale Integrated Ambient Systems applied in the healthcare monitoring application domain. Healthcare, as an application area for IAS (HCIAS) can be subdivided into three main categories: emergency, therapy and care. Although these categories are partly overlapping, and sometimes possess similar functionalities, they will all be used here as they provide a cross domain collaborative information environment for monitoring people's health status. This means that we give full emphasis in this study to the communication infrastructure. But, administration, management, logistics and support will not be addressed here, as they are specific to the health sector. The rest of this paper is structured as follows: section 2 resumes related works; Section 3 presents backgrounds of this work; Section 4 explains our proposed XMPP based system architecture and Section 5 describes our prototype. Finally, section 6 concludes and presents perspectives of this work.

2 Related Works

Services focusing on personal well being have been developed with a primary focus on the social care domain and are reliant solely on body sensor networks for collecting physiological and contextual data. HCIAS has the potential to extend those choices and to move these services further into the mobile and continuous medical care domain.

Body sensor networks (BSN) provide a platform for collecting physiological and contextual information about the service end user. On the other hand, sensor data needs to be sent up to higher networks to get the complete picture; for analysis and feedback or alarm services. Pertaining to this data collection and processing needs, the following studies are representative of the state of the art:

- **CodeBlue** [1] comprises a suite of protocols and services that let many types of devices (wireless sensors, location beacons, handheld computers, laptops, and so forth) coordinate their activities. CodeBlue is an “information plane”, which lets these devices discover each other, report events and establish communication channels. CodeBlue incorporates (i) a flexible naming scheme; (ii) a robust publish/subscribe routing framework; (iii) authentication and encryption provisions. It also provides services for credential establishment and handoff, location tracking, and in-network filtering and aggregation. It does not focus on presence detection; although an ambient system should be able to detect the presence of users, and machines [2]. Communication is based on a particular protocol CodeBlue Query (CBQ) which limits interoperability.
- **Mobihealth** [3] resulted in the development of an m-health service platform including a generic Body Area Network (BAN) for tele-healthcare. Bio-signals measured by sensors connected to the BAN are transmitted

to a remote healthcare location over public wireless networks (e.g. GPRS, UMTS), where physicians can monitor, diagnose and provide advices to patients in real time. Mobihealth is based on Jini [4] which is a good technology with respect to device interoperability and network plug-and-play. It also contributes to network service discovery, especially for a dynamic network. However, Jini services are more efficient in small and medium-scale than large-scale applications services [5].

- The **Awareness** project [6] focuses on a service and network infrastructure enabling rapid and easy development of context-aware and pro-active applications in a secure and privacy-conscious manner. Particular attention is paid on mobile applications in the healthcare domain, specifically to tele-treatment of patients with chronic pain and tele-monitoring of epileptic seizures and uncontrolled movements in spasticity. The project proposes a network infrastructure based on SIP/SIMPLE protocol which is an IETF standard. SIP/SIMPLE is poor in term of inter-domain scaling [7]. SIP/SIMPLE does not support advanced messaging mechanisms [8] like Workflow Forms, Multiple Recipients, Reliable Delivery, and Publish-Subscribe which are the bases concepts for large scale and real time distributed applications.
- **uMiddle** [9] is a bridging framework for universal interoperability providing seamless device interaction over diverse platforms. It introduces four design patterns for interoperability frameworks and implements prototype at each chosen design point: Mediate, Aggregate, Fine-grain, and Infrastructure. Given the state of “standards”, it maybe a useful starting point for interoperability, however it seems not clear in practice; how the mapping between device semantics and different protocols will be handled and how an unified abstraction of he QoS management over multiple different protocols will be provided.
- In [10] the authors propose a mobile healthcare system architecture based on JADE (Java Agent DEvelopment Framework) framework for scalability. JADE is a framework fully implemented in the Java language. It simplifies the implementation of multi-agent systems through a middleware that complies with the FIPA specifications [11]. But scalability in JADE platform depends on the number of agents which decreases performance in large scale contexts. Indeed, as proven in [12] JADE is characterized by a nearly linear scalability.
- There are also many other industrial related works as IBM Personal Care Connect [13], Microsoft Research Integrated Systems [14], Intel Personal Health [15], Oracle and Toumaz Personal Health Monitoring System [16].

3 Backgrounds

3.1 Event Notification Middleware:

Ubiquitous systems are characterized by the heterogeneity of systems and devices, as well as the “spontaneous” patterns of interconnection. An event-based

architectural style is particularly well suited for such distributed environments without central control [17]. At the core of an event notification middleware is an event processing engine. This engine is based on Publish-Subscribe pattern. Not only does the event processing engine provide decoupling between publishers and subscriber in space, time and synchronization, but it also filters out new events against subscriptions at the publisher's event broker, exploits overlapping subscriptions, and employs multicast-like routing of events to subscribers. Filtering at the publisher's event broker is achieved in three different ways: (Topic-based [18] filtering, Content-Based [19] filtering and Type-based [20] filtering).

3.2 XMPP:

eXtensible Messaging and Presence Protocol [21] base specifications formalize the core protocols developed within the Jabber [22] open-source community in 1999. They were produced by the IETF's XMPP Working Group and published as RFCs in October, 2004.

Presence is a mechanism for communication and interaction. The classic example is Instant Messaging (IM), which was the first aim of Jabber/XMPP. Because these IM services enabled us to see when our contact list's members were online, they familiarized a whole generation of Internet users with the concept of presence-based communication.

The "publish-and-subscribe" model forms the core of the XMPP Event-Broker technology formally specified in XEP-0060 [24]. This Event-Broker enables fine grained access control over publishing and subscribing as well as a payload agnostic routing model enabling publishers to syndicate any XML data format. It integrates a sophisticated content based filtering. Indeed, content matching is based on everything from simple keywords to structured data embedded in an XML message which allows us to call out text of particular importance and dynamically trigger real-time published information.

4 Proposed Architecture

The problem of designing scalable network architecture is of primary importance. Most research works in HCIAS proposed multi-tiers architecture based on BAN which consist of portable sensors, and a Personal Gateway. The Personal Gateway has two functions: the aggregation and the transmission of sensor data. Each BAN is interconnected to a Medical Center (MC), which is in charge of storing data locally for subsequent retrieval. The MC is established by combining medical information system and mobile monitoring services.

We are opting for a client-server architecture as opposed to a peer-to-peer architecture [25] [26]. Client-server separation and transferring complexity to the server-side bring several benefits:

- » Keep the client as light as possible.
- » Clients not need to be modified if the inter-server was modified or updated.

- » Personal information is maintained at the server level and we can access to this information with any client from any operating system. We don't need to synchronize data every time we use different clients.

The use of an event notification pattern brings many advantages, such as scalability and loosely coupled entities. Additionally, Service Federation guarantees more spreading of resource usage and control between services [27] [28]. In a federated architecture, the server can be viewed as a federation of heterogeneous systems that provides a uniform interface to the outside world and at the same time preserves their local autonomy and stand-alone access. Both local autonomy and same time access are extremely important as the data collection is distributed and groups that are using the data are not always the groups that generate the data.

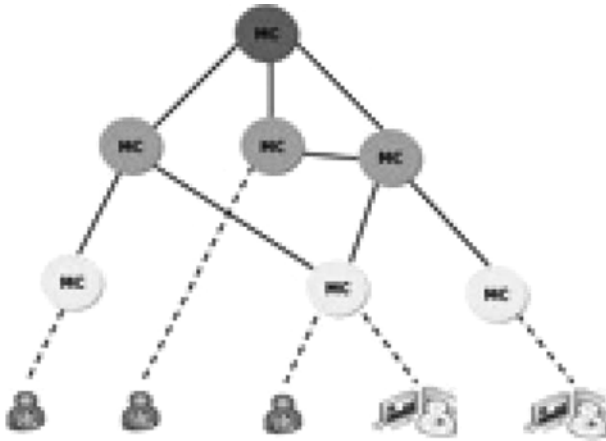


Fig. 1. Federated client-server architecture

XMPP uses a federated client-server architecture; each client connects to the server that controls its XMPP domain. This server is responsible for authentication, message delivery and maintaining presence information for all users within its domain. If a user needs to get information pertaining to a user outside of its own domain, its server contacts the external server that controls the “foreign” XMPP domain and retrieves information from that XMPP server. The foreign XMPP server takes care of delivering information about the intended user within its domain. This same server-to-server model applies to all cross-domain data exchanges, including presence information.

The Service Oriented Architecture (SOA) has initially been introduced for supporting business processes built out of the composition of services implementing complex business related applications. However, skins of SOA make it also

particularly suited for the dynamic composition of complex systems. SOA can be viewed as a network of services, which may implement our middleware related functionalities, and be available on any kind of node. In the case of HCIAS we have identified different basic middleware services: the Lookup service, the Event Communication service, the Information Routing service, the Context Awareness service and the Security and Privacy service (services related to bottom communication layers are out of the scope of this paper).

4.1 Service Discovery

The widespread deployment of inexpensive communications technology and computational resources in the network infrastructure for HCIAS poses an interesting problem for end users: how can one locate a particular service or device out of hundreds of thousands of accessible “disappearing” services. To avoid the old static paradigm based on simple URL’s scattered through configuration files, it is necessary to have a reliable discovery process by which applications can discover services, but current service discovery protocols are not by themselves sufficient to facilitate the spontaneous sharing of services [29].

XMPP networks provide a standardized [30] ability to discover information about entities on the network and their presence. This mechanism allows to querying information such as features offered or protocols supported by an entity, the entity’s type or identity, and additional entities that are associated with the original entity in some way. This is an invaluable advantage over existing protocols when it comes to negotiating sessions in communication spaces. In a distributed network architected around a clear separation between communication control logic and service control logic, this capability will allow to discover existing services and their “availability”.

4.2 Information Routing Framework

As described above, our proposed architecture is based on a Publish/Subscribe routing framework in which BANs publish relevant physiological and contextual data to a specific channel while monitoring applications subscribe to channels of interest by expressing their information content filters.

By definition, any extensible infrastructure, should be extensible, cope with evolution, and should provide means for adaptability. Although these requirements were the main reason for building middleware in the first place, they gain more importance in ubiquitous and ambient settings where the overall setting is highly dynamicity and bindings between clients and services are volatile and casual at most.

Another issue is the inherent heterogeneity of the environment. The description of functionality should be independent from the actual technology found in a certain environment in order to separate the semantics of the functionality from the actual implementation and the technology applied. This provides the means for evolution and extensibility.

Based on XML, XMPP offers more extensibility and flexibility allowing better collaboration capabilities. XML structured communication provides better interoperability means and wider compatibility. Indeed, XMPP is already compatible with many different protocols, and it has the ability to extend to future protocols as they become established.

4.3 Context Awareness

A context is any information used to characterize the situation of an entity. A system is context-aware if it uses a context to provide relevant information and/or services to the user, where relevancy depends on the user's task [31]. The major objective of a context aware middleware service for HCIAS are the seamless integration of heterogeneous context sources, an efficient mechanism for distribution handling, and the support of different HCIAS contexts ("Mobile context", "Home context" and "Hospital context"). This includes the support of environment-aware devices. In short, a context-aware service can range from "intelligent notification systems" that inform the user about events or data, to "smart spaces", i.e. places/environments that adapt to the users.

The Naming scheme based on Virtual Identities and the distribution of presence information provided by XMPP is particularly suitable for the transport of messages in ubiquitous environments. Indeed, Virtual Identities make possible to build an overlay network allowing mobile terminals to carry on complex interactions while continuously changing network coordinates, with the only constraint being to be able to directly communicate with the home server (domain). Moreover, XML flexibility can integrate richer information such as: Contact information, Session capabilities, Role, Availability and Priorities.

4.4 Security and Privacy

A very important aspect in handling medical data is its security and privacy. For HCIAS, data access and software exchange are achieved over insecure networks such as the public Internet. We are therefore forced to be proactive with regard to verifying the identity of both human users and software processes that request access to protected resources such as physiological data of a particular patient. User identification and medical records can not be disclosed indiscriminately. Also, different healthcare providers have different access rights to these records. Therefore, such applications must support authentication, authorization, federation, and privacy requirements. Not only are those requirements difficult and complex to implement but their definitions varying widely. In fact, security and privacy depends on the rules and policies specified by each service provider.

Certainly, security is not a one-time task, but an ongoing process and we concur that information security is more than just encryption and cryptography. However, by integrating standards security protocols [32], XMPP presents a foundation for a security infrastructure.

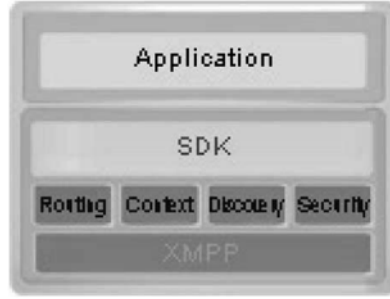


Fig. 2. Middleware Layered Architecture

5 Prototype

The goal of the pilot study is to evaluate the medical value of HCIAS in general and to more assess our middleware solution. Figure 3 shows the IT (information technology) infrastructure used for this pilot study. It includes the following components: a BSN, a Personal Gateway, an XMPP Pub/Sub broker, a Rich Internet Applications (RIA) Server, a Data Warehouse, a Directory Tree and a Remote Monitoring Client.



Fig. 3. Prototype Logical Architecture

According to [33], Bluetooth currently represents the best option for a personal area network for medical applications. As shown in the Fig. 3, we used SensPod (our Bluetooth multi-sensor platform [34] for capturing location “GPS sensor”, heart rate “HeartBit sensor” and movement “Accelerometer sensor”), and a Nokia70 mobile phone as a SymbianOS based Patient Gateway and a Samsung SGHi 300 mobile phone as a Windows Mobile based Patient Gateway. The system supports three different user profiles. The main users are patients and their relatives. For this group it is important that the system was reliable and had a simple user interface so that it could be operated without any expert knowledge. The second user group are physicians who are responsible for regularly monitoring their patients’ data to ensure its conformity with the expected course of

therapy. The final user group consist of administrator who supervise the system, analyze the user behavior from a technical point of view (e.g., to ensure that patients' data was uninterrupted), and generate from the collected data special reports that are sent to the hospital staff for medical analysis.

The key behind our design of the real-time large scale inter-process communication model can be quickly summarized as follows: real-time capture of patient data (heart rate, 3D acceleration and geographical location) generated by special sensors platform in a reliable way, combine them with time-stamp information, to aggregate them on a portable communication device, and transfer them in a secure and reliable way to a medical server. The server had to store the data and offer different views of patient data for physicians, allowing them to analyze the therapy of their patients.

We have tested the prototype in a real-world environment, however, the number of concurrent users was small, and so we can not say exactly what the performance would be for a large scale deployment. But since the amount of data that is transported over XMPP has a relatively small footprint, we believe that this will not be an issue. This is, however, a point that needs to be more thoroughly investigated; our prototype implements only three monitoring services that are identical for each client. Another point is that our current middleware implementation need more investigation on high-availability and fault-tolerance mechanisms integration.

6 Conclusion and Future Works

The approach implemented here provides a versatile use of the eXtensible Messaging and Presence Protocol to serve as a core protocol in an event notification middleware platform for real-time and large scale health care integrated ambient systems. It does so by proposing a concrete infrastructure within a service-oriented architecture, while taking into account requirements in terms of scalability, interoperability, security and privacy.

We have come to the conclusion that XMPP is well suited to the real-time and large scale health care integrated ambient systems. Even though it is a verbose protocol based on XML, it is not so verbose as to negatively affect a client's ability to participate in event notification services. Of course, when very large amounts of notifications are sent to a client, it is possible that the client can not cope with the data flow. This is, however, not strictly XMPP related. The same thing could happen using any other protocol.

Interesting future works lies in analyzing the possibilities of the OSGi framework and other existing dynamic software components container to reduce the complexity of our current Personal Gateway implementations. This complexity mainly consists of the large amount code elements coupling. Without such proper tools for code and service reuse, we have been obliged to duplicate many functionalities for every smart client.

References

1. M. Welsh: Sensor Networks for Emergency Response Challenges and Opportunities (IEEE 2004).
2. P. Remagnino, G. Luca Foresti and T. Ellis: Ambient Intelligence A Novel Paradigm (Springer2005).
3. D. Konstantas, R. Bults, A. Van Halteren, K. Wac, V. Jones, I. Widya, R. Herzog, B. Streimelweger: Mobile Health Care Towards Commercialization of Research Results (2006).
4. Jini: <http://www.jini.org/>
5. J. Yu, J. Newmarch, M. Geisler: JINI/J2EE Bridge for Large-scale IP Phone Services (IEEE 2003);
6. M. Wegdam: AWARENESS A project on Context AWARE mobile NETworks and ServiceS (14th Mobile & Wireless Communications Summit 2005, Germany).
7. A. Hourri: "Problem Statement for SIP/SIMPLE," (draft-ietf-simple-interdomain-scaling-analysis-00, February 2007).
8. P. Saint Andre: XMPP-SIMPLE Feature Comparison (JSF 2005).
9. J. Nakazawa, W. Keith Edwards: A Bridging Framework for Universal Interoperability in Pervasive Systems Distributed Computing Systems (ICDCS 2006).
10. N. Kim, Y. Jeong, S. Ryu, D. Shin: Mobile Healthcare System based on Collaboration between JADE and OSGi for Scalability (IEEE 2007).
11. FIPA specifications: <http://www.fipa.org/>
12. F. Lo Piccolo, G. Bianchi, S. Salsano: A Measurement Study of the Mobile Agent JADE Platform (IEEE 2006).
13. IBM PCC : <http://www.zurich.ibm.com/pcc/>
14. MS Research Integrated Systems : <http://research.microsoft.com/is/>
15. Intel Personal Health: <http://www.intel.com/healthcare/personalhealth/>
16. Oracle and Toumaz: <http://www.toumaz.com/healthcare/>
17. IEEE DS Online-Event Based Middleware Community <http://dsonline.computer.org/>
18. TIBCO Software Inc: TIBCO TIB/Rendezvous. (1999).
19. Carzaniga, A., Architectures for an Event Notification Service Scalable to Wide-area Networks, PhD. Thesis, Computer Science, University of Colorado, Boulder, 1998.
20. P. EUGSTER: Type-Based Publish/Subscribe. Computer Science Thesis, University of Lausanne, EPFL, 2001.
21. XMPP: <http://www.xmpp.org/>
22. Jabber : <http://www.jabber.org/>
23. XMPP Extensions : <http://www.xmpp.org/extensions/>
24. XEP-0060: <http://www.xmpp.org/extensions/xep-0060.html>
25. N. Maibaum, T. Mundt: JXTA A Technology Facilitating Mobile Peer-To-Peer Networks (IEEE 2002).
26. Philips Research: http://www.extra.research.philips.com/swa/cluster_phcs.html
27. L. Fuentes, D. Jimenez, R. Meier: Implementation of an AmI Communication Service Using a Federated Event System Based on Aspects (2006).
28. T. Bass: The Federation of Critical Infrastructure Information via Publish-Subscribe Enabled Multisensor Data Fusion (ISIF 2002).
29. R. Liscano, A. Ghavam, M. Barbeau: Integrating Service Discovery Protocols with Presence-based Communications for Ad hoc Collaborative Scenario (IEEE 2006).
30. XEP-0030: <http://www.xmpp.org/extensions/xep-0030.html>.

31. G. D. Abowd, A. K. Dey: Towards a Better Understanding of Context and Context-Awareness (CHI Workshop 2000).
32. Extensible Messaging and Presence Protocol (XMPP)-Core:
<http://www.xmpp.org/rfc/rfc3920.html#security> (Internet Society 2004).
33. E. Visinescu, "Analysis, Outlook and Perception of Telemedical Technology at Home and in a Mobile Environment," Diploma Thesis, Mannheim University of Cooperative Education (May 2006).
34. M. Setton, W. Labidi, R. Guignier: Bluetooth sensors for wireless home and hospital healthcare monitoring.

Increasing Interactivity in Agent-based Advanced Pocket-Device Service Application

Sameh Abdel-Naby, Paolo Giorgini, and Stefano Fante

Department of Information and Communication Technology (DIT)
University of Trento, Povo 38100, Italy.

{sameh, paolo.giorgini, stefano.fante}@dit.unitn.it

Abstract. Independence, intelligence and interactiveness are making software agents strongly approach the development of advanced service applications for both, pocket and fixed computing devices. In this paper we present an interactions protocol that is used by intelligent agents operating in a dynamic environment. In particular, we focus our research on the situation where a multi-agent system is serving lightweight devices through advanced communication methods (e.g., Bluetooth). Like similar contributions, our interactions protocol provides agents with a monetary system and a mechanism for feedback calculation. The goal of our research was to accelerate efficient agents interactions while resolving end-user composite tasks.

1 Introduction

Lightweight devices such as cellular phones and PDAs are increasingly involved in most of our daily life duties. Nowadays, people can go anywhere carrying their pocket devices which allow them to check their emails, surf the internet and do shopping. Services are provided through user-friendly and well-developed interfaces, and almost costless in regard to the value of services users are getting. Currently, standard mobile services that never existed before are becoming a must (e.g., SMS and MMS), and advanced ones that newly existed are now highly desired (e.g., Service Guides and Group Gaming).

Several efforts in literature, for example [3], tackled the scenario where the cellular phone of a visiting scholar establishes a connection with a localized Multi-Agent System (MAS) and, a synchronization is made to finally come up with meetings agenda. Participants of such scenario are moving within a university carrying their lightweight devices or, they have previously delegated an agent to act on their behalf. Automated system agents cooperate and negotiate available times to create a suitable agenda for everybody. Accordingly, the visiting scholar and meeting requesters are forming together a Mobile Virtual Community [7] that is location-based.

Another approached scenario is about tourists that turn to be MAS users after enabling the Bluetooth functionality of their pocket devices and, using a preinstalled application, their devices communicate with distributed servers and

retrieve useful information related to the places they are visiting (e.g., [1]). In different approaches, every single item available at a museum can be represented by its own software agent, and this agent can cooperate with others to fulfill certain complex user desires (e.g., relevant places opening times and transportations).

Through lightweight devices, users in previous scenarios are performing a set of actions that are driven by application instructions to finally create a delegative agent. Eventually, this agent will be searching for methods to fulfill user desires and, a matchmaking process will take place; an agent that carries specific information will look for another agent that is willing to give extra data so a task gets completed. Still, sometimes an agent will never find a single completer and thus, there are complex one-to-many scenarios where group of agents cooperate.

Unless software agents learn to properly interact there will not be an extra capability for people to cooperate. A negotiation language that is applied among distributed agents is helping them to understand each other, discuss their desires and finally achieve their objectives. Several of the negotiation protocols proposed by scholars are inspired from sociological, political and psychological studies about human negotiation in real-life situations such as auctions, peace agreements and biddings.

We focus on multi-agent systems that deliver location-based services to users of lightweight devices through advanced communication capabilities. We contribute to existing literature by presenting a negotiation algorithm we adopted in a rideshare application, which increased the interactivity level among involved agents. Although there are some restrictions given by users (e.g. time to achieve) and others given by involved technologies (e.g. Bluetooth data exchange rate), still the architecture we developed is reliable and increases system usability.

The remainder of this paper is structured as follows. Next section emphasizes our research motivation. Section 3 looks at the building blocks of the proposed interactions protocol. Section 4 applies the presented negotiation algorithms to a testbed application. Section 5 highlights the related work. Section 6 demonstrates our future work and concludes the paper.

2 Motivating Scenario

In a MAS delivering service content to lightweight devices, a set of uncooperative agents that are self-interested and benefits maximizers are located. It is more often that this set contains two different types of agents, BUYER AGENT (BA) and SELLER AGENT (SA). Each of them holds information related to its role in the system and, a BA keeps data that helps SA increases his profit, and the data SA keeps helps BA to achieve the overall objectives of the system. If agents predefined behavior is strict and intelligent “usual case in MAS” this will lead both agents to - *sometimes* - reach a situation of disagreement.

The fact of having two successfully matched agents and yet no useful results are gained is quite challenging. The existence of autonomous agents in MAS is necessary to increase system reliability and, interactivity between all application entities is still highly desired, but an unfruitful negotiation process among in-

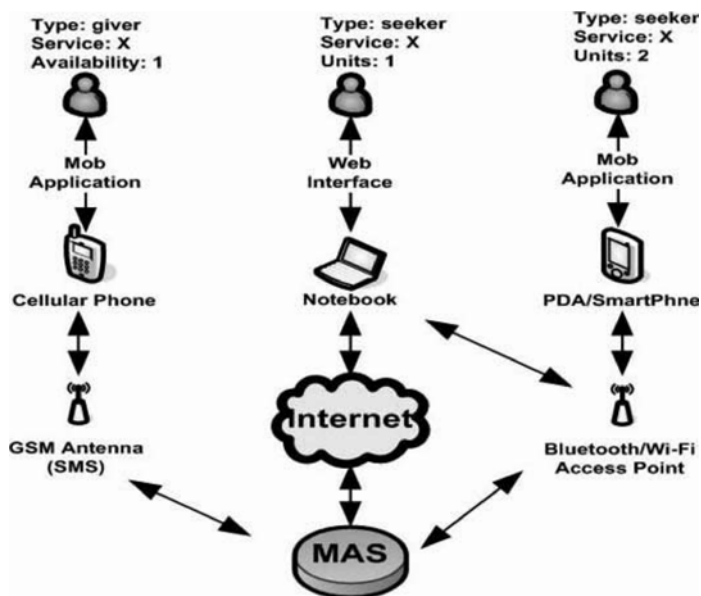


Fig. 1. Different devices use different communication methods to interact.

involved software agents is what a complete application should avoid, and this is what we precisely try to address.

In figure 1, we assume that three different users are interested in using the same multi-agents architecture to obtain a certain item or service. This service is limited to the demand and supply of a specific product among system users (e.g., available care seats in a carpooling system or used books in trade environment). These users are using their lightweight devices to communicate with the service architecture and, each is adjusted to the use its pocket application. Actors differ, one can be a service giver and the others are the requesters. If we move to the point where the number of acquisition requests is greater than the number of offered items, insufficient matches occur.

Each of the involved lightweight devices is configured to utilize specific communication method to access the service, a cellular phone or a notebook may exchange service requests using SMSs, The Web or a distributed Bluetooth or even Wi-Fi access points. If a user is offering a single item that more than a single requester is interested to have, the managing MAS will drive these three - or more - users to a complex situation where the ownership of the offered item is not determined. In this case, the system hangs at the pre-agreement point where the service preferences are matching, items are available, but conflict is located and no actions are taken.

An auction mechanism can be invoked to resolve any complex situation that may occur among several competing agents. This mechanism can be restricted to

different conditions, such as time and location constraints, and it can be wisely adapted to ensure ultimate benefits gaining for both, the supplier and demander agents. The invoked mechanism can also be heuristic by storing auctions results that involve same software agents - *representing same users* - more than a certain number of same scenario participation.

3 The Auctioning Interactions Protocol

In this section we present the negotiation scenario involving concerned agents to finally establish proper communication channels, achieve better results, and increase the level of efficient interactivity.

Given a set of lightweight devices that are capable of communicating specific data with central MAS servers via distributed access points and, given that the overall architecture is providing end-users with a predefined location-based service. The lightweight devices here are used to clarify users preferences and consequently, a Mobile-to-Server Link Agent (MSLA) is created. This particular agent carries specific user desires details and, it is capable of transferring from a lightweight device through the nearest access point to reach server side. When the MSLA arrives to one of the central service servers, its carried desires are forming an autonomous software agent that reflects certain user characteristics. This MSLA is basically a configuration file that is produced by each lightweight device participating in a certain trade scenario.

Eventually, the arrival of a new agent to the server side requires the running MAS to verify whether this agent is new and to be bootstrapped or, it already exists and it meant to update the behavior of a running agent.

A group of delegative autonomous agents that are seeking to achieve different tasks in different times is located at the server side of the architecture. When some of the tasks to be achieved are complex and require high level coordination, a negotiation scenario that requires a single agent to deal with several service requests coming from different greedy agents is situated. However, in agent-to-agent situations, the negotiation protocol applied is simple and efficient; it is the same as market demand and supply equality. When the supplier and the demander are matched, a mutual benefits exchange is achieved. This usually occurs because only one demander and one supplier are located within the service range of each other. Unsurprisingly, in agent-to-many it is more complex.

In figure 2, Algorithm 1, we show the algorithm used by Seller Agent (SA) to invoke an auctioning situation that is expected to resolve a complex negotiation situation. From line 1 to line 3, both SA variables, `bestValue` and `numLoop`, are initially set to '0'. In line 4, the seller agent requests the Buyer Agent (BA) to start the auction by sending the value of the best offer previously obtained during the pre-offer session. From line 5 to line 7, the SA waits to receive new offers from all involved BAs, and a `val` is created as a function to calculate the currently obtained best-offer-value. From line 8 to line 10, if the algorithm had its first round and a `val` is gained, the `bestvalue` in line 1 is now updated with the value of `val` and the number of loops `numLoop` is gradually incremented.

<pre> Seller_Agent_procedure() 1: bestValue = 0; 2: numLoop = 0; 3: auctionIsOpen = true; 4: askBAToStartAuction(bestPreOffer); 5: while (auctionIsOpen) do 6: waitForOffers(); 7: val = calculateBestValueOfFunction(); 8: if (numLoop == 0) then 9: bestValue = val; 10: numLoop++; 11: else 12: if (val > bestValue) then 13: bestValue = val; 14: requireNewOfferToBuyers(bestValue); 15: numLoop++; 16: else 17: if (val <= bestValue) then 18: quitAuction(); 19: informWinners(); 20: end while 21: quitAuction(); </pre>	<pre> Buyer_Agent_procedure() 1: BABestOffer = 0; 2: sent = false; 3: while(auctionIsOpen) do 4: sent = false; 5: bestOffer = waitForRequest(bestPreOffer); 6: decision = decideIfAcceptOrRefuse(); 7: if (decision == accept) then 8: while(modificationsArePossible && !sent) do 9: newVal = reviewParameters(); 10: if (newVal > BABestOffer && newVal > bestOffer) then 11: BABestOffer = newVal; 12: sendOffer(BABestOffer); 13: sent = true; 14: if (!sent && !modificationsArePossible) then 15: sendOffer(BABestOffer); 16: end while 17: else 18: if (decision == refuse) then 19: quitAuction(); 20: end while 21: quitAuction(); </pre>
---	--

Algorithm: 1 The procedures taken by the Seller Agent.

Algorithm: 2 The procedures taken by the Buyer Agent.

Fig. 2. The negotiation protocol assisting agents to establish proper communications.

Otherwise, since it is not the first loop, from line 11 down to line 19, the SA checks whether the `val` function is increasing with respect to last obtained best value. At this point, two scenarios may occur, if `val` is greater, the value obtained from the concerned BA is communicated with other BAs and, they are asked to Re-offer if applicable, then the algorithm is restarted - *line 14 and line 15*. If the `val` is less or equal to the best value previously obtained, the auction is suspended and the BA currently had the `bestValue` wins - *line 17 to line 19*. Finally, the algorithm is terminated and the auction scenario is ended - *line 20 and 21*. Following to that, we explain the BA responses with respect to SA.

In the same figure but Algorithm 2, from line 1 and line 2, a variable `BABestOffer` that carries the buyer agent best offer value is created and set to '0'. A variable `sent` is initially set to `false` and it changes to `true` only after a BA has communicated his offer. From line 3 to line 6, while the auction is open, BA holds its offer transfer until a communication was received from the Seller Agent (SA) asking for an auction participation decision. The BA puts the results from the evaluation function into the `decision` variable.

From line 7 to line 9, if the BA accepts the SA call for auction participation a self-revision for its parameters is made. This revision indicates BA's insistence to obtain the auctioned item and its intentions to show extra negotiation flexibility. The part from line 10 down to line 13 refers to the comparison made by the BA

to put together the newly obtained value and the existing one. If the new value obtained is greater than the previous one and, greater than the `bestOffer`, the future offered value `BABestOffer` is set to new one and stored in `newVal` and the offer is sent to the corresponding SA.

Line 14 to line 16, after the BA self-revision, if the value gained is the same as the previous one, this specific BA do not send the previous value if `modificationArePossible` is true. The BA continues to review the carried parameters until `modificationArePossible` becomes false or it communicates new better offer. If `modificationArePossible` stays on false and parameters are not sent, the BA communicates same previous offer.

From line 17 to 19, if BA refuses the auction call the algorithm terminates and the auction involves this particular agent ends. Eventually, the algorithm passes on the first condition if `decision == accept` but the condition of the successive while `modificationArePossible&&!sent` return false. The method `decideIfAcceptOrRefuse` return `refuse` if for instance, a BA has enough time before the auction deadline and it decides to refuse present participation. Finally, the algorithm is terminated - *line 20 and 21*.

Auctioning among agents requires high level agent-to-user interactivity and network resources consumption. Therefore, agents' intelligence may appear when a repetitive scenario occurs. The algorithms presented can be further adapted to maintain system and participants history.

Once the pocket-device application is configured to repeat the same service request on daily or weekly basis, and similar agreements are achieved between a specific supplier and a demander at a certain price, the next time this demander agent will be first looking-up the very exact supplier agent that has potential agreement than others. This can be simply added through a learning agent behavior that maintains an array that saves last successful agreement details.

4 A Case Study

ToothAgent [2] is an example of a Multi-agent system (MAS) that allows university frequenters to use any of their computing devices to exchange used books requests and offers. Once an agreement is reached, the system helps students to agree on meeting places and times. This is all done through normal Bluetooth communications that take place between both, user and distributed servers. Agent-oriented programming techniques are used to form a Mobile Virtual Community [7]. This helps the system, including its Intelligent, Mobile and Autonomous agents to go through the matchmaking and exchange of requests processes and, support the price negotiation phase.

Andiamo [11], is an example of a MAS implementation that provides its users with a possibility to utilize their lightweight devices to offer/look-up shared car rides. To understand the *Rideshare* service or *Carpooling* as stated in literature; it is a method to reduce the use of cars in a specific town or area, and it take place by having a car owner who uses his/her car to move from a place to another, and another person who is interested to go somewhere along the car owner's way

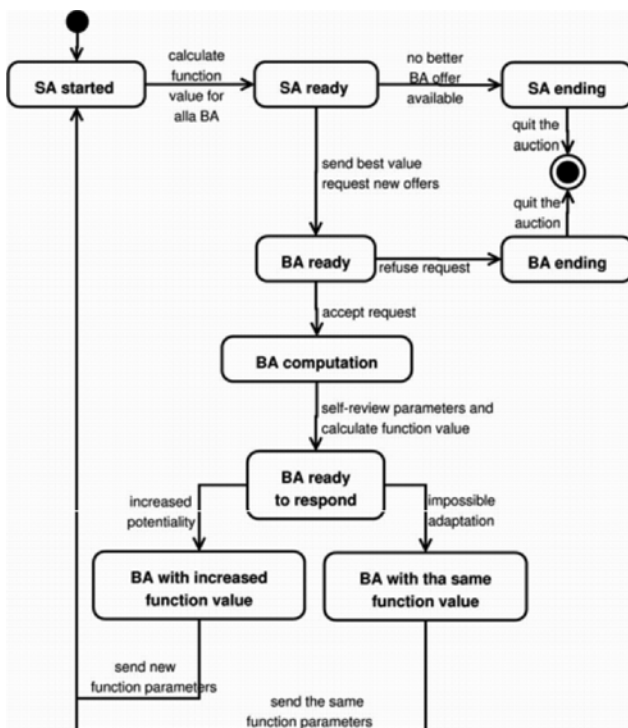


Fig. 3. Auction call and termination in a Rideshare MAS service architecture

to destination, and at the same time the ride seeker is willing to share the ride cost with the car owner. This system would, among other advantages, rationalize energy consumption, save money, and decrease traffic jams and human stress, and eventually make a significant improvement in human life.

In this section, we further elaborate on the mechanism we proposed through the demonstration of a pocket-device rideshare service architecture we developed. In our example, we primarily assume that a car ride giver (Seller Agent) - **SA Started** - has communicated and submitted the offer details to the Multi-Agent System, this MAS is managing the exchange of service requests among connected computing devices, and we assume that only one available car seat is given by the car owner, and a matching phase has resulted three or more interested ride seekers that are all willing to share the given ride cost.

As shown in figure 3, from this point on SA Ready, which is the agent acting on behalf of the ride-giver, will be responsible of resolving this complex situation by: 1) according to the parameters given by agents of the ride seekers, a calculation process is performed and each agent is assigned a value, 2) a comparison between the yielded values is made and sent to interested ride seekers, then a call for auction is made, 3) a request to all interested agents to send new offers is

communicated. Each agent acting on behalf of a ride seeker is free to choose to participate in the auction, but hence an agent has decided to skip an auction, the negotiation process involving both parties is ended - **SA Ending - BA Ending**.

This was considered because end-users may put more rigid or loose behavior on the representing agent at anytime. But once a seeker agent has decided to go through the auction - **BA Ready**, a self-revision process for the carried parameters is made - **BA Computation**, and then a value calculation is made and compared to the previous one obtained, then results are communicated with the ride giver agent originally invoked the mechanism. The seeker agent keeps trying to compromise in accordance with interests so a new agreement is reached.

Results reached after parameters modification - **BA Ready to Respond** - will indicate if a new auction winning potential is found. Depending on the value obtained in earlier step, the same old parameters or new ones will be communicated back with the ride giver agent (SA) - **BA with Increased Function Value** or **BA with Same Function Value**. The ride giver agent re-evaluates the received parameters including those received from newly joined agents, if any. Then, an announcement is made for the only available car seat winner. Accordingly, the auction terminates and the entire negotiation process ends. The mechanism can be repetitive only if no agreement situation was found and the time to achieve the actual ride is yet far.

Auction invocation and the exchange of messages among involved agents consume time and network resources. Therefore, the operating MAS can further store the auction initiator and winner to rapidly resolve future complications. This can only happen if the algorithms used were adapted to observe certain auction results that are identically repeated, so the system would automatically consider this winning ride seeker agent as high-potential future auctions winner, or one of the winners - *if more available seats were given*.

5 Related Work

Part of the research conducted in Distributed Artificial Intelligence (DAI) focuses on the coordination among objects located in distributed environments. Thus far, a research topic under DAI that is Distributed Problem Solving (DPS) proposes negotiation strategies that mostly seek the construction of what we call Distributed Objects Communication Language (DOCL). Among other advantages, negotiation languages are helping the establishment of cooperative environment that successfully achieve multipart tasks and deliver refined services.

Scholars have also attempted to address the problem of enhancing multi-agent coordination by reflecting real human negotiation skills inside a computing environment [4], [5], [6]. These studies were mainly carried out because, 1) the need to construct a computing program that entirely acts on behalf of its operator has imposed the need to apply Agent-oriented concepts and theories. 2) The need to construct a cooperative computing program that automatically interacts with other entities to achieve complex tasks has raised the need for a proper negotiation language. These two reasons are forming together the need to

design the negotiating agents that are able to meaningfully interact, talkatively negotiate and mutually maximize their benefits.

In their book [9], J. S. Rosenschein and G. Zlotkin are doing what they call Social Engineering; they have dedicated part of their research on how designers of software agents would react to the development process of Multi-agent systems and, the use of certain design steps regarding the accomplishment of suitable negotiation protocol, which in return will lead to appropriate interactions among several MASs. They emphasized the urgent need to look at agents as the new era of human *surrogates*, and this is because of the nowadays speed taken to approach full system and machines delegation.

In Game Theory [12], a clear approach was taken to study the rational behavior among self-interested agents. Different software designers are working on the development of several software agents; these development processes will only produce an agent that is reflecting designer's personal behavior. Although the agents produced are self-interested and autonomous, they are going to interact with different agents that are designed differently and contain different level of autonomous performance and complexity. An agent that is rationally driven within a system entities will make goals and procedures to achieve them clear for all system actors, but it will apply an atmosphere of firmness and inflexibility in formed interactions. This earlier discussion has raised the confrontation of two important design aspects, would it be more appropriate to design an agent that is deterministic or an agent that is flexible?

When Distributed Artificial Intelligence (DAI) started to have its own structure as independent research area, Reid G. Smith has contributed significantly to this structure formation by having his PhD thesis defense, in 1978, discussing a new perspective in achieving proper negotiation and interactivity among multiple automated network-nodes. Later to that, an important contribution was added to literature regarding the same topic, which is Contract Net [10]. When applied to multi-agent systems, the Contract Net protocol assumes that each node in the network is an agent that is seeking another completer-agent that may, together, form a coalition to resolve a complex task. This coalition can yield some results that can not be achieved if each agent is operating separately.

When the exact rare resources are to be used by several agents, an Auction [8] is formed between these agents so that system resources are utilized at the highest possible value, and certain negotiation language that perfectly applies in this situation is used. Due to issues related to equality, ordering and planning, Auctions have gained a wide range of applications in multi-agent systems. Four major auction types that are widely recognized: 1) English, 2) Dutch 3) First-Price Sealed-bid, 4) Vickrey's Mechanism or Second-price Sealed-bid. These auctions are reflecting real human behavior in different auction styles and similarly apply it to agents.

6 Conclusions and Future Work

Negotiation protocols used among agents that are serving computer based applications differs from those used for computing pocket devices. We are rapidly approaching the era of lightweight device services, and as a result a great focus and immediate redirection is realized towards the achievement of cooperative agents in mobile-based service architectures. In this paper we explained the motivation behind our interests to find an appropriate agents' negotiation protocol that serves pocket-oriented applications. We demonstrated the research conducted in reaching cooperative MAS architectures, and the negotiation protocols previously proposed by scholars that mostly targeted fixed computing devices environments. We proposed our negotiation protocol, and we applied it on Rideshare service architecture.

Our future research will focus on increasing the usability of agent-based pocket service application, and accelerating the efficient delivery process of any mobile service content. We will work on integrating the newly proposed negotiation protocols to architectures that support lightweight devices. Eventually, we will simulate agents behavior in achieving complex tasks while applying different adaptive negotiation mechanism. This will help us observe differences in application performance and refine the proposed protocols. We also intend to study the possibility to make developers of pocket software agents able to a standardized but customizable negotiation protocol.

Acknowledgement

This work partially involves EU-SERENITY, PRIN-MEnSA, PAT-MOSTRO, PAT-STAMPS, and PAT UNIQUIQUE SUUM. We also thank ArsLogica for the unabated cooperation and support given to innovation.

References

1. M. Bombara, D. Cali, and C. Santoro. Kore: A multi-agent system to assist museum visitors. In *Proceedings of the Workshop on Objects and Agents (WOA2003)*, Pp 175-178, Cagliari, Italy.
2. V. Bryl, P. Giorgini, and S. Fante. Toothagent: A multi-agent system for virtual communities support. In *Proceedings of The Eighth International Bi-Conference Workshop on Agent-Oriented Information Systems (AOIS)*, Hakotade, Japan, May'06.
3. O. Bucur, P. Beaune, and O. Boissier. Representing context in an agent architecture for context-based decision making. In *Proceedings of the Workshop on Context Representation and Reasoning (CRR'05)*, Paris, France, 2005.
4. K.-M. Chao, R. Anane, J.-H. Chen, and R. Gatward. Negotiating agents in a market oriented grid. In *Proceedings of the 2nd IEEE/ACM International Symposium on Cluster Computing and the Grid*, pages 436-437, IEEE Computer Society, 2002.
5. Jennings, N. R., Parsons, S., Noriega, P. and Sierra, C. On argumentation-based negotiation. In *Proceedings of the IWMAS*, MIT Endicott House, Massachusetts, USA, October'98.

6. S. Kraus. Negotiation and cooperation in multi-agent environments. *Artificial Intelligence journal*, Special Issue on Economic Principles of Multi-Agent Systems, 94(1-2):79-98, 1997.
7. A. Rakotonirainy, S. W. Loke, and A. Zaslavsky. Multi-agent support for open mobile virtual communities. In *Proceedings of the International Conference on Artificial Intelligence (IC-AI 2000)*, Las Vegas, Nevada, USA, pages 127-133, 2000.
8. Kate Reynolds. A survey of auction types. Agorics, Inc., 1996.
9. J. S. Rosenschein and G. Zlotkin. *Rules of Encounter: Designing Conventions for Automated Negotiation among Computers*. The MIT Press, 1994.
10. R. G. Smith. The contract net protocol: High-level communication and control in a distributed problem solver. *IEEE Transactions on Computers*, C-29(12):1104-1113, December, 1980.
11. A. Sameh, F. Stefano and G. Paolo. Auctions Negotiation for Mobile Rideshare Service. In the *Proceeding of the Second International Conference on Pervasive Computing and Applications (ICPCA07)*, July'07, Birmingham, UK.
12. J. von Neumann and O. Morgenstern. *Theory of Games and Economic Behavior*. Princeton University Press, 1980.

Towards a Model Driven Development of Context-aware Systems for AmI Environments ^{*}

Estefanía Serral, Pedro Valderas, Javier Muñoz, and Vicente Pelechano

Departamento de Sistemas Informáticos y Computación
Universidad Politécnica de Valencia
Camí de Vera s/n, E-46022, Spain
{eserral, pvalderas, jmunoz, pele}@dsic.upv.es

Abstract. In this work, we introduce a software engineering method for AmI applications which is based on a model driven strategy. This method allows us to describe an AmI application a high level of abstraction by means of a set of models and then automatically obtain code from these models by following an automatic code generation strategy. To do this, a method proposed by authors in previous works is extended to support AmI applications properties. The introduced extensions are: (1) a set of models that allow us to represent the context information at conceptual level and (2) a strategy to allow the system infer knowledge in execution time to anticipate user actions and to adapt the system according to the context data. This method allows us to provide the development of AmI system with the benefits of using a software engineering method.

1 Introduction

Ambient Intelligence (AmI) is a new computing paradigm which tries to make reality the vision of Weiser [14]. AmI systems consist of mechanics, electronics, and software where the system intelligence is realized by software. AmI systems are in constant evolution of hardware and software which force these software products (AmI applications) to be highly evolvable and adaptable to different implementation technologies. The use of engineering methods is crucial to properly developing this type of software. However, current efforts in AmI are mainly focused on aspects such as the development of new implementation technologies, communication protocols or AI algorithms. AmI applications are usually developed by ad-hoc solutions, which make their maintenance and further adaptation or evolution difficult.

In this work, we introduce a software engineering development method for AmI applications which is based on a model-driven strategy [12]. Our main objective is to provide mechanisms that allow the developers to represent an AmI application in an abstract way (in a model) and then automatically generate (by a generation tool) the corresponding code. This method provides the development of AmI applications with benefits that are historically well known

^{*} This work has been developed with the support of MEC under the project DESTINO TIN2004-03534 and cofinanced by FEDER.

in the software engineering community: high productivity, high quality, quick adaptability, easy maintenance.

In order to obtain all these benefits, we extend the method for pervasive systems that is presented in [10]. This method provides us with: (1) PervML, a domain-specific modelling language for pervasive systems and (2) a code generation strategy based on the Software Factories (SF) [7] and Model Driven Architecture (MDA) [12] philosophies which obtain Java code based on an OSGi Framework [10]. To support the characteristics of an AmI application, we extend this method with:

- A set of models that allow us to represent the context information at conceptual level. By context information we mean information such as location information, user profiles, privacy and security policies, etc.
- A strategy that allows the system to infer knowledge from the context in run time. This allows the system to learn from people’s behaviour to adapt itself to better support this behaviour (for instance, by anticipating the user actions). We support this inference with an OWL-based ontology (which represents concepts such as user, action, location, service, etc) and a set of rules that analyses the descriptions defined by means of ontology concepts.

The rest of paper is organized as follows: Section 2 presents the development process proposed by our MDD method for AmI applications. Section 3 analyzes the concept of context information and gives an overview of PervML (the modelling language for pervasive systems). Section 4 introduces three new models which allow PervML to properly capture context information. Section 5 introduces the proposed strategy to infer knowledge from the user actions in run time. Section 6 introduces the related work about modelling methods and reasoning systems in the context of AmI. Finally, conclusions and further work are commented on in Section 7.

2 The Method for AmI Systems in a Nutshell

In [10] a method for the development of a software factory for building the core of AmI systems is proposed. This method applies the guidelines defined by: Model Driven Architecture (MDA), which is supported by the Object Management Group (OMG); and Software Factories, that is supported by Microsoft. Following these guidelines, the method provides (1) a modelling language (PervML) for specifying pervasive systems using conceptual primitives suitable for this domain, (2) an implementation framework that provides a common architecture for all the systems that are developed using the method, and (3) a transformation engine that translates PervML specifications into Java code.

In order to increase the expressiveness of the generated systems and to be able to develop context-awareness systems for AmI ecosystems, we have extended both PervML and the implementation strategy.

As Figure 1 shows, on the one hand, a set of models has been added to PervML that allows us to properly represent the context information (contribution

1). Therefore, the transformation engine that translates the PervML specifications into Java code of the context-awareness system for AmI can be applied. On the other hand, we have developed the PervML ontology, and have proposed a strategy to allow the system to infer knowledge from the context using the PervML ontology, in order to adapt the system to the needs of users (contribution 2). This strategy consists of automatically transforming the PervML models in OWL specification according to PervML ontology. The Java code keeps this OWL specification updated according to run time information. Finally, an OWL reasoner, which is integrated with pervasive system, is used to infer knowledge about system data in order to adapt the system accordingly.

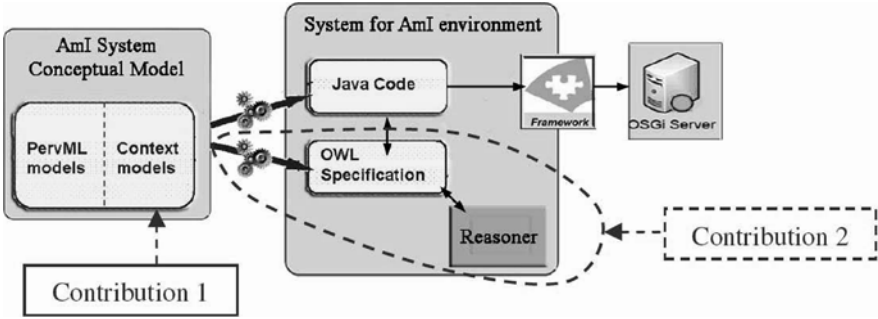


Fig. 1. Proposed method

3 Context Information and PervML

In this section we introduce both the concept of context and a brief overview of the main characteristics of the PervML models. Furthermore, we identify the context information that can be captured in these models and the context information that is not supported.

3.1 The Concept of Context

In this paper we consider that context is the state in which the system is, the relevant information that allows the system to react accordingly, making the system more productive and efficient. In order to identify this information, we have based on SOUPA ontology [6]. SOUPA is the most influential published ontology model for supporting knowledge sharing, context reasoning and interoperability in pervasive computing systems. It is frequently cited as a good example of pervasive computing ontologies too. Therefore, according to this ontology, the context information is made up of: 1) information about system users: name,

age, address, native language, etc.; 2) user preferences or attitudes, such as beliefs, desires or intentions; 3) space information; 4) services available to the user; 5) privacy and security policies that indicate what operations each user can execute; 6) temporal information: date and time, holiday, working day, etc.; 7) user mobility; 8) user actions: what the user is doing at present moment and what the user has done in the past. The actions performed in the past are necessary to predict the next action or to memorize and to reproduce scenes (repetitive sequences of actions within a certain time interval) at the opportune moment.

3.2 PervML

PervML [11] is a language designed to provide pervasive system developers with a set of conceptual primitives that allow them to describe the pervasive system independently of the technology. PervML promotes the separation of roles where developers can be categorized as system analysts and system architects.

On the one hand, systems analysts capture system requirements and describe the pervasive system at a high level of abstraction by using the service metaphor as the main conceptual primitive. The analysts construct three graphical models (the Services Model, the Structural Model and the Interaction Model), which constitute what we called the Analyst View. In these models, the analyst describes (1) the types of services that the system must support (by describing its interfaces, the relations among services and a state transition diagram which depicts the behaviour of each type of service); (2) the components that provide the identified services; and (3) how these components interact to each other.

On the other hand, System architects specify which devices and/or existing software systems support the system services. We refer to these elements (devices and software systems), as binding providers because they bind the pervasive system with its physical or logical environment. Therefore, the system architect constructs three other models (the Binding Providers Model, the Component Structural Specification, and the Components Functional Specification), which constitute the Architect View. In these models the system architect describes (1) the types of binding providers (by describing its interface), (2) the binding providers that are used in each component, and (3) the actions that must be carried out when each operation of each component is invoked.

Context in PervML From the point of view of context information, PervML only provides support for specifying the available services and the locations of these services, although it does not allow relate the different locations. Thus, context information is not properly considered by PervML.

According to the concept of context introduced in Section 3.1, we can identify two type of context information: (1) Those that is available when the system is being developed (when we are creating the PervML models) such as information about users, the user preferences, locations where the system is going to be deployed, privacy and security policies, etc.; and (2) those that is available in run time such as temporal information, user mobility and actions that users

perform. To properly model context: (1) PervML must allow us to specify all context information available in modelling time and (2) the code generated from this specification must provide support to handle run time information. Next, we explain the extensions introduced to support this requirements.

4 Including Context-Awareness in PervML

This section explains how context information is introduced in PervML. According to SOUPA, the concepts of users, policies and space information must be added to the system specification, which will be specified by the system analyst. In the next subsections we present the *User Profile Model* to specify policies, the *User Model* to describe the system users, and the *Location Model* to describe the spacial information.

4.1 The User Profile Model

This model has been introduced to specify behaviour and privacy policies. It allows the system analyst to create a policy that can be applied to a user or a set of users.

With this model, the system analyst specifies the types of user (profiles), indicating the service operations that are available for each one. Analyst associates a list of operations to each profile, which can be done in different ways: 1) by adding a service type so that every operation of every component that provide that service will be allowed; 2) by adding a component so that every operation of that component will be allowed; 3) by adding a service operation to allow this service operation to be permitted in every component that provide this service; or 4) by adding a component operation to be permitted this operation of this component is allowed.

Inheritance relations can also be established in this model to define capacities of a profile taking as a basis the capacities of a previously defined profile. We can do it in two ways: 1) By adding new capacities to the parent ones (the additional capacities are marked with “+”). 2) By removing capacities of the parent type of user (where the excluded capacities are marked with “-”). For instance, in the example of Figure 2 the type *father* can execute operations related to the services *Lighting*, *GradualLighting* and *BlindManagement*. The type *child* can execute the same operation except the operations of the *BlindManagement* service.

This model provides support for the privacy, the security and the views of the system, since users can see and execute only system actions that they are authorized to use.

4.2 The User Model

The *User Model* has been introduced to specify user information. It contains **personal data** (name, surname, sex, marital status, etc.), **contact information**

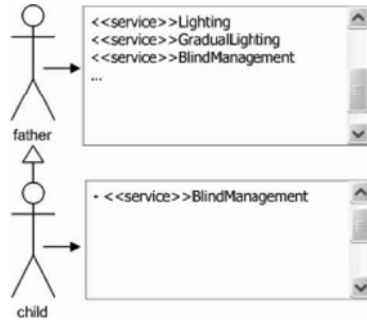


Fig. 2. User profile model

(email, mobile, telephone, direction, etc.) and **social relations** (information related to people that user knows). The analyst must indicate the policy that is associated to the user, which has been previously specified in the *User Profile Model*.

4.3 The Location Model

The *Location Model* describes the different areas where the user can move or where services can be located. It is specified by means of an UML package diagram. Each package represents a certain area, and the hierarchy between packages symbolizes the space hierarchy between the areas. Also, two types of associations can exist between the areas: adjacency and mobility (or accessibility). Adjacency means that the zones are one next to the other, whereas mobility is the possibility to go from one area to another. Adjacency is represented by a line between two areas. Since mobility implies adjacency, it is represented by adding arrows to the line between two areas.

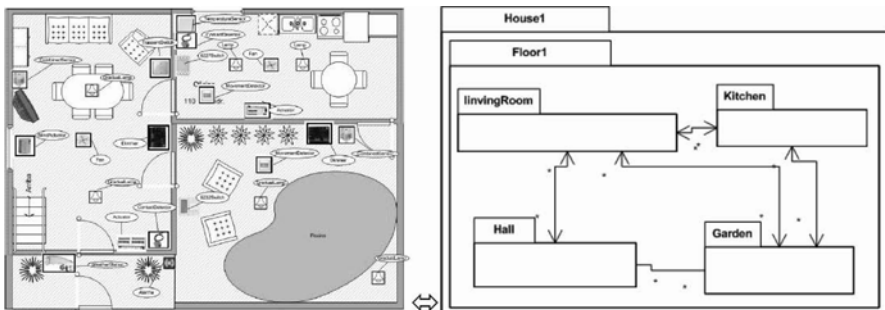


Fig. 3. Location Model of Floor1

Figure 3 shows an example of the Location Model. It models the locations of the first floor of a house that has four areas: Hall, LivingRoom, Kitchen, and Garden. The figure shows that, for instance, Hall and Garden are adjacent but a user can not go from one to another, however, Hall and LivingRoom are adjacent and user can go from one to another too. This model allows us to infer information such as transitive relations (for example, if the Kitchen is on Floor1 and Floor1 is in House1, we know that Kitchen is in House1). In the component structural model, each component is related to its physical location.

5 Extracting Knowledge from AmI Systems in Run Time

In this section, we introduce a strategy to extract knowledge from the pervasive system in run time. This strategy allows the system to infer knowledge from the context data in order to anticipate user actions and adapt the system according to the context data. To do this, all the information about the system is stored according to the PervML ontology in OWL.

5.1 PervML Ontology

The PervML ontology is detailed in this section through the description of the most important concepts, their properties and the relations among these concepts. We graphically show these concepts in Figure 4 by using the approach presented by Al-Muhammed et al [3]. According to this approach, two kinds of concepts can be defined: lexical concepts (enclosed in dashed rectangles), which represent the properties of each class; and nonlexical concepts (enclosed in solid rectangles), which represent the ontology classes. Figure 4 also shows a set of relationships among concepts, which are represented by connecting lines. The arrow indicates a cardinality of one and the non-arrow represents a multiple cardinality. The small circle near the source or the target of a connection represents an optional relationship.

For instance, the concept *Service*, which is the entity that provides a coherent set of functionality, is specified through its operations, its behaviour and its relations. As we can see in Figure 4, the properties that describe this primitive are: (1) Its name, which identifies it in the system. (2) The category to which the service belongs (illumination, multimedia). Figure 4 indicates that its *belongsTo* relationship is a many-to-one relationship. (3) The set of operations provided by a service. (4) A set of triggers which allows the specification the proactive behaviour of the services. (5) The valid sequence of operations, which indicates the operations that can be invoked at a specific moment. (6) Its general service, if it exists. (7) And the set of services that the service aggregates, i.e., the set of services that the service needs to work.

As far as the rest of PervML concepts, see [11] for detailed information. Additionally to PervML concepts, the PervML Ontology has a set of classes based on the concepts introduced by SOUPA to represent the context data. This set of classes includes *Person*, *Policy*, *Location* and *Action*. *Person* represents

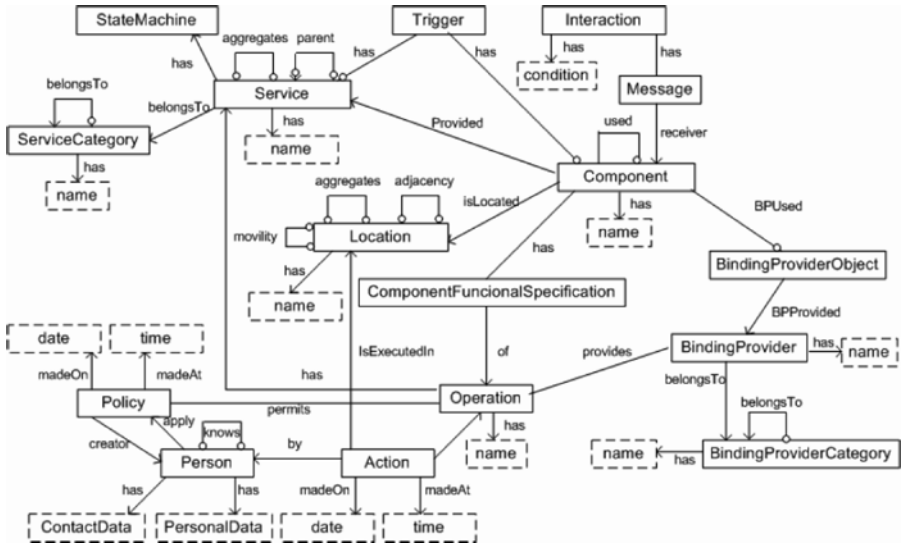


Fig. 4. A partial view of PervML Ontology

a set of the system users. *Policy* is a set of rules that is specified by a user to restrict or guide the execution of actions. *Location* represents the different environment areas. Lastly, *Action* constitutes the execution of an operation. Its properties are: the operation that is carried out; the moment in which the action has been executed; and the person who executes it.

5.2 OWL Reasoning Strategy

To reason about the system and to adapt it according to collected context data, we store all system data using the PervML ontology. This data includes both type of information identified in section 3.2.

On the one hand, in order to store all the information available at modelling time in OWL we transform the PervML models in OWL automatically. To do this we base on the fact that the tool [4] which supports the creation of PervML models is developed using the Eclipse Modelling Framework (EMF) plugin [1]. EMF is a modelling set of tools and code generation facilities for specifying metamodels and managing model instances. The PervML ontology has been developed using the EMF Ontology Definition Metamodel (EODM) plugin [1]. EODM is built on top of EMF and conforms to the ODM (Ontology Definition Metamodel) standard of OMG. Furthermore, EODM allow us to relate conceptual elements defined in the PervML models to the corresponding concept in the PervML ontology. For instance, we can indicate that each service define in the Service Model correspond to an individual of the ontology concept service. This allow us to obtain an OWL specification where appear classes (derived from

the ontology concepts, e.g. Service) together with individuals (derived from the PervML models, e.g. Lighting). As commented above, the OWL specification is automatically obtained by means of an ATL transformation taking as input both the PervML models and the PervML ontology. The Atlas Transformation Language (ATL) has been used since it can be integrated into the Eclipse framework and provides a model transformation engine.

On the other hand, the run time information is extracted by the AmI system from their interaction with users. When the context information changes the system creates the corresponding OWL description of this change by using the Ontology concepts. For instance, when users perform an action the system creates an OWL individual of the concept action (see Figure 4). This individual will be moreover related with other OWL individuals such as date, time, etc. (individuals from concepts related with the concept action see Figure 4).

In this context, the OWL specification, which is continually extended in run time, can be used by any OWL-based reasoner or inference engine, such as RACER [2] (which is implemented in Java), that infers additional and indirectly observable context data. In this work, the reasoning about individuals is the most important since it deduces knowledge such as locations where a person can go or even to predict the following action of a user based on previously executed actions. The reasoner must be integrated into the AmI system and it can use rules that we can define by using, for instance, a declarative language like the one shown in the code above (Prolog). Using the next rule the system can infer where Peter can go from his current location.

```
Mobility(SittingRoom, (Kitchen, Garden, Hall))
IsLocated(Peter, SittingRoom)
Where_can_go (X, L) <- IsLocated(X,Y), Mobility (Y, L)
Peter can go to Kitchen, Garden or Hall
```

6 Related Work

This section presents an overview of context modelling and reasoning systems that model context using ontologies. The architecture of the Context Managing Framework (CMF) presented by Korpipaa et al. [9] is comprised in four main functional entities: the context manager, the resource servers, the context recognition services, and the application. The ontology structure and vocabulary applied in CMF are described in RDF. CoBrA (Context Broker Architecture) [5] is an agent based architecture that supports context-aware computing in intelligent spaces. CoBrA has adopted an OWL-based ontology approach, and it offers a context inference engine that uses rule-based ontology reasoning. The SOCAM (Service-oriented Context-Aware Middleware) project introduced by Gu et al. [8] is another architecture for building context-aware mobile services. SOCAM divides a pervasive computing domain into several sub-domains and then define each sub-domain in OWL to reduce the complexity of context processing. SOCAM has also implemented a context reasoning engine that reasons over the knowledge base. According to the study made in [13], ontologies are the most expressive models and best fulfil system requirements. But, none of these

works attempts to model context and reason about it by applying the MDA and SF guidelines. Besides, none of them set reasoning out from the point of view of OWL individuals in order to infer relevant data from pervasive systems and adapt this behaviour accordingly.

7 Conclusions and Further Work

In this work, we have presented a model driven method for AmI applications which automatically generate context-awareness AmI systems from models. We have extended the method for pervasive system proposed in [10] by introducing:

- A set of models to properly represent the context information at conceptual level. These models describe information related to location aspects and behaviour policies, as well as to the system users.
- A strategy to infer context knowledge in run time. This strategy is based on OWL-based ontology that represents concepts such as user, action, service, etc., and a set of rules that inferring knowledge from context data.

As further work, we plan to 1) extend the expressiveness of PervML to support modelling beliefs, desires and intentions; 2) specify and implement the rules for automatically transforming the new Perv-ML models in java code; 3) adapt automatically the system according to context data and 4) develop cases of study for context-aware systems for AmI environments.

References

1. <http://www.eclipse.org>.
2. <http://www.sts.tu-harburg.de/~r.f.moeller/racer/>.
3. M. Al-Muhammed, D.W. Embley, and S.W. Liddle. Conceptual Model Based Semantic Web Services. *Proceedings of the 24th International Conference on Conceptual Modeling (ER 2005)*, 3716:288–303, 2005.
4. Carlos Cetina, Estefanía Serral, Javier Munoz, and Vicente Pelechano. Tool support for model driven development of pervasive systems. *Fourth International Workshop on Model-Based Methodologies for Pervasive and Embedded Software (MOMPES'07)*, 0:33–44, 2007.
5. H Chen. *An Intelligent Broker Architecture for Pervasive Context-Aware Systems*. PhD thesis, University of Maryland, Baltimore County, 2004.
6. H. Chen, Tim Finin, and A. Joshi. An ontology for context-aware pervasive computing environments. *The Knowledge Engineering Review*, 18(03):197–207, 2004.
7. Jack Greenfield, Keith Short, Steve Cook, and Stuart Kent. *Software Factories*. Wiley Publishing Inc., 2004.
8. Tao Gu, Hung Keng Pung, and Da Qing Zhang. A middleware for building context-aware mobile services. *Vehicular Technology Conference, 2004. VTC 2004-Spring. 2004 IEEE 59th*, 5:2656– 2660, 2004.
9. P. Korpipaa, J. Mantyjarvi, J. Kela, H. Keranen, and EJ Malm. Managing context information in mobile devices. *Pervasive Computing, IEEE*, 2(3):42–51, 2003.

10. Javier Muñoz and Vicente Pelechano. Building a Software Factory for Pervasive Systems Development. In *17th International Conference CAiSE 2005, Porto, Portugal, June 13-17*, LNCS, pages 329–343. Springer-Verlag GmbH, 2005.
11. Javier Muñoz, Vicente Pelechano, and Joan Fons. Model Driven Development of Pervasive Systems. In *I International Workshop MOMPES*, pages 3 – 14, June 2004.
12. Object Management Group. Model Driven Architecture Guide, 2003.
13. T. Strang and C. Linnhoff-Popien. A Context Modeling Survey. In *Workshop on Advanced Context Modelling, Reasoning and Management as part of UbiComp 2004*, 2004.
14. Mark Weiser. The Computer for the 21st Century. *Scientific American*, 265(3):94–104, Sept. 1991.

Taking Ownership of Computational Resources

Alain Rhelimi

Technical Advisor GEMALTO. France.
alain.rhelimi@gemalto.com

Abstract. Today users are faced with a wide variety of access methods to computational resources. These methods may include the use of different devices. In this paper we present a new type of devices, called eGo (ego: latin root expressing "me"), capable of providing a uniform, flexible and secure way to access such services. Furthermore, these devices allows users to take ownership of services and other devices in a natural and transparent way: by touching them.

1 Introduction

In order to get access to various services, all of us are using personal devices which may come with different form factors. For each provider of service and according to the nature of such services, the right device has to provide specific features convenient to carry and communicate the credentials needed. For example a bus ticket is a service-device issued by a mass transit operator, a SIM card is another device carrying credentials coming from your Mobile Network Operator, a banknote is a vector for a government for monetary exchange and your key is a tool to open the door of your flat.

In the first example mentioned, it is fair to observe that a bus ticket is not a secure device. It is cheap, portable, disposable, and the credentials are often limited to one trip. In the second case, the credentials are more important since they open the gate to access to multiple services (e.g. phone calls, SMS, Internet access,...). That may translate into a financial commitment for the end-user. Consequently, the SIM card is portable, non disposable, secure and much more expensive than the bus ticket. The value of the banknote is limited by nature to the amount printed on it, but the protection of the banknote is sophisticated and complex enough and to prevent counterfeiting. The last example: the door key, is a device aiming at protecting your privacy, your safety and your valuables.

Our whole environment uses multiple vectors of services, some as simple as a password to access a PC (conditional access), some more sophisticated like memory cards to carry, for example, the pictures we care for.

What are the different attributes we see in such devices?

- Portable: obviously the services may be anywhere and we need to carry our credentials anywhere with us.
- Connected: The vector of service must be able to communicate with a wider system that participates in the complete transaction.

- Secure: the credentials must be protected (i.e. available only to the person(s) they were initially intended for). They must also be impossible to clone.
- Non repudiable: The vector of service may complete a transaction without any risk of repudiation of service from its original user.
- Capable of data storage: The vector of service may need to carry large amounts of data (e.g. pictures, emails with attachments) which may be private, public, protected, verifiable (i.e. your driver license).

All of these features clearly remind us smart cards attributes... but with some important differences.

2 Envisaged application scenarios

The purpose of the Ambiance Intelligent project is to simplify all basic accesses to services in a natural and well organized manner, in order to just make it seamless. Therefore the concept of vector of services is clearly one key element of its foundation in order to carry the end-user's credentials to use those services.

Each service is related to a service-provider managing its network and its users/ customers relationship. Having a unique portable device emulating multiple vectors of services sounds like an attractive idea but it clearly introduces several complex challenges, the main one being sharing a customer base between multiple service providers. The concept has been thought for a long time and is technically feasible thanks to multi-application smart cards. However the complexity of the business model of such shared credential management solutions has long prevented its deployment. The missing concept until now to enable such a new route is the notion of "aggregator of services".

The aggregator of services is definitively the most important component/actor of the Ambiance Intelligent project to federate multiple service providers. In other words, your services aggregator is your personal assistant to contact other parties to carry your credentials into your global vector of services.

The business model behind the service aggregator concept is the concept of brokerage of services. The service aggregator is a broker able to negotiate massive discounts and facilities due to the large volume of transactions under his management. The negotiated services are retailed to the end-user who gets a discount compared to dealing with the prime service provider directly.

On the one hand, the role of service aggregator can be played by any organization having a wide installed base of customers/users such as banks, Mobile network Operators, insurance agents, universities, governmental organizations. The model could be pyramidal in the way that we may have an aggregation of service aggregators.

On the other hand, it is also possible that it is the end-user himself who may aggregate multiple service aggregators and may administrate the service providers.

2.1 Example use cases

Let's move from the conceptual approach and go into practical use cases.

- Alice enters in a movie theatre, takes a seat, enjoys the show and leaves the theatre. At no point in time Alice purchased a ticket or gave any money to any teller.
- Bob arrives in the airport, looks for the parking lot for cars rental. Bob goes to the information billboard. A personal instantaneous welcome message provides him with all necessary information for him to find his car. Bob goes to the parking lot, opens the door, starts the engine and leaves the lot. At no point in time, Bob received a car key from anyone, nor was asked to fill in a form.
- Because she forgot to take her own phone, Julie borrows a cell phone from an unknown person she meets in the street. Julie selects the phone number of her husband in the handset phonebook, calls him and sends him an e-mail. At no point in time, Julie has inserted a SIM card in the handset, nor entered any private information in the handset; the unknown person who accepted to let Julie temporary use his phone will not pay for Julie's calls or Julie's e-mails access.
- Steven enters the subway network and leaves two train stations later. At no point in time Steven purchased a ticket , nor waved a contactless card to a entrance gate.
- Xavier walks on the beach and thinks: "God, the sunset is so nice!". Xavier borrows a digital camera from someone passing by, takes nice pictures, gives back the camera to its owner and finally thanks him for his kindness. Later on Xavier switches on his personal computer, clicks on the eGo icon on the PC desktop and drags and drops the nice pictures he took on the beach. At no point in time, the pictures have been stored in the digital camera. The camera's owner and Xavier never exchanged any information.
- Xavier selects some pictures on his PC photo album and drops these into the "favourite pictures" directory of his eGo. Later on, Xavier arrives in his office and touches the digital poster on his desk, instantaneously the first picture of the eGo favourite pictures directory appears. Oops! The picture is not the right one so Xavier touches several times the digital poster and each time a new picture appears.
- Axel is three years old and today it is a great day for him because he is going with his mother to his favourite place: the shopping mall. Axel likes this shopping mall because there is a large toy store. While Brigitte, his mother, is busy with a teller, Axel disappears and rushes to the toy store on his own. Five minutes later Axel is lost and his mother and him are looking for each other. Brigitte goes to the information panel and quickly a map is indicating Axel's exact location and a window on the panel shows a video showing Axel close to the toy store.

As you understand by now, the common point between all these use cases is that, in the most natural manner and without any specific user education nor

any specific devices, Services were made available and personalized to those individuals. Taking ownership of a Service means installing your credentials, for the duration of the usage of such a service. All in a safe, simple and portable way. This is where the eGo concept comes in.

2.2 A new Service-oriented business model that fits the way we live

The use-cases described above all illustrate situations where an opportunity of service was created by simply removing all the barriers, often driven by the requirement to use a pre-configured device, between the need and the user: “I forgot my cell phone today” so never mind, “I will call later, or not at all”. Such barriers are often materialized by highly personalized objects that do perform the service for us in a unique and secure manner... except when we do not carry them with us at all time.

The most obvious example to describe this model and the need for a new business model is the PC market: Until now, we have seen several products serving various needs we may have: Desktop PCs bring performance and comfort of use at home and in the office. Laptop PCs try to enable desktop-like performance on-the-go. Laptops PCs are more expensive and somehow limited performance-wise compared to Desktop PCs. It would be easier if public-PCs were available at the corner of every street and every office with a way to rebuild our very-own “desktop”. Nothing like Laptops would then be theoretically useful any longer (or a least far less needed). It is a fair assumption to assume that consumers will always come across situations where “they would have used a given service” if they had had (carried) with them the enabling-device to access such a service. By creating a footprint of “blank products” that are easy to temporary (and securely) personalize with the User’s credentials, data and application profile, there is a potential to boost the usage of a given service by reducing the level of non-availability due to “logistics” reasons.

Ultimately consumers should be able to travel, commute, hang around with their hands in their pockets and without the worries of performing a complete checklist before living their home or their office (did I take my cell phone?, my PC?, my credits cards?, my healthcare card?, my ID document?, etc...) Let’s admit that with the quick rise of the Digital world of services, the chance to fail the checklist is converging to 100%.

2.3 Everything I touch is (temporarily) mine!

Let’s take the business model of GSM phones. For a given Subscriber base, each subscriber gets a SIM card to materialize the service offered by his/her Operator. This Operator wants:

- to keep the customer happy and retain him/her,
- to offer more services (voice, data, entertainment) to deliver more value therefore obtain more revenue for each subscriber.

Whenever a Subscriber places a call from a land-line phone in his hotel room for example, or any other phone service, this is lost business for the Operator.

The Operator can do two things to re-capture that lost revenue:

- Explain to his customers that in all cases calling from your GSM phone is more valuable than with any other method.
- Capture the business of this land-line phone in that hotel room and bring it back inside the framework of the GSM contract that binds him to his customers.

By installing a network (with hotels, public spots) of “touch-and-use phones” that literally operate GSM-like service, the Operator can serve the needs of all his customers, even the one who failed their checklist and accidentally left their phones at home.

This Touch-and-Use business model is a solution (and business booster) for three reasons:

- It offers an “accident-free” coverage of service for already registered subscribers that may have failed their checklist and accidentally forgot their credential-enabler devices.
- It stimulates pre-paid models for service-trials for consumers who are not yet registered subscribers for a given service.
- It competes against alternative services that may have a “context-given advantage” that is hard to compete (example: A land-line phone in an hotel room brings more comfort than GSM).

3 The eGo concept

The eGo device inherits most of the smart card features but the form factor (e.g. a watch, a ring, a belt, a shoe,...) is definitively different and two wireless communication means are provisioned:

- Ultra short distance and low speed: as illustrated in Figure 1, the first communication channel uses the human skin as a communication medium to carry an unidirectional small bundle of data from an eGo compliant device (e.g. a gun, a door handle, a digital camera, a handset, a car,...) to the eGo device carried by the end user. The operating distance to perform this contactless communication is much shorter than a millimetre and the data rate is as low as a single kbit/s. The communication channel required an ultra low power transceiver and is permanently activated.
- Short distance and ultra/high speed: the second communication is bidirectional and provides high data rate (ten to hundreds MBit/s) on a short distance (less than 3 m). The perfect candidate is the UWB but less power hungry interfaces such as Wibree or Bluetooth which could be convenient.

The first communication channel is used to bootstrap the second one. The goal is to establish a virtual and private channel of communication over the second

channel of communication between the eGo device carried by the user and an eGo compliant device (e.g. an handset). The connection is established when the user touches (via her hand, a finger,...) explicitly the aforesaid eGo compliant device. What you touch is what you own; that could be the slogan to illustrate eGo.

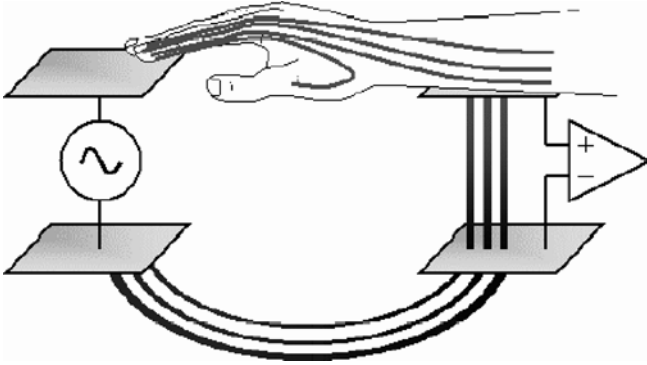


Fig. 1. Ultra short distance over-skin communication channel

3.1 System functioning

The eGo compliant device periodically sends a code able to be carried over the skin [1]. The code could be a pseudo random generator having a long sequence (e.g. 64 bits). The code is collected by the user's eGo (working in a permanent listening mode). Such a receiver is easy to design to expose ultra low power capability and most probably has no impact on a health level because no signal is injected in the user's body. The Over Skin Communication receiver wakes up the wireless transceiver (UWB, Bluetooth, Wibree, Wireless USB,...) which opens a Secure and Private channel (equivalent to a VPN) in using the received code as a session key. As soon as the code is consumed to establish the VPN, the eGo compliant device generates a new code.

Only two eGo devices connected via the skin of the user may establish a (RF) wireless VPN. This is another way to pair two RF capable devices in using a natural and explicit connector: your hand. The settlement is obvious and explicit through a natural gesture that can be compared to a hand shake.

The system does not suffer drawbacks related to contactless based devices such as the relay attack in implementing easily protection like time based protocol [2] to check the proximity of the end-user and the final eGo compliant device. Moreover, a convenient form factor may allow the embedding of huge memory comparable to the usual USB dongle key and having a comfortable throughput up to hundreds Mbit/s to reach a good user experience.

Well, we have a convenient principle to pair two devices but how is the eGo device carried by the user paired with the user?

Obviously without a pairing between the user and his/her eGo device, anyone may use the credentials of anyone just in carrying an eGo device. To bypass this issue, an eGo device embeds two functions for respectively authenticate the user to emulate a pseudo login and to monitor the presence of the user to emulate a pseudo logout. The user authentication may be based on a biometric sensor (e.g. fingerprint sensor) and the user's monitoring based on a heart pulse sensor. So when the user wants to activate her eGo device, the authentication process is required until the eGo device is carried by the user.

The user's authentication may be asked during specific transactions (e.g. a payment) mandating a non repudiation operation. Additionally, a periodic authentication may be programmed to bypass some security issues, for example a malicious person may ask a user to activate the eGo device after its installation on a malicious person.

The architecture of eGo is depicted in Figure 2.

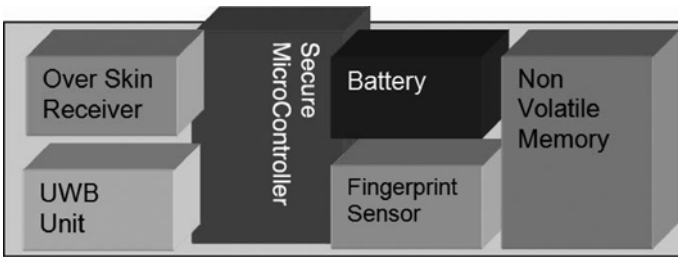


Fig. 2. eGo architecture

3.2 Limitations of the eGo system

Due to the nature of the initial communication channel using the intra-body communication, the bootstrapping may fail if the user's body is short to the earth. Consequently, a user walking barefoot on a conductive floor connected (about 12 dB attenuation if the eGo device has a watch form factor) to the earth may disable the intra-body communication. Of course due to the previous drawback, the system may not work properly in the water.

4 Conclusions

All technologies involved in the eGo system are available off-the-shelf. The global infrastructure is the only part missing. Nevertheless, an eGo based application may start from a limited and local organization (e.g. a school, a company or your

home) and progressively spread into other eGo applications. This seed phase is the one of the current NFC technology and the main concern we may face in the future is the standardization of heterogeneous installed bases which may have been rolled out in the meantime. Some famous innovations have been inspired from popular writers, so the portable GSM handset possibly comes from the very well known Star trek saga (the communicator). The eGo concept has been inspired from a novel written by René Barjavel namely “La nuit des temps” (A.K.A The ice people) where people used a ring to access all services.

The eGo applications may cover many aspects of our daily life, the limit is our imagination. eGo reinforces the fact that objects are just objects. What makes a service is a combination of us, our identities, our needs, our knowledge and the help of smart objects. There is no need to own a phone, there is just a need to place phone calls. eGo will help people not to be limited in their daily lives by the absence of a particular object, by a particular piece of data or by the knowledge of any fuzzy secret (like a password for example).

References

1. Thomas Guthrie Zimmerman. Personal Area Networks (PAN): Near-Field Intra-Body Communication. Master Thesis. Massachusetts Institute of Technology. September 1995.
2. Jason Reid, Juan M. Gonzalez Nieto, Tee Tang, and Bouchra Senadji. Detecting Relay Attacks with Timing-Based Protocols. In Proceedings of the 2nd ACM symposium on Information, computer and communications security. ACM. 2007.

Bluetooth Indoor Positioning and Ambient Information System

Karim Khalil^{1,2}, Hiroshi Mizuno¹, Ken Sasaki¹, Hiroshi Hosaka¹, and Pierre Maret²

¹ Dept. Of Human and Engineered Environmental Studies, Graduate School of Frontier Science, University of Tokyo 5-1-5 Kashiwanoha, Kashiwa-shi, Chiba-ken, 277-8563 JAPAN

² Dept. Informatique, LIRIS, INSA Lyon, 21, Av. Albert Einstein, 69100 Villeurbanne, FRANCE

{ksasaki, hosaka}@k.u-tokyo.ac.jp,
{kkhalil, mizuno}@ems.k.u-tokyo.ac.jp,
{karim.khalil, pierre.maret}@insa-lyon.fr

Abstract. Our system utilizes signal strength of Bluetooth wireless connection for indoor positioning. The position of a user carrying an information device equipped with Bluetooth, e.g. a mobile phone, will be estimated from signal strengths measured by base stations, e.g. desktop PCs in the rooms. One of these base stations will serve as a position server that collects signal strength measurements and calculates the user's position. Using the indoor position as context information, we created a guidance system on our campus which gives relevant information according to the position and to the user's goal or task.

1 Introduction

Recently, Information Systems are a more and more important subject of research due to their usefulness, in all situations and every day life. Thus more and more Information Systems are under creation in order to give people information to make life easier, to achieve a goal or just to get informed.

AmI ecosystems being naturally very unpredictable require applications and system capable of rapid responses and dynamic replies to context changes. Systems that help in the context management are thus a major element for AmI applications. Lot of technologies nowadays allows to get outdoor position of people (like GPS, PHS...) and to give context information according to that position. Still, very few systems are using an indoor positioning system as a base for their context source. However, a person spends much more time indoor than outdoor. Then using an indoor positioning system can be fully used almost everyday and time for a person. It would give useful information about the context.

1.1 System's goal

The actual society is more and more based on information. Our system focuses on the context information and particularly on a person's indoor position. According

to that indoor position, we provide information that might help users in many ways about the environing context and places.

Indeed, using a Bluetooth connection as basis, our application gets user's indoor location by measuring the connection signal (as long as the user is equipped with a mobile station) and provides information according to that position.

1.2 Different locating principles

As already explain the locating system is based on a Bluetooth signal measurement. To perform that Bluetooth connection, we need base stations and mobile stations. We use different devices as base/mobile station. We will now explain in this paper the specification of them.

2 Bluetooth Indoor Positioning

The Bluetooth indoor positioning system allows the measuring of the users' indoor location thanks to a Bluetooth connection.

Indeed a Bluetooth wireless connection takes place in-between bases stations and the mobile station the user is wearing. From the signal strength of those wireless connections, we can estimate the user position.

2.1 Base Station

The Bases Stations represent places. They are thus placed at some strategic places and are fixed. They are used as bases for the calculation of the position of the mobile station. When a user brings his/her mobile station in the covered area of a base station, a connection takes place between that mobile station and the base station to measure the distance of the mobile station from the base station. We have performed experiences with 2 kinds of base stations: our developed device (Fig.1) and computers.

2.2 Mobile Station

The Mobiles Stations represent users and persons. They are constantly transported by the persons and their locations are thus considered as the persons' locations.

In order to have a mobile station's position, a Bluetooth connection is performed with all accessible bases stations. According to the distance between the mobile station and all bases stations, we can estimate its position. We performed experience with 2 kind of mobile station: our developed device (Fig.1) and mobile phones.

2.3 Principle

When a user enters a service area covered by the system, base stations installed in the area will connect to the user's mobile station and will measure the signal strength, which is ideally proportional to the inverse square of the distance.

By using the three-point method, we can calculate with some certain accuracy the exact position of a person. The three-point method is possible only by placing bases stations a way that at any point of the covered area there are at least 3 bases stations that cover the place. Thus estimating distance from each the bases stations we can estimate location of the mobile station. Tests with our developed device (Fig.1) proved that the positioning accuracy goes actually up to 1.2 m with one base station placed every 8.3 m².

When the user is outside the service area or simply outdoor, then the positioning could be done through GPS by using these mobile phones.

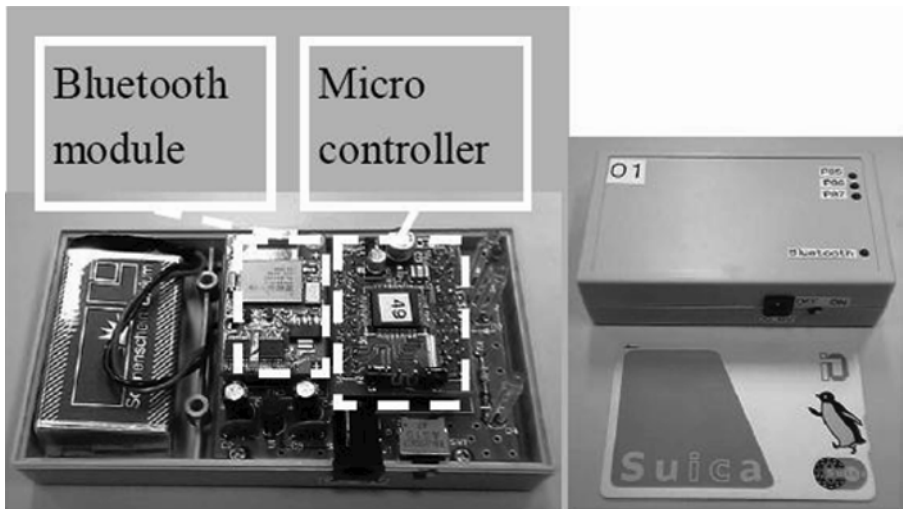


Fig. 1. Our developed device used as both Base and Mobile Station

For the positioning, we developed a device using the Zeevo³ Bluetooth module (Fig.1) that could stand both for a Base Station or a Mobile Station. That device is composed mainly of a Bluetooth module for the connection and a micro controller to program it.

Preparation for the Base Station side is as follow:

- Reset the module

³ Zeevo, Inc (actually Broadcom) was a semiconductor company focused on 'system-on-a-chip' solutions for the communications industry.

- Configure it so that it accepts Bluetooth scans from other devices (have to configure the scanning setting, like connection timeout...)
- Begin scanning the area and send connection request to entering Mobile Station

For the Mobile Station side, beginning configuration are basically the same. The main difference is that the Mobile Station accepts connection.

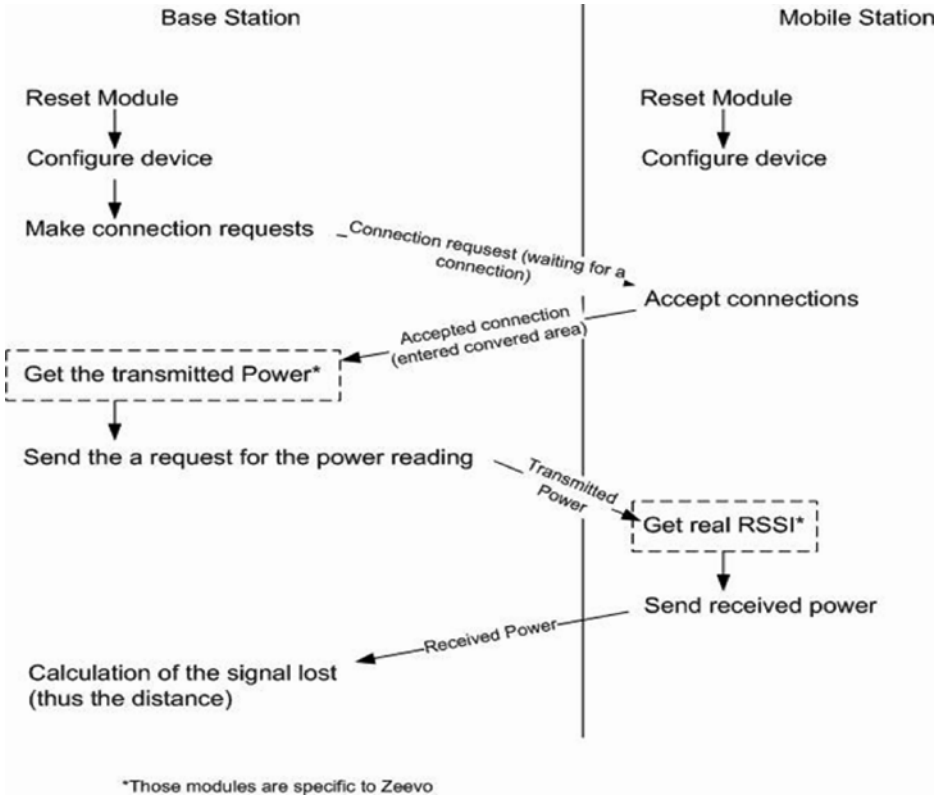


Fig. 2. Connection between Base and Mobile Station

- The Mobile Station accepts connection attempt from the Base Station and sends a notification message.
- The Base Station calculates the transmitted power and sends it to the Mobile Station⁴
- The Mobile Station calculates the absolute RSSI (Received Signal Strength Indication) and sends it back to the Base Station.

⁴ Those steps are specific to our developed device and are thus not performed during computer/mobile phone connection.

- From the power lost, the Base Station calculates the distance of the Mobile Station.

For the mobile phone and computer connection, we can not calculate the connection power, but instead the mobile phone gives an indication of the connection status. According to how good the connection is, we can estimate the connection power.

2.4 Mobile Phone and Zeevo technology comparison

Our developed device is programmed to be used only for the Bluetooth Indoor Positioning. We thus made it to have the transmitted power (base side) and the received power (mobile side). The Zeevo developed Bluetooth module has a linear response according to the transmitted power (Fig.3 left side). However, the real usability of the system pushed us to use a normal mobile phone instead of our developed device. Indeed, a mobile phone is a device that almost everyone owns and everyone wears it all the time. It is thus a much more realistic device to use as Mobile Station.

In that mobile phone case, we used computer as the Bases Stations.

As mentioned before, the main difference between the mobile phone and Zeevo is the way to calculate the connection strength. Indeed, Zeevo gives a direct value of the connection strengths, whereas the mobile phone goes like the normal Bluetooth standard and gives only a status indication of how good the connection is. Basically the mobile phone returns a number as indication: a negative numbers is a bad connection situation, a positive numbers is a good connection situation and finally zero is the normal connection situation. This is the main issue with the mobile phone, which returns for normal connection condition zero. In fact, the mobile phone has a large zone of connection that it considers as being normal (Fig.3).

This makes the Mobile Phone precision much less good, as we can't make any differences for the entire zone where the signal power is considered to be normal. We thus have uncertainty about the exact location in the Mobile Phones' case, but we still have a global region where the user is positioned.

3 Information System based on the Indoor Location

Using the context information obtained from the Bluetooth Indoor positioning system, we created an information system which purpose is to guide users on our campus and to deliver some information about the campus' inhabitants.

The main goal of that information system is indeed to guide users on the campus. It would provide them with information on places and also information about persons present at those places, or about regular inhabitants of the place and their actual positions.

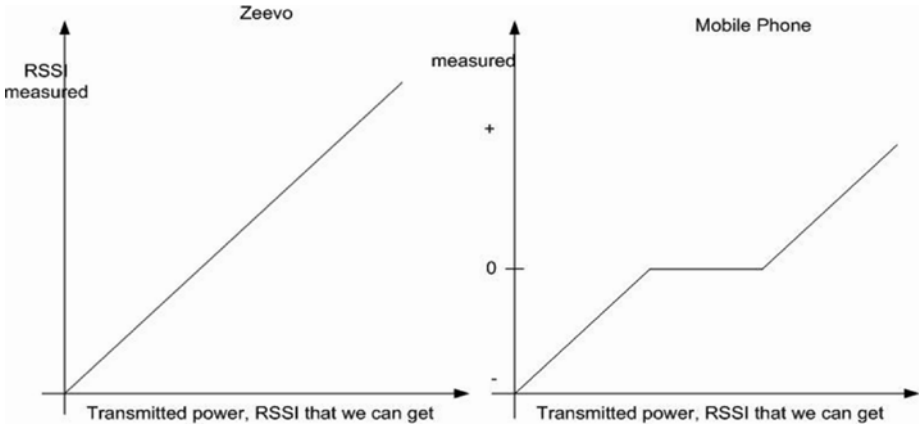


Fig. 3. Comparison of the Mobile Phone and Zeevo’s signal strength

3.1 System’s Architecture

The whole system is divided into 4 main units:

- The Bluetooth Indoor Positioning System, used for the location of users through Bluetooth connections.
- A database, where diverse information is stored (such as the users’ data, places, ...).
- A web server that receives different requests from clients and communicates with other units in order to provide the clients (users) with replies (information). This unit is the only one having access to all other units.
- The clients are the users. They get access to the system by using their mobile station or computer.

The Bluetooth Indoor Positioning System is equipped with a presentation server, thus a simple access through internet allow asking directly for the actual position of a user. The database contains following information:

- First of all, the profile of every registered user. Indeed, the system is at the moment focused on information about places and peoples of the places. Thus users’ profile is mandatory, if we want to give detailed information about every inhabitant of a particular place. Beside, without a fully updated profile, the system would be unable to locate users.
- Information about base stations’ position. The position of a user is detected thanks to the Bluetooth connection between their mobile phone and a base station⁵. Thus positions correspond to base stations’ positions. It is then necessary to have some information about these places (in our example:

⁵ We consider in this system that the user’s global location is sufficient. Thus we use the mobile phone and we don’t use the three-point method.

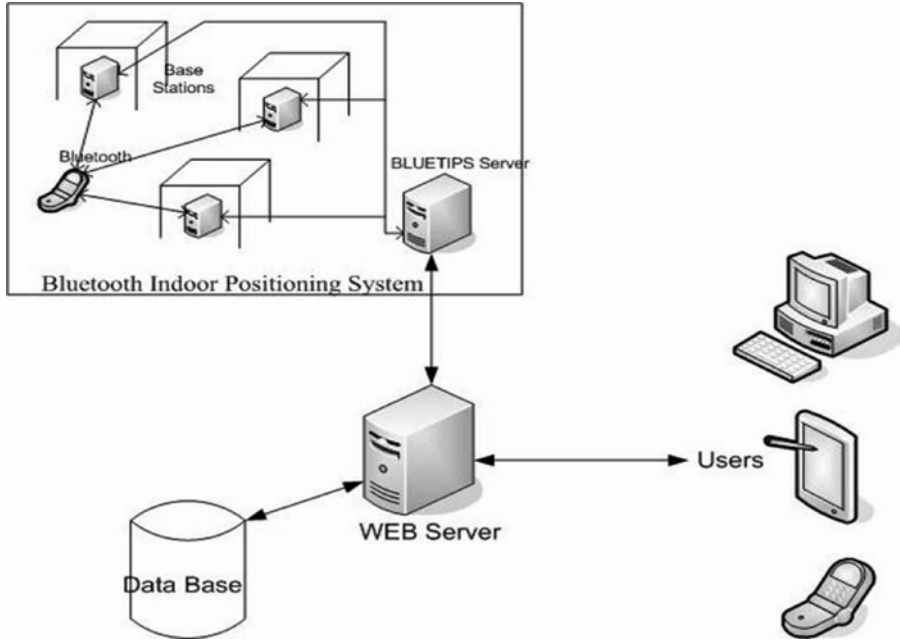


Fig. 4. Global Architecture

descriptions, kind of place, what happens there and what kinds of persons are normally there).

All services are provided by the Web Server. Clients access to the system by using any web browser (thus a mobile phone, a computer, a Personal Digital Assistant...) and they send their request to the Web Server.

3.2 Provided services

First of all, in order to ask for any services, the user must be logged into the system. In fact, many of the services (almost all) depend on the user's location. To get the users' location we need his/her mobile phone's Bluetooth ID, which is stored in the user's profile.

Overview the location

After entering into the system, the user is directly on the overview page, where the system updates the user's actual position. On that page, the user can see the name of the place he/she is actually as well as the names of the inhabitants of that place and if they are actually present or absent.

By just approaching another place, the user will receive basic information:

- Name of the place - User can then check position and keep informed of where he/she is;

- List of Inhabitants - Who are the person normally here. That's especially useful when the user is looking for someone.

From the overview page, the user can access others services.

- For each inhabitant, the user can get full detailed information about that person (mainly the profile and actual location).
- The user can get full detailed information about the place. Indeed, when user found a place that attracts his/her attention, he/she can get more information about that place.
- The user can get access to the research tool.

Research tool

The user can get access to this service from the overview page. Through this research tool, the user can search for a particular user within all the system. The research tool is done to take into account different criteria of selection, and would provide a list of persons corresponding to the desired criteria. For every person found there are some information for the user to identify the right person.

From that tool, user either can go back to the overview page of actual position; either can get an access to full detailed information on a person. Indeed for every returned person, a link is attached to allow easy access to the full detailed information (see the corresponding service for more information).

Place's and inhabitant's information

This service is accessible through the overview page of the place or while looking for the location of a person (from the person full detailed information). If the user is interested in a specific place, then this service will provide him with more information concerning the place.

User gets first of all a full description of the actual position (what kind of place it is, its use and purpose) and some pictures, videos and access plans of that place. The system also displays information about registered inhabitants of the place. Contrary to the overview page, this service provides little information about inhabitants of the place. Thus all inhabitants' information is displayed for a period of 10 seconds before changing to another one. The displayed information is the person's basic data, the person's photo and also that person's actual location. From this page, the user can also ask for detailed information on a given person.

This is a useful service, as it gives detailed information on the actual place as well as information about inhabitants and their real time actual location.

User full detailed information

This service is accessible through many ways and is used to give full information on a user registered in the system. Through it, the user can view information about a person. Displayed information is: age, address ... but also photos, videos of that person. Detailed information about the person location is also displayed.

This service allows the user to get a person's profile and also to know exactly where this person is actually. From this page, the user can also access detailed information on the place actual place where the person is located (a map for instance).

4 Other uses of the indoor position

Working on the field of human behaviour studies, we also worked on using the indoor location as a tool for recognizing human behaviour.

4.1 Behaviour recognition

Using different sensors for capturing the user's context we can also recognize his/her behaviour. This process can be enhanced in using also the indoor positioning system (as another context sensor). As an example let us consider the user is sitting . If we do not have any further information on the user, we are in a situation where we can't recognize or guess anything else. However, considering that the user is sitting in his/her office in front of the desk, allows us to guess that he/she is working. Considering that the user is sitting in a meeting room allows us to conclude that he/she is attending a meeting.

The indoor position also can allow inferring more detailed information about the user's behaviour. For example, behaviour of a user sitting⁶ in his/her office might be with great probability: writing, reading, giving a phone call or working on a computer. In the same way a user in the meeting room could be just listening, speaking or writing. All those behaviour could be recognized thanks to other sensor in correlation with the indoor position system.

4.2 Position guessing

Information gathered from various sensors is saved into a log file of user's previous movement. In other terms, a file records all the places the user went to, with date and time. By taking in account those previous movements and also in which order the user went to these places (using dates and times), the indoor position information could also be used to guess a person's location.

Indeed, by studying the order in which the user went to some places and the moments he/she went there, we can find some pattern in the behaviour. Human have a good tendency to have habits. Thus there are high chances to detect some habits in those movements and then to use these pattern to guess the user location when we are unable to measure it. It would also be possible to make guessing about users' future location (thus the place they might be heading for).

5 Conclusions

Due to the urging needs of the AmI applications for context information there is a racing for systems that would react dynamically to the context and would provide information about it. Using a Bluetooth wireless based connection system, we measure users' indoor position. Indeed, by measuring the connection

⁶ In this case, the sitting position is recognized thanks to a foot pressure sensor, which detects pressure applied on the user foot. It allows detection of sitting, standing, running and walking behaviours.

signal strength between mobile station (standing for the user) and base stations placed in the covered area, we measure the users' location relatively to the base stations.

This paper explained the way to measure the position using a developed device as stations or using computers and mobile phones. Mobile phone gives a connection status indication instead of the real connection power. This makes the measuring less accurate but has a more realistic side.

We also presented an information system based on the Bluetooth indoor positioning system that gives the user useful information according to his/her actual position. That system provides different information services. First it gives information about a place (a rapid overview or detailed information), it also gives information about persons of that place (quick resume or full information) and it gives these persons' location in real time. Finally, it allows users to search for these persons.

We also presented another field of studies for using the indoor position. Working on the human behaviour studies field, we are working on the human behaviours' recognition and behaviour prediction. The indoor position can be used in those fields.

XACML as a Security and Dependability Pattern for Access Control in AmI environments *

Antonio Muñoz¹, Francisco Sánchez-Cid¹, Paul El Khoury², and Luca Compagna²

¹ Computer Science Department. University of Malaga.

² SAP Labs France

{amunoz,cid}@lcc.uma.es

{paul.elkhoury,luca.compagna}@sap.com

Abstract. One of the most interesting paradigms of Ambient Intelligence is that networks of pervasive intelligent interfaces recognize our presence and mould our environment to our immediate needs. In this paper, we present an example of how an access control model such as XACML adapts its functionality at runtime to new and unforeseen requirements. In previous work, we have proposed a three levels hierarchy of artefacts to semantically represent Security and Dependability solutions so that they can be automatically applied and adapted to new context requirements. Here we apply those artefacts throughout two case studies covering (i) the representation of the XACML model and (ii) a Policy Enforcement Point. The use of these artefacts provides the interoperability, run-time reaction to changes in the application context, and the possibility to monitor the applied solutions.

1 Introduction

Most of current techniques to address Security and Dependability (S&D) issues are designed for static architectures, with well-defined pieces of hardware, software, communication links, limits and owners. Thus, they fail when confronting new and challenging computing paradigms for highly dynamic environments such as Ambient Intelligence, where networks of pervasive intelligent interfaces recognize our presence and mould our environment to our immediate needs.

Several approaches have faced the security management of multiple devices with a large number of small interconnected applications [1] [2], paving the way to further advance in the three building blocks of AmI technologies [3]: Ubiquitous Computing, entailing the apparition of numerous heterogeneous computing nodes, which must cooperate despite their heterogeneity, and lack of a central control; Ubiquitous Communication implying the intercommunication of these objects, probably in an unpredicted way, introducing two important challenges:

* Work partially supported by E.U. through projects SERENITY (IST-027587) and GREDIA (IST-034363) and by Junta de Castilla la Mancha through MISTICO-MECHANICS project (PBC06-0082)

(i) the development of an adequate interface to permit secure communication among diverse components and (ii) the ability to negotiate the different parameters of the communication; and finally, Intelligent User Interfaces that will enable people to control and interact with the environment in a natural (voice, gestures) and personalized way (dependence on the context) without saturating users with technical decisions.

AmI considerations lead us to argue that it is essential for S&D mechanisms to be able to adapt themselves to renewable context conditions in order to be applied to the ever-changing AmI scenarios. The key for this dynamic adaptation of the security mechanisms is the ability to capture the expertise of S&D engineers in such a way that it can be used by automated means. With that goal in mind, in [5] we proposed the precise modelling of S&D Solutions (previously analysed by security experts) by means of what we called S&D Artefacts. These S&D Artefacts adopt an integral methodology covering the complete system lifecycle going from S&D Classes, used at development time, to S&D Patterns and S&D Implementations, devoted to deployment and runtime use. In order for these artefacts to be exploited at runtime, a whole architecture is introduced and described as the SERENITY Runtime Framework (SRF). The SRF, already introduced in [4][6], represents an integral approach for the automated selection, adaptation and monitoring of the S&D Artefacts. This paper provides a guide on how to use the S&D Artefact, creating a set of them from the analysis of two well-known security solutions: the XACML access control model and a Policy Enforcement Point.

In what follows, section 2 covers a necessary introduction to the concepts of S&D Pattern, Classes and Implementations, along with a brief description of the architecture where the SRF and S&D Artefacts converge. Section 3 presents the analysis and representation of a security solution as an S&D Pattern. Section 4 follows the results of section 3 and presents the concept of Integration Scheme as set of S&D Patterns whose composition allow us to characterize a complex access control model. The previous work on analysis and representation of security models and the different approaches for adaptive dependability is given in section 5. We close with conclusion and further work.

2 S&D Artefacts for Runtime use

2.1 A hierarchy of solutions: Classes, Patterns, and Implementations

As outlined in the introduction, one of our goals is the development of artefacts for the representation of S&D Solutions in the form of semantic descriptions, in such a way that these solutions can be selected, adapted, used and monitored at runtime by automated means. In the interest of enabling this automation, three are the artefacts that integrate the hierarchy proposed to represent the S&D Solutions: S&D Classes, S&D Patterns, and S&D Implementations. Although this paper emphasized the use of S&D Pattern artefact, [5] presents an intuitive and extensive description of them all.

S&D Solutions refer to widespread and well-known S&D mechanisms, going from a secure key exchange protocol or a VPN application, to a data encryption algorithm. S&D Patterns are detailed descriptions of abstract S&D Solutions that contain all the information necessary for the selection, instantiation and adaptation, and dynamic application of the solution represented in the S&D Pattern. One important aspect of the solutions represented as S&D Patterns is that they can contain a description of the results of any static analysis performed on them. Such descriptions provide a precise foundation for the informed use of the solution and enhance the trust in the model. Despite of that, the limitations of the current static analysis tools introduce the need to support the dynamic validation of the behaviour of the described solutions by means of monitoring mechanisms. However, we will skip the details of the monitoring mechanisms to concentrate in the functionality of the S&D Solutions presented here.

While each S&D Pattern describes the behaviour of one solution, the complexity of the S&D requirements to address in a system might require the combination of S&D Patterns. Integration Schemes (IS for short) capture this compositionality means, melting the functionality of two or more S&D Patterns, which if not properly analysed, can lead to interferences among them causing an unpredicted functionality.

If two S&D Patterns provide the same S&D Properties (e.g. confidentiality or non- repudiation) and comply with a common interface, then we group them in an S&D Class. S&D Classes represent abstractions of a set of S&D Patterns characterized for providing the same S&D Properties and complying with a common interface [16]. (Notice that S&D Patterns that belong to an S&D Class can have different interfaces, but they must describe how these specific interfaces map into the S&D Class interface.) With this approach it is possible for developers (at development time) to create an application bound to a specific S&D Class. Given that this artefact defines the high-level interface, all S&D Patterns belonging to this S&D Class and matching the context requirements will be selectable by the framework at runtime, thus providing a high degree of interoperability.

Finally, to close the gap between the real executable components (HW or SW) and the S&D Patterns, one last artefact is introduced: the S&D Implementation is an artefact that describes the specific context conditions to meet before deploying the executable component. It conforms directly to the interface, monitoring capabilities, and any other characteristic described in the S&D Pattern implemented.

2.2 Underlying Architecture: the Serenity Runtime Framework

This section describes how the SERENITY Runtime Framework (SRF) navigates throughout the S&D Artefacts' hierarchy in order to discover, select and deploy an S&D Solution. Figure 1 shows a simplified structure of the SRF.

Our approach assumes that instances of SRF can be embedded in any type of device with a minimum computational power. Every SRF instance acts as a dynamic provider of S&D solutions to applications also allowing the monitoring

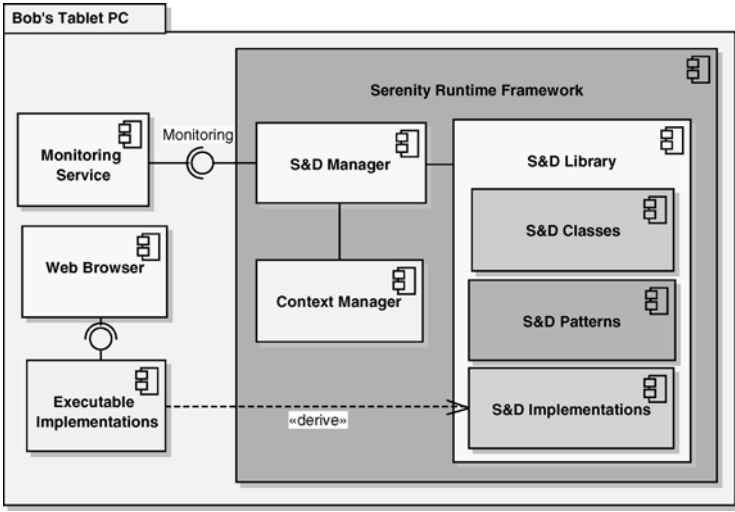


Fig. 1. Simplified perspective of SRF

of the behaviour of the solutions. Each SRF instance has an S&D Library containing a selected set of the artefacts described in section 2.1, including all S&D Classes, Patterns and Implementations corresponding to the solutions already deployed, along with additional solutions for future use. When a change in the context is detected via the Context Manager, the library is accessed by the SRF to look for the best pattern to meet the new requirements (detailed in section 3.3). Eventually, if a solution is selected, the SRF uses the information provided by the S&D Implementations and dynamically deploys the corresponding Executable Component.

After that, the run-time monitoring mechanism starts monitoring the workflow of the system. This process is indispensable in case of change of context (e.g. swapping the connection from a trusted to an untrusted network), when the Framework has to adapt on-time the current solution in order to face the new requirements.

3 A worked-out example: XACML captured via S&D Patterns and Integration Scheme

A brief example will help us to understand the overall functionality. Bob uses the internal forum of his company to manage his team. The internal forum is the company's essential communicating platform, where news raging from confidential to top secret are posted. Alice, the network and forum administrator have to keep the confidentiality of the data maintained, however provide these data only to legitimate employees. This example clearly asks for an Access Control (AC) mechanism to be in place at the company that Bob is working for. An

AC mechanism is the means by which a system grants or denies the right for a subject to perform some actions on some resources according to the policy defined by the system's security officer.

More precisely, a subject is the initiator of a request for access, e.g., Bob. A resource is the valuable data to be protected, e.g., the information stored in the working group forum of Bob's company. Actions are the set of operations that subjects can request to interact with the resources, e.g., post a message in the working group forum. Last but not least, a policy is the set of rules prescribing whether a subject can perform an action on a resource or not, e.g., the security officer Alice has defined the following policy rule: a message can be post in the working group forum if, and only if, (i) the sender is subscribed to the forum, (ii) the message is sent from within the intranet network that contains the server running the working group forum. As a matter of fact, not all the available AC mechanisms allow for the specification and enforcement of environmental conditions such as (ii) strongly required by our (simple) example and by AmI scenarios in general.

In the sequel of this section we will present XACML (eXtensible Access Control Markup Language [17]), an AC mechanism offering that level of granularity and adaptability necessary to express and enforce general environmental conditions as required by AmI scenarios. Then we will show how our S&D artefacts hierarchy allows for capturing this AC mechanism through an Integration Scheme and S&D patterns. With respect to our worked-out example and at development time, the SERENITY framework would suggest to the system designer the XACML Integration Scheme as security solution and AC mechanism for the system to develop. Last but not least we will discuss how the SRF exploits the S&D artefacts hierarchy to deal at runtime with a context change in our example.

3.1 XACML

As depicted in Figure 2, XACML is built on top of six basic entities: the Policy Enforcement Point (PEP), the Policy Decision Point (PDP), the Policy Administration Point (PAP), the Context Handler (CH), the Obligation Service (OS), and the Policy Information Point (PIP). The PEP is the XACML's front-end that receives a subject's request, initializes its evaluation process, and sends back the answer. The PDP selects the applicable policies and computes the authorization response by evaluating the requests with respect to these policies. The PAP stores the policy rules required for the PDP. The CH acts as a bridge translating the received requests into a proper XACML format and vice versa for the responses. Finally, the OS and PIP are used to retrieve obligations resulting from evaluating the policies and to retrieve the attributes for the subjects or resources, respectively. The AC decision process is hereafter described in more details (see again Figure 2):

1. The Subject requests authorization from the PEP to access the resources.
2. The PEP sends the request for access to the CH in its native request format, including attributes describing the subjects, resource, etc.

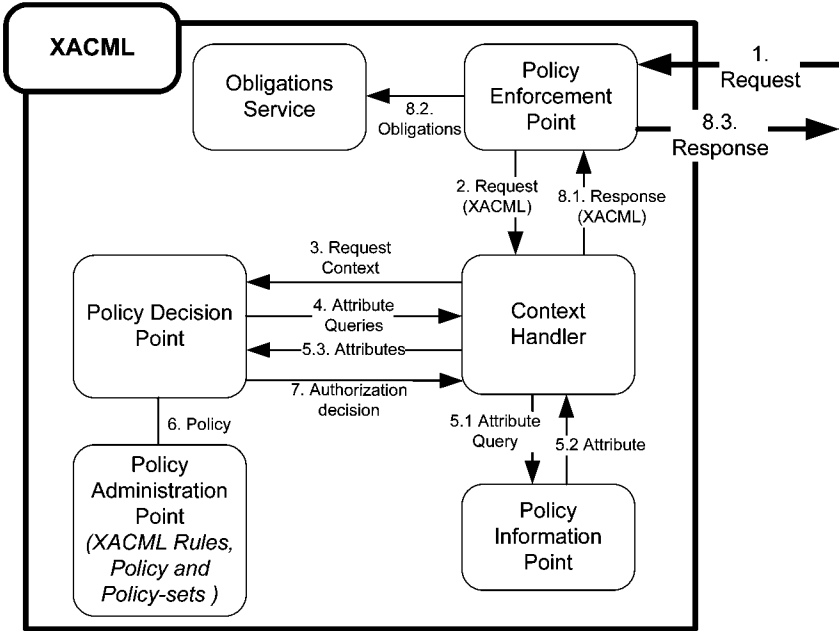


Fig. 2. XACML process overview

3. The CH takes the received data, constructs a corresponding XACML request context, and sends it to the PDP.

4. The PDP analyses the XACML request and if necessary, ask the CH to retrieve additional attributes.

5. The CH requests the necessary attributes from the PIP and sends them back to the PDP.

6. The PDP gets the applicable policies, stored in the PAP, and check if the subject’s request satisfies the policies. Notice that since several policies can be in place, the PDP uses algorithms such Deny-Override, Permit-Override or Only-Once Applicable to decide over them.

7. The PDP returns the authorization decision to the CH. Notice that the positive authorization decisions can comprise some additional obligations the subject has to satisfies to get access to the required resource.

8. The CH translates the XACML response received from the PDP to the native response format and returns the authorization decision to the PEP. Using this information, the PEP checks the obligations (if any) and either grant or deny access to the subject.

3.2 XACML as an Integration Scheme and S&D Patterns

S&D Integration Schemes (IS) are particularly suited to capture composed object like the XACML model. The basic idea is to capture each component

of the XACML model as an S&D Pattern and to capture their composition and interaction through an IS. Figure 5 S&D Class for Policy Enforcement Points shows an excerpt of the IS capturing the XACML model for automated application by the SRF (see the Appendix for a complete commented version of the IS). Components, e.g., the PEP, are specified within row 6. The name of the component is used to distinguish calls to one S&D Pattern or another (e.g., a call to the PEP is specified through PEP.operationName). Row 4 describes the IS interface, where several calls to operations fulfilled by external components are defined. Row 5 includes the explicit mapping from the S&D Class grouping AC patterns and IS to the XACML's IS. The PatternClass consists of the S&D Class Reference providing the name of the S&D Class parent for this IS (`Access_Control.security.uma.es`) and the Interface Adaptor providing the sequence of operations applied by the IS. In this case, the pseudo-code points to the `accessRequest` operation that constructs the sequence of actions in the IS. The full sequence presented in the Appendix depicts the XACML overview in getting the AC decision as described previously. For instance, the `PEP.getDataFromSubject()` describes the operation where the PEP gets the access information from the Subject, including the resource to be accessed, the action to perform, etc. The `authorizationDecision` holds the response decision that the IS returns to the requester when the process is finalized.

S&D IntegrationScheme: XACMLAccessControl	
...	...
4	Interface
	<p>Calls:</p> <pre> PEP.getDataFromSubject (in:resourceAttributes, in:environmentAttributes, in:contentResources, in: subjectAttributes, out: requestForAccess) PEP.getObligationFromResponse (in: responseForAccess, out: obligationID) CH.translateRequest (in: requestForAccessData, out: XACMLRequest) </pre>
5	PatternClass
	<p>S&DClass Reference: Access Control.security.uma.es</p> <p>Interface Adaptor:</p> <pre> accessRequest (in: resourceAttributes, in: environmentAttributes, in: contentResources, in: subjectAttributes, out: authorizationResult) { requestForAccess = PEP.getDataFromSubject (resourceAttributes, environmentAttributes, contentResources, subjectAttributes) XACMLRequest = CH.translateRequest (requestForAccess) requiredAttributesID = PEP.getListOfRequiredAttr (XACMLRequest) ... return authorizationResult } </pre>
6	Components
	<p>Component PEP (S&D Pattern for Policy Enforcement Point)</p> <p>....</p> <p>...</p>
...	...

Fig. 3. S&D Integration Scheme XACML

The XACML IS depends on the PEP, PAP and other entities to provide the S&D solution for Alice's requirement. For sake of simplicity we only discuss how the Serenity tool captures in our artefact the PEP patterns' instances i.e., the

two S&D Patterns Fedora-PEP and the QoS-PEP through their shared S&D Class. The S&D Class represents the Policy Enforcement Point requirement at high level. The system receives (from a subject) a request for access and returns an enforcement of the access response. The process in between is transparent from the subject’s side, but includes a complex procedure that provides different types of PEP S&D Properties to the system. Table presented in figure 4 shows an S&D Integration Scheme XACML, which is a visual representation of the structure for the PEP S&D Class. All provided properties are specified in the S&D Class, making it possible for the Serenity tool to decide whether this class matches with the system requirements. The ID field of the property describes a universal identifier (e.g. Fedora-PEP, identifies the PEP property as the one formally defined by Fedora.com). The S&D Class also includes an interface that defines the operations that conforms to its functionality. In the example, a unique call is specified and all S&D Patterns belonging to this S&D Class have to consent with this interface.

S&D Class: PolicyEnforcementPoint	
...	...
3	Provided Properties:
	Property: PolicyEnforcementPoint: ID: PEP.Fedora.com
	Property: PolicyEnforcementPoint: ID: PEP.QoS.Fedora.com
4	Interface Definition:
	Calls: getAccess (in: subjects::text, in: objects::text, in: ACL::text)

Fig. 4. S&D Class for Policy Enforcement Point

Next table (figure 5) S&D Pattern Fedora-PEP shows the Fedora-Policy Enforcement Point representation in our S&D pattern structure, while figure 6 S&D Pattern QoS-PEP shows the one for the QoS Policy Enforcement Point. The basic difference between these two Patterns remains in the implementation applied at the lower level. The Fedora-PEP pattern can not retrieve the data from the requester if the requester is using a SmartPhone while the QoS-PEP pattern enables it with the getDataFromSubjectSupportingQoS. Further details are omitted on the basic difference as it falls out of the paper’s scope.

3.3 SRF at work

Bob’s job requires posting messages in the working group forum very frequently. He usually works from office using his company laptop under Windows XP. Due to Bob’s outstanding results, he got promoted and awarded with a brand new SmartPhone that gives Bob a 24h access to the Internet. The SmartPhone has some QoS requirements that the actual PEP does not provide. Bob uses his new device to access the forum, however he access was denied. As a matter of fact, the

S&D Pattern: Fedora-PEP	
...	...
5	PatternClass
	S&DClass Reference: Policy_Management.security.uma.es Interface Adaptor getAccess (subjects [], objects [], ACL []){ getDataFromSubject(in: subjects, in: objects, in: ACL, out: requestForAccess) getObligationFromResponse(in: responseForAccess, out: obligationID) checkObligation(obligationToFulfil, responseForAccess)}
...	...

Fig. 5. S&D Pattern Fedora-PEP

S&D Pattern: QoS-PEP	
...	...
5	PatternClass
	S&DClass Reference: Policy_Management.security.uma.es Interface Adaptor getAccess (subjects [], objects [], ACL []){ getDataFromSubjectSupportingQoS(in:subjects, in:objects, in:ACL, out:requestForAccess) ... }
...	...

Fig. 6. S&D Pattern QoS-PEP

Context Manager realizes that the browser is trying to connect to the intranet from an unsupported system. As the SRF was configured to work over systems supporting the Fedora-PEP, the active S&D Pattern providing the PEP is no longer valid, and the system must be reconfigured (needs to support the QoS requirement). The S&D Manager analyses the context information coming from the Context Manager along with the current S&D Requirements and triggers a query to find the best solution available in the S&D Library. Since the new requirement is to extend the PEP pattern with the QoS option, the SRF queries the S&D Library and finds the S&D pattern QoS-PEP. The new S&D pattern QoS-PEP is activated and its implementation is selected and replaced in PEP part of the XACML IS. On the next day at the restaurant, using his SmartPhone, Bob succeeds in posting some messages on the internal forum.

4 Related Work

Our work proposes a complete framework for the rigorous treatment of S&D solutions that covers the automated selection, deployment and monitoring of the artefacts. Several approaches going from component-based to multi agent systems have been proposed for this problem in the literature.

Current work on component-based software development is mainly focused on the dynamic analysis of component compatibility, usually from a functional point of view, with the objective of adapting components and synthesizing suitable software architectures [7] [8] [9] [10]. Several component-based security models

have been proposed in the literature. Unfortunately, these proposals have been based on oversimplified views of security, like those based on security levels [11], not applicable in Aml.

The most related approach to our work is the one presented in [12], where security patterns are used to construct secure and efficient inter-company coordination systems. This approach addresses the selection of the security pattern issue by dealing with the messaging models and the security models in the design phase. As a result, they were able to give the developers guidelines that consist in modelling the performance of data associated with each pattern for model selection in which security is considered. However, these guidelines are in natural language and thus do not allow security patterns to be expressed and supported for their automatic selection and posterior deployment.

The agent paradigm is especially well-suited for highly distributed environments where independent components from different owners coexist and interact. In [13] authors present a methodology that considering the organizational structures of agent systems, designs the abstract models of agents in a top-down manner. This method can cope with simple access controls and interaction patterns, but when modelling security aspects agent paradigms are quite limited, since an agent is an independent entity by definition and many security solutions like XACML, can not be represented.

A security architecture that system administrators, users, and application developers can use to compose secure systems is presented in [14]. This architecture is designed to support the dynamic composition of systems and applications from individual components, but it lacks of flexibility and is restricted to access control models. The CORBA RAD service is an example of this type of security model for access control to resources in component systems [15].

5 Conclusions and future work

This work presents a bottom-up approach that includes a Framework to provide S&D Solutions to applications by means of three S&D artefacts: (i) S&D Implementations to describe SW/HW components; (ii) S&D Patterns, which describe S&D Solutions and groups the S&D Implementations that realize them, and (iii) S&D Classes, which groups the S&D Patterns that provide the same S&D Properties and share a common interface. We have used them to analyse and describe XACML model as an Integration Scheme. In addition, we provided the full deployment of Policy Enforcement Point pattern, one of the components of that Integration Scheme.

Next steps include the provision of a framework to assist security experts in the creation of S&D Solutions, currently in progress, along with the definition of (i) a language for S&D Properties and (ii) the formalization of the monitoring rules.

References

1. Khan, K. M., Han, J., and Zheng, Y. 2000. Security Characterization of Software Components and Their Composition. In Proceedings of the 36th international Conference on Technology of Object-Oriented Languages and Systems (Tools-Asia'00) (October 30 - November 04, 2000). TOOLS. IEEE Computer Society, Washington, DC, 240.
2. Sewell, P. and Vitek, J. 1999. Secure Composition of Insecure Components. In Proceedings of the 1999 IEEE Computer Security Foundations Workshop (June 28 - 30, 1999). CSFW. IEEE Computer Society, Washington, DC, 136.
3. Kurt Bauknecht. 2002. LV-Nummer: 400376. Ambient Intelligence: The Vision of Information Society. BWZ der Universitat Wien.
4. Francisco Sanchez-Cid, Antonio Muñoz, Daniel Serrano, M.C. Gago. Software Engineering Techniques Applied to AmI: Security Patterns. In Proceedings of the First International Conference on Ambient Intelligence Developments (September, 2006). Developing Ambient Intelligence, Springer. Pages 108- 124. ISBN: 2-287-47469-2
5. Francisco Sanchez-Cid, Antonio Maña. Patterns for Automated Management of Security and Dependability Solutions. 1stInternational Workshop on Secure systems methodologies using patterns (SPattern'07), Regensburg (Germany), September 03-07, 2007.
6. Antonio Maña, Francisco Sanchez-Cid, Daniel Serrano, Antonio Muñoz. Building Secure Ambient Intelligence Scenarios. Eighteenth International Conference on Software Engineering and Knowledge Engineering (SEKE'06), San Francisco (USA), 2006.
7. Becker, S.; Canal, C.; Diakov, N.; Murillo, J.M.; Poizat, P.; Tivoli, M. 2006. Coordination and Adaptation Techniques: Bridging the Gap between Design and Implementation. Report on the ECOOP'2006 Workshop on Coordination and Adaptation Techniques for Software Entities (WCAT'06). ECOOP 2006 Workshop Reader, LNCS, Springer.
8. Khan, K.; Han, J. Composing Security-aware Software. 2002. IEEE Software, Vol. 19, Issue 1, pp 34-41. IEEE.
9. Brogi, A.; Camara, J.; Canal, C.; Cubo, J.; Pimentel E. 2006. Dynamic Contextual Adaptation CONCUR'2006 Workshop on the Foundations of Coordination Languages and Software Architectures (FOCLASA'06). Electronic Notes in Theoretical Computer Science, Elsevier, ISSN 1571-0661.
10. Khan, K.; Han, J.; Zheng, Z.; Security properties of software Components. 1999. Proceedings of Information Security: Second International Workshop, ISW'99, Lecture Notes in Computer Science, Volume 1729.
11. McDermid, J.A; Shi, Q. 1992. Secure composition of systems. Proceedings of Eighth Annual Computer Security Applications Conference. Pp. 112-122.
12. Nobukazu Y., Shinichi H., Anthony F. Security Patterns: A Method for Constructing Secure and Efficient Inter-Company Coordination Systems, Enterprise Distributed Object Computing Conference, 2004. Eighth IEEE International Volume , Issue , 20-24 Sept. 2004 Page(s): 84-97.
13. M. Wooldridge, N. R. Jennings, and D. Kinny. The Gaia methodology for agent-oriented analysis and design. Journal of Autonomous Agents and Multi-Agent Systems, 3(3),pp. 285-312, 2000.
14. Jaeger, T; Liedtke, J; Pantellenko, V; Park, Y; Islam, N. 1998. Security Architecture for component-based Operating System . In ACM Special Interest Group in Operating Systems (SIGOPS) European Workshop, 1998. 118.

15. Lopez, J; Maña, A; Ortega, J.J; Troya, J.; Yagüe, M.I. 2003. Integrating PMI Services in CORBA Applications. *Computer Standards & Interfaces*, 25, 4, pp. 391-409, Elsevier.
16. C. Canal, L. Fuentes, E. Pimentel, J.M. Troya, A. Vallecillo. "Adding Roles to CORBA Objects". *IEEE Transactions on Software Engineering* 29(3):242-260, Mar. 2003.
17. XAMCL and OASIS Security Services Technical Committee, "eXtensible Access Control Markup Language (xacml) committee specification 2.0," Feb 2005.

6 Appendix

Next table includes a short version of the Integration Scheme structure. Where new fields like Creator and TrustMechanisms are included and the Interface adaptor is fully deployed.

S&D IntegrationScheme: XACMLAccessControl	
1	Creator: University of Malaga, 2007-05-05
2	Trust mechanisms <code>^*{[{TEC#~ERT\$} (=?) ?=/UHYG5E€ #EW·\$%&\$}ç+</code>
3	Provided Properties
	Property: AccessControl ID: accessControl.security.uma.es Timestamp: 1083753687
4	Interface
	Calls: PEP.getDataFromSubject (in: resourceAttributes, in: environmentAttributes, in: contentResource, in: subjectAttributes, out: authorizationResult out: requestForAccess) PEP.getObligationFromResponse (in: responseForAccess, out: obligationID) CH.translateRequest (in: requestForAccessData, out: XACMLRequest) SO.getObligation (in: obligationID, out: obligationToFulfil)
5	PatternClass
	S&DClass Reference: Access_Control.security.uma.es Interface Adaptor: <pre> accessRequest (in: resourceAttributes, in: environmentAttributes, in: contentResources, in: subjectAttributes, out: authorizationResult) { requestForAccess = PEP.getDataFromSubject (resourceAttributes, environmentAttributes, contentResources, subjectAttributes) XACMLRequest = CH.translateRequest (requestForAccess) requiredAttributesID = PDP.getListOfRequiredAttr (XACMLRequest) for attributeID in {requiredAttributesID} do if (attributeID = null) then break endif requiredAttributes += PIP.getAttributeFromName (attributeID) endfor CH.sendAttributesToPDP (requiredAttributes) requiredPolicy = PDP.analiseRequestForPolicy (XACMLRequest) policy = PAP.getPolicy (requiredPolicy) responseContext = PDP.analiseRequest (requiredAttributes, policy) responseForAccess = CH.translateResponse (responseContext) obligationID = PEP.getObligationFromResponse (responseForAccess) obligationToFulfil = SO.getObligation (obligationID) authorizationDecision = PEP.checkObligation (obligationToFulfil, responseForAccess) return authorizationResult = authorizationDecision } </pre>
6	Components
	Component PEP (S&D Pattern for Policy Enforcement Point) Component PIP (S&D Pattern for Policy Information Point)
7	Pre-Conditions
	Supports labelling XACML, PAP, PDP, PIP, ContextHandler and PEP are available
8	Static Tests Performed
	Test: Tested for Confidentiality satisfied for objects Conditions: of test: APA from SIT Attack models considered: Unauthorized disclosure, Message replay, Message insertion, Message deletion, Message modification, NotApplicable results, Negative rules

Fig. 7. Short version of the Integration Scheme structure

Rationale for defining NCIPs (Neighborhood and Context Interaction Primitives) position paper*-**

J r mie Albert and Serge Chaumettea

LaBRI, Universit  Bordeaux I
351 cours de la Lib ration
33405 Talence cedex
FRANCE.

{jeremie.albert,serge.chaumette}@labri.fr

Abstract. With the increasing number of mobile terminals, the development of applications that will provide new dedicated services by taking advantage of the technology is an effective challenge. The combination of such terminals communicating with each other in a peertopeer and dynamically self organized manner is referred to as a Mobile Ad Hoc NETWORK, MANet for short. MANets can be composed of many different kinds of devices. To help the developers to cope with their heterogeneity, we believe that it is required to precisely (re)define the basic functions that communication and context interaction primitives can effectively provide, and to give the precise associated assumptions if any. We call these primitives Neighborhood and Context Interaction Primitives, NCIPs for short. The rationale for defining NCIPs is the topic of this position paper.

1 Introduction

Mobile Adhoc Networks can be composed of many kinds of devices like personal computers, PDAs, mobile phones or even sensors. These are very heterogeneous in terms of computing power, memory capacity, operating system (Windows or UNIX based systems, SymbianOS, TinyOS, etc.), supported programming languages (Java, C#, NesC, etc.), autonomy (from a few hours to several days), and radio technology (WiFi, Bluetooth) which affects their potential communication range. The presence of additional features such as sensors, cameras, etc., also depends on the brand of terminal. The management of this heterogeneity imposes many constraints and makes it mandatory to decide on a number of assumptions which make application development extremely context dependent.

* This work is supported by the French Agence Nationale de la Recherche under contract ANR05-SSIA000201.

** Java and all Javabased marks are trademarks or registered trademarks of Sun microsystems, Inc. in the United States and other countries. The authors are independent of Sun microsystems, Inc. All other marks are the property of their respective owners.

For instance, assume cars in a vehicular ad hoc network (also known as VANet [8]) that communicate using some radio technology. There is almost no chance, if no assumption is made regarding either their relative speeds or the radio technology that is used, that two cars moving in opposite directions can communicate because of parameters such as the latency inherent to the connection establishment process.

It thus appears that most existing middleware have been developed not to offer universal APIs that could be supported by any communicating device but for particular devices supporting particular technologies and targeted to a particular context. They make strong, even if not always clearly stated, assumptions about the environment and the mode of operation of the target platforms. An important side effect is that these middleware, making different assumptions can be neither interoperable nor universal and the applications developed on top of them therefore work in very specific contexts.

2 NCIPS

To help the developers to cope with this heterogeneity, still being able to access the low level features of the target platforms, we believe that it is required to precisely (re)define the basic features that communication and context interaction primitives can effectively provide, and to give the precise associated assumptions if any. We call these primitives Neighborhood and Context Interaction Primitives. The topic of this paper is to explain the rationale for this approach.

The methodology that we have adopted in our preliminary work is as follows. To decide what paradigms NCIPs must support, we have studied those existing environments that we consider significant to our approach, such as TinyOS [2], [11], TOTA [9], JXTA [6], Mate [7] or Squawk [12]. We then have classified and analyzed the primitives available in these middleware or software layers. Based on that state of the art, we have defined and given a precise semantics to a number of low level primitives that support similar concepts without making any hidden assumption.

In this paper, we show by means of examples that even though these primitives are low level because they try to be universal, they can be really useful in supporting MANet dedicated applications. This is a substantial reason to pursue the development of this research.

In the future, we intend to use this approach to define a set of universal primitives (NCIPs) and to develop a middleware that will make them available on any device integrated within a Mobile Ad hoc Network.

3 NCIPS can effectively support complex operations.

Example of the one way send NCIP

The goal of this section is to show that in spite of their simplicity, NCIPs can still be used to develop complex services or high level operations.

To illustrate this point, we consider the (difficult) problem of synchronizing a number of nodes. More precisely, we have up to three nodes¹ that want to access a critical resource that must not be accessed by more than one node at a time.

This is usually achieved by some sort of rendezvous [10] and relies on a number of assumptions on the environment:

- communication is bidirectional;
- communication channels are stable during the execution of the operation;
- etc.

Our approach is different in that we do not want to impose any unnecessary or unrealistic constraint. We simply rely on basic communication primitives which are part of our NCIPs. These are:

1. a one way send method (send), one way meaning that it does not return any information or status and does not guarantee that the target node effectively receives the message;
2. a receive method (receive).

We then propose the implementation presented algorithm 1 (See figure 1). In order to get access to the shared resource, each node goes through the following steps:

1. randomly choose a neighbor chosenNeighbor (line 26);
2. send a random number n (randomNumberSent in algorithm 1, lines 27 and 28) to chosenNeighbor;
3. send 0 to the other neighbors if any (line 30 to 37);
4. if the number m (message.value in algorithm 1) that is (possibly) received (line 8) from node chosenNeighbor (m can be received while any other step of the algorithm is executed) is such that $m \neq 0$ and $m < n$ then the resource is acquired for a predefined period of time t_2 (line 13) otherwise the node waits during t_2 ;
5. loop to step 1.

The temporal arrangement of the different steps of the algorithm for a sample run is shown figure 2.

Despite the fact that this algorithm relies on a very basic one way send method that does not return any information about what it has effectively done, it still ensures that the shared resource is used by at most one node at a time.

Even though this is out of the scope of this paper, we discuss the performance of this primitive to show that this is not simply a toy example and that it works in the real world. The resource sharing algorithm performance depends on several parameters:

- the number of nodes (two or three) that execute the algorithm;
- the interval where the random number is selected;
- the time t_1 required to decide which node is going to have the resource (it corresponds to steps 1, 2 and 3 of the algorithm);

```

1  [...]
2
3  int randomNumberSent = 0;
4  Node chosenNeighbor = null;
5
6  // this method is invoked when a message is received
7
8  void receivedMessage(Node from, Message message) {
9
10     if (from == chosenNeighbor) {
11
12         if (message.value != 0 && message.value < randomNumberSent)
13             // I have the resource and I keep it for t2
14             [...]
15         else // I do not have the resource, I sleep for t2
16             sleep();
17     }
18 }
19
20 // this method is invoked when the internal timer is fired
21
22 void timerFired() {
23
24     // send a random number n to a random neighbor
25
26     Node chosenNeighbor = selectRandomNeighbor(); // from the static list of neighbors
27     randomNumberSent = randomNumber();
28     send(chosenNeighbor, randomNumberSent);
29
30     // send 0 to all other nodes
31
32     NodeList knownNodes=getNeighborhood(); // get the static list of neighbors
33     Node node= knownNodes.firstNode();
34     while (node != null) {
35         if (node != chosenNeighbor)
36             send(node, 0);
37         node = knownNodes.nextNode();
38     }
39 }
40
41 [...]

```

Fig. 1. Algorithm 1 Resource sharing

- the time t_2 while the nodes keep the resource or wait for the following round (step 4 of the algorithm).

For example, for two nodes, if we consider that the probability for each of these nodes to choose the same random number is negligible, then the utilization ratio of the shared resource is FORMULA.

This algorithm has been implemented on a number of Xbow nodes [1],[4] running the TinyOS [2],[11] system and the experimental results effectively confirm the above analysis.

4 NCIPs can significantly impact efficiency. Example of the neighborhood density NCIP

The goal of this section is to show that properly defining some NCIPs to operate in a really mobile context sometimes makes it possible to improve the efficiency

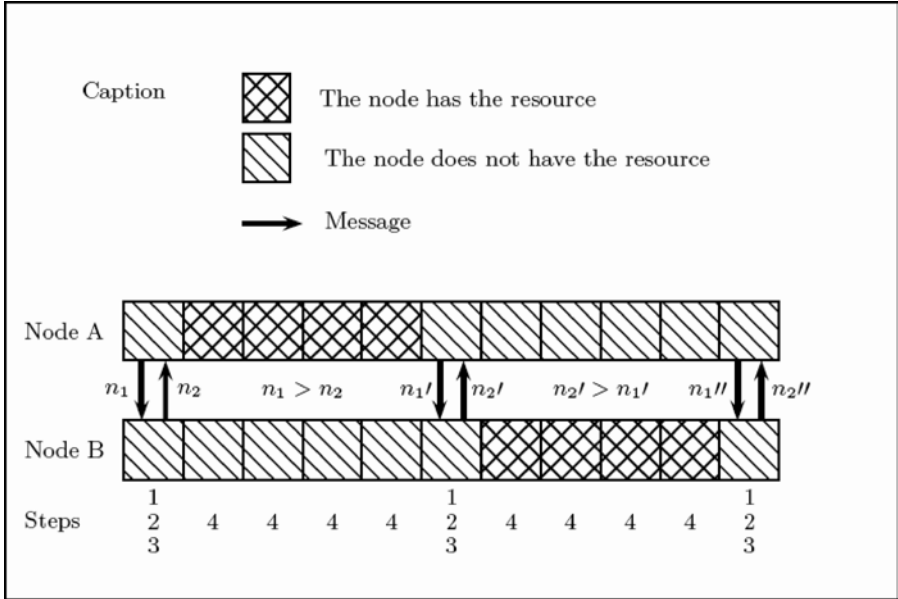


Fig. 2. Temporal behavior of the resource sharing algorithm executed by two nodes

of algorithms. We illustrate this point with the computation of the neighborhood density NCIP and its usage in a flooding algorithm.

In a static framework it is relatively straightforward to compute the number of neighbors of a node (basically because it is stored in a table). When switching to a mobile context, either such primitives are dismissed or the problems raised by the mobility of the environment are simply ignored (see below). In our opinion these solutions are unacceptable.

Density awareness is used in several algorithms [14] [15]. Here we consider the Delayed Flooding with Cumulative Neighborhood (DFCN) algorithm presented in [5]. The basic goal of this last algorithm is to propagate information over the network by using flooding. Based on a multicriteria optimization approach, it tries to find a compromise between the number of messages exchanged in the network and the speed at which the nodes are informed. Its behavior is directed based on several parameters, among which the number of neighbors, i.e. the neighborhood density at each node and the ratio of neighbors that already have been informed. It is shown that considering a density threshold, below which it is decided not to broadcast the information to the neighborhood, diminishes the network load without increasing too much the time necessary to inform all the nodes.

The density computation in a mobile network is usually implemented as follows. A node regularly broadcasts a beacon to signal its presence to its neighborhood. Based on the collection of all the beacons it is aware of, a node can then compute the density of its neighborhood. The thing is that because of the

instability of the network, the resulting value is possibly false as soon as it has been computed. Instead of ignoring this, we propose an alternative in our NCIPs framework: the result of the density computation primitive contains a stability value that says how long the information remains true. This can be used to further improve the algorithm: if the stability period is too short, using the computed density value does not make sense; if it is long enough, the algorithm can wait for new nodes to arrive or for nodes to leave (which is useful to control more precisely the number of messages in the network).

This example shows that there can be significant advantages that come from having low level universal primitives. In this case, instead of hiding information and problems from the user, giving him access to low level context information can help optimize the algorithms.

5 NCIPs can restore hidden features. Example of anonymity ensured by the one way broadcast NCIP

Assume the following problem. A piece of information, say I, is stored at a given node, say N. The goal of N is to get rid of I, after making sure that it is now stored by another node of the network. Using standard primitives this would most likely be implemented as show algorithm 2 (see figure 3). Let us analyze

```

1  [...]
2
3  // this method is invoked when a message is received
4
5  void receivedMessage(Node from, Message message) {
6
7      switch (message.getType()) {
8
9          case DATA_TO_STORE :      // someone passed me a piece of data (I) to store
10             I = message.getData();
11             send(from, ACK);
12             break;
13
14             case ACK :                // some one as got my data I, and I can thus get rid of it
15                 I = null;
16                 break;
17         }
18     }
19
20     // this method is invoked when the internal timer is fired
21
22     void timerFired(){
23         Node neighbor = selectRandomNeighbor();
24         send(neighbor, I);
25     }
26
27     [...]
```

Fig. 3. Algorithm 2 Information storage with the standard primitives

this algorithm. First, it makes a number of implicit assumptions. At line 23, it supposes that it can access the identities of its neighbor nodes. It furthermore

assumes that the information that it gets is stable and that it can use it at line 24. Nevertheless, in a real world mobile network, it might be the case that between the execution of these two lines of code, the target node has moved or disappeared and cannot be accessed any longer. So, there is an implicit assumption about the stability of the network at that point of the algorithm. The same kind of assumption is made line 11. In the real world, there is no reason why the target of the ACK message should be in reach of the current node at that time. Second, from a functional point of view, there is an indirect side effect of using a high level communication primitive: the initial (respectively the final) owner of the information knows which node is finally (respectively was initially) owning the information.

```

1  [...]
2
3  void receivedMessage(Node from, Message message) {
4
5      switch (message.getType()) {
6
7          case DATA_TO_STORE :
8              I = message.getData();
9              send(*, (ACK, I.number));
10             break;
11
12         case ACK :
13             if (message.number == I.number) { // this is the ACK for our own I
14                 I = null;
15             }
16             else {
17                 send(*, (ACK, message.number));
18             }
19             break;
20         }
21     }
22
23     void timerFired(){
24
25         if (I!=null) {
26             I.number++;
27             send(*, I);
28         }
29     }
30 }
31 [...]

```

Fig. 4. Algorithm 3 Information storage with NCIPs

The point is that we have considered an algorithm designed for a reliable static framework and we have ported it almost directly to a totally distributed context. This implicitly assumes a number of hypothesis that do not hold in a MANet.

Therefore we have designed algorithm 3 (see figure 4) which is a NCIP based implementation. We just assume a communication primitive that makes it possible to broadcast a message without any knowledge of the neighborhood, without any guarantee regarding the possible reception of the message and without any

knowledge about the identity of any possible receiver. We call this NCIP one way broadcast.

The behavior of the algorithm is as follows. A node that holds the information broadcasts it at regular intervals (line 27). It still holds the information till an acknowledgment gets back to it through the network. Nevertheless, this acknowledgment does not necessarily come from a node that directly received the message since there is no guarantee that we have bidirectional communication. Rather, when a node receives the information, it broadcasts an acknowledgment to its neighborhood (line 9). This neighborhood in turn broadcasts this ACK (line 17), until a given TTL (the TTL management is not shown on the algorithm to make it easier to read). At some point in time, the initial node might receive an acknowledgment. It then removes the information (line 14). While no acknowledgment is received, the node simply holds the information and at some point possibly restarts the whole process. The behavior of the algorithm is illustrated figure 5.

This algorithm has been simulated on an adaptation to a mobile context of the DAGRS simulator [13] that is developed in our team. This simulation allowed us to validate this algorithm in an experimental way. By adapting/developing this algorithm based on NCIPS we have gained two major benefits: no unrealistic or useless assumption on the network mobility nor communication capacities have to be made; the privacy problem described above disappears, i.e. no node knows which other nodes now store the information or have stored the information in the past.

Once again this shows that working with too high level functions necessarily leads to implicit assumptions that are basically false in a MANet. It is furthermore especially interesting to see that we can achieve a better result (here in terms of anonymity) with less assumptions.

Once again this shows that working with too high level functions necessarily leads to implicit assumptions that are basically false in a MANet. It is furthermore especially interesting to see that we can achieve a better result (here in terms of anonymity) with less assumptions.

6 Conclusions and Future Work

In this paper we have introduced the notion of Neighborhood and Context Interaction Primitives (NCIPs). These are the most basic features that can be supported by a mobile network without making unrealistic assumptions. We have described a number of examples that illustrate some interesting features of NCIPs: they can be used to define complex operations (example 1); they can improve the efficiency of algorithms (example 2); they can guarantee properties that are not supported by more standard primitives (example 3).

Nevertheless, this is preliminary work and a lot remains to be done. We are currently working on the definition of a number of basic primitives. Based on these definitions we explore the higher level operations and algorithms that they make possible to implement. In the short term we will implement these primitives

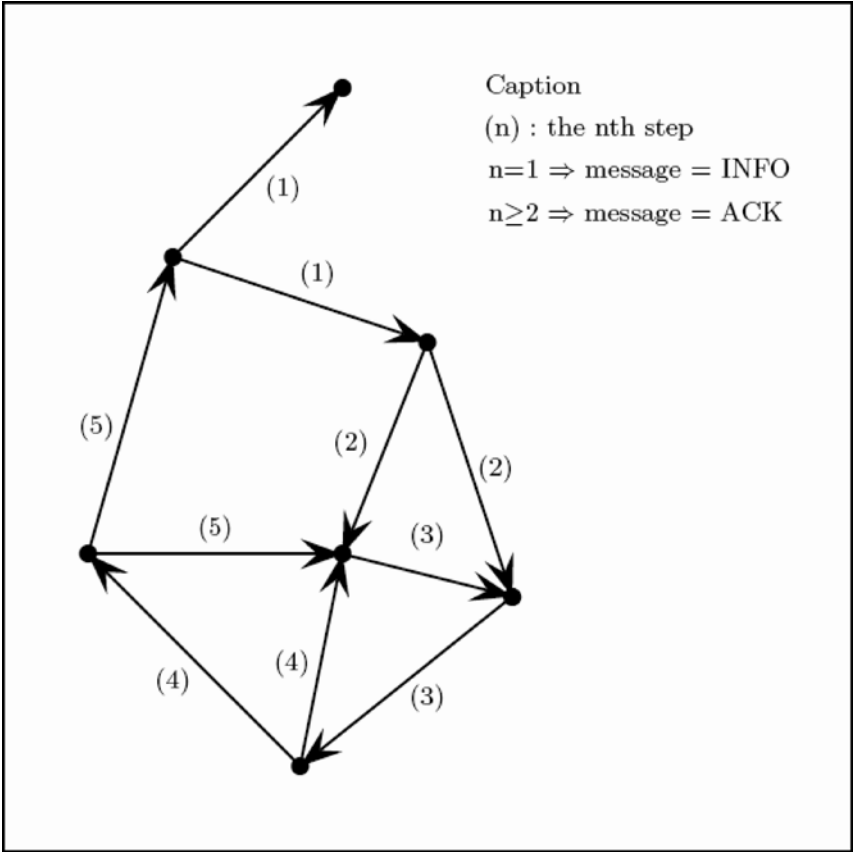


Fig. 5. The different steps of the information storage algorithm on a sample network

on several platforms that we are working on in the team, i.e. mobile phones, PDAs, and sensors. We furthermore work on a formal model based on a graph rewriting approach[3] that we have extended to deal with dynamic networks.

References

1. Crossbow Technology. <http://www.xbow.com/>.
2. TinyOS: An opensource OS for the networked sensor regime, 2007. Available at <http://www.tinyos.net/>.
3. A. Casteigts and S. Chaumette. DynamicityAware Graph Relabeling Systems (DAGRS), a local computationbased model to describe MANet algorithms. In International Conference on Parallel and Distributed Computing and Systems (PDCS'05), Dallas, USA, 2005. IASTED Press.
4. Jason L. Hill and David E. Culler. Mica: A Wireless Platform for Deeply Embedded Networks. IEEE Micro, 22(6):1224, 2002.

5. Luc Hogue. Mobile Ad Hoc Networks: Modelling, Simulation and Broadcastbased Application. PhD thesis, University of Le Havre, University of Luxembourg, 2007.
6. Sun Microsystems Incorporation. Jxta v2.0 protocols specification, January 2007.
7. P. Levis and D. Culler. Mate: A tiny virtual machine for sensor networks. In International Conference on Architectural Support for Programming Languages and Operating Systems, San Jose, CA, USA, Oct. 2002.
8. Jun Luo and JeanPierre Hubaux. A survey of intervehicle communication. Available at citeseer.ist.psu.edu/luo04survey.html.
9. M. Mamei, F. Zambonelli, and L. Leonardi. Tuples On The Air: a middleware for contextaware computing in dynamic networks. In IEEE, editor, Proceedings of the 2nd International Workshop on Mobile Computing Middleware at the 23rd International Conference on Distributed Computing Systems (ICDCS), pages 342-347, Providence, RI, USA, May 2003.
10. Y. Mi, $\frac{1}{2}$ etivier, Nasser Saheb, and Akka Zemmari. Randomized rendezvous. In Colloquium on mathematics and computer science: algorithms, trees, combinatorics and probabilities, Trends in mathematics, pages 183194. Birkh \ddot{u} $\frac{1}{2}$ anser, 2000.
11. S. Madden P. Levis, J. Polastre, R. Szweczyk, K. Whitehouse, A. Woo, D. Gay, J. Hill, M. Welsh, E. Brewer, and D. Culler. Ambient Intelligence, chapter TinyOS: An Operating System for Sensor Networks, pages 115148. Springer, 2005.
12. Doug Simon, Cristina Cifuentes, Dave Cleal, John Daniels, and Derek White. JavaTMon the bare metal of wireless sensor devices: the squawk Java virtual machine. In VEE '06: Proceedings of the 2nd international conference on Virtual execution environments, pages 7888, New York, NY, USA, 2006. ACM Press.
13. The DAGRS simulator. <http://www.labri.fr/perso/casteigt/simulator.html>.
14. Ting Wang, Shuang Hao, Ping Wang, and Gang Peng. Efficient and densityaware routing in wireless sensor networks. In The 15th IEEE International Conference on Communication and Networks (ICCC'N06), 2006.
15. Sau Yee Wong, Joo Ghee Lim, S.V. Rao, and W.K.G Seah. Densityaware hopcount localization (DHL) in wireless sensor networks with variable density. In Wireless Communications and Networking Conference, IEEE, pages 18481853 Vol. 3, 2005.

Agent Oriented AmI Engineering

Raian Ali¹, Sameh Abdel-Naby¹, Antonio Maña², Antonio Muñoz², and Paolo Giorgini¹

¹ University of Trento - DIT, 38100 Trento, Italy.
{raian.ali, sameh, paolo.giorgini}@dit.unitn.it

² University of Malaga - E.T.S.I.Informatica, 29071 Malaga, Spain.
{amg, amunoz}@lcc.uma.es

Abstract. Ambient Intelligence (AmI) refers to an environment that is sensitive, responsive, interconnected, contextualized, transparent, intelligent, and acting on behalf of humans. This environment is coupled with ubiquity of computing devices that enables it to transparently sense context changes, to react accordingly, and even to take the initiative towards fulfilling human needs. Security, privacy, and trust challenges are amplified with AmI computing model and need to be carefully engineered. From software engineering perspective, the shift towards AmI can be seen abstractly similar to the shift from object paradigm towards agent one. Objects provide functionality to be exploited, while agents possess functionality and know how and when to use and offer it autonomously. Agent paradigm is suitable for implementing AmI considering AmI as an open complex system. Moreover, we argue that agent paradigm is equally useful for engineering all aspects of such systems from the early phases of software development life cycle.

1 Introduction

Notebooks, PDAs, and third generation cellular phones are now computing devices equipped with wireless connectivity features allowing them to access different data networks anytime anywhere. The evolution in size and capabilities of those computing devices, along with those in wireless communications have effectively enabled people to be always online. This increased mobility in its raw form is not more than going beyond the classical desktop into a portable one. People are still requested to deal with different computers, and to adapt themselves to them. The next step would be to relieve people of even being aware of computer existence [1]. Computing is going to be seeded in the environment as an integral part of it, instead of being a set of external entities, used explicitly by trained humans.

Many challenges are related to enhancing the usefulness of the current advances in computing devices and communication ubiquity. One of them is that current software development methods were created mainly for what we can call request/response software. There is a lack of sufficient models, development experience and even of imagination about how the new software systems can exploit

the new technology advances [2]. The expectations of new software is that it will support features like location and context awareness, personalization, adaptability, organic growth, mobility, and some other features that impose the need of more comprehensive software engineering methods and new innovative modeling languages [3].

AmI focuses on making our environment sensitive to our needs and responsive smartly to people and environment context changes [4]. Objects around us in office, home, club, and other daily life locations, are expected to play their roles autonomously on behalf of us humans. AmI implies the ability of environment to learn and adapt by time to people characters and profiles, so ambient intelligence is always growing in organic style together with humans. This ambient is intertwined with invisible computing, it aims to give people what they need transparently without they explicitly ask or even know. AmI will relieve humans of being busy of at least the most repetitive actions they might take during their daily life.

It is well known that agent paradigm is a promising paradigm for implementing complex open systems like e-commerce, air-traffic, enterprise resource planning, and so on [5]. The characteristics of these domains fit well to what agent and multi agent systems can do. Software Agent is a software element that realizes the concept of agency, and acts on behalf of people or other agents. Agent paradigm was firstly dealt with inside AI community. Recently, and after the long hard experience of artificial intelligence, researchers could find other areas to exploit fruitfully agent paradigm. Agent paradigm has received a special interest in software engineering community as a paradigm shift from the object oriented one [6][7]. The shift is based on seeing the world as a society of distributed intelligence units, called agents, that have characters and can decide. This way of viewing the world differentiates itself from the object oriented one that conceptually view the world as a collection of objects. Objects provide encapsulation of data together with the procedures related, they are used by main well defined central control, and do not have their own autonomy.

One of the challenges that face building an AmI is the lack of models and software engineering practice that help analysing system requirements, designing the system to be built, verifying and testing the implemented one. Until now the research is in its first stages, and the need for suitable development methodologies has been already recognized. For engineering AmI, we might need different software engineering methods from those that are suitable for developing request/response systems, where system behavior is well known and determined strictly, and where human-computer interaction is desktop driven one. AmI shifts this way of interaction into contextual, direct, and invisible human environment interaction, hiding the computers in the background of this environment. The disappearance of computers and coupling environment appliances with computing devices will arise like any new technology a variety of challenges. The system domain is no longer some sort of business or organization has a clear business process and tasks. Users are no longer those clerks or students in a library system; instead users are now those normal people in houses, offices, campus and

other daily life environment. The request/response scenario is replaced here by continuous sensitive, reactive, intelligence surrounding computing.

We believe that agent paradigm is not only useful for implementing AmI systems, but rather we see it appropriate in all phases of the software development life cycle. As in object-oriented and component-oriented worlds, AmI ecosystems are composed of independent pieces of software with well defined interfaces, but the main difference is that in AmI each of these pieces has a different owner and has its own goals. This is another fundamental aspect that reinforces the appropriateness of agent oriented approaches for AmI. We are aware that current agent oriented software engineering methodologies, which are still inside the academic areas, have to be checked again for engineering AmI. If we succeed to analyze and design such systems by the use of agent driven software engineering, we might come up with final agent based system that is robust, scalable, and intelligent enough to satisfy AmI needs.

The remainder of this paper is structured as follows; next section shows AmI as multidisciplinary complex system. Section 3 outlines the agent paradigm. Section 4 introduces the agent oriented software engineering research. Section 5 discusses the possibility of exploiting agent paradigm for engineering AmI, for this purpose in subsection 5.1 we address the the potential agent paradigm has with regards to AmI systems engineering, and in the last but not least subsection we focus on how agent paradigm can be exploited to face security challenges in AmI ecosystems. In Section 5 we conclude.

2 The Multidisciplinary AmI

Approaching an ambient that is perceptive, intelligent, and active will involve multiple disciplines to contribute creating the final scene. Several researches are being done in AmI area, with some differences in emphasis and direction. Multiple terminologies are being used as this research is in its first steps. In the rest of this section, we will investigate the vision of AmI, and try to capture a variety of disciplines that need to meet in order to achieve this vision.

Philips vision of AmI [8] is based on shifting computers into the background, and supporting the ubiquitous computing with more awareness capabilities. The vision is based on three elements, 1) the ubiquity, which refers to those computing devices intertwined with human environment anywhere, and functioning anytime, 2) the transparency of such computing systems, so they are hidden in the background, 3) and the intelligence; they should act instead of being only responsive to human commands. Such system relieves people of thinking about many repetitive needs and takes the initiative of doing what should be done in the correct moment and approach.

MIT vision of AmI [9] similarly views it as an unobtrusive integration of computing with our daily life. Such computing provides humans with relevant information and performs necessary tasks when needed on their behalf. Such ambient will be continuously careful, doing the suitable tasks in a transparent, invisible and intelligent way. Traditionally, computers work as an apparent mes-

senger or mediator between humans and environment. In AmI, this relation is replaced by direct non-disruptive relation between humans and the environment they are located within. In short, AmI computing is no longer visible.

The vision of invisible disappearing computers was addressed by Weiser [10]. The vision expected ubiquitous existence of computing and communication capabilities anytime and anywhere. AmI focuses on assisting the intelligence and awareness of this ubiquity of interconnected computing devices, so computing starts to take the initiative on behalf of human. AmI is meant to orchestrate the variety of environment objects in a way they might interoperate to do more complex tasks as well. Ubiquity of computing is the basis an AmI is built on. However, the terms ubiquitous computing, pervasive computing, ambient computing, ambient intelligence are now used interchangeably with some differences in the context and emphasis.

AmI is now about integrating computing devices with the environment we all live in; it is then sitting on the opposite side of virtual reality which brings world inside computers [10]. This makes computers invisible and relieves people mind of even knowing about their existence. To arrive this point, computers has to adapt to user needs and character by contrast of the traditional scene in which user is supposed to adapt to computer systems. This is now of great importance because people spend increasingly more time to interact with computing systems. To people, it is becoming a source of stress being obligated to remember when and what and how to do tasks. With AmI, artefacts encapsulate implicitly the role of computer mediation. Artefacts will look as they have their own character, autonomy, and intelligence, they are more agents than normal objects.

Consequently, AmI is by nature a multidisciplinary paradigm [11]. Distributed intelligence is needed to cover this intelligent ambient, it is now composed of distributed intelligence units that we might call Agents. New hardware design is needed for embedding computing devices invisibly inside the surrounding physical environment. AmI system is situated within a highly dynamic environment that is open for changes, these changes need to be sensed and interpreted in a way that is timely fashion and relevant to what might serve user needs. The input now is coming implicitly, and continuously from a variety of sensors, cameras, and other kind of peripherals. Such environmental information need to be modeled and reasoned about in order to take the correct contextual decision.

Computer disappearance was considered by Weiser as one of the most profound technology features [10]. Apart from the physical disappearance of computing devices, there is that mental disappearance toward peace of mind in human life. To achieve such peace of mind, the interaction between human and computer is updated to direct interaction between human and environment [1]. New novel ideas of interaction design have to be invented to move from the explicit interaction to an implicit one [12]. The implicit interaction includes the notion of implicit input known more commonly as Context [13].

Context awareness [14][15] is an essential feature an AmI system has to tackle in order to act in adaptive and intelligent way. This context, that might be spatio-temporal, environmental, personal, social, and so on, needs to be modeled,

captured, analysed and reasoned about [2]. Reasoning about context needs a model and formalization acts as a knowledge base, and enables inferring more high level knowledge. For example blood pressure and body temperature besides user current activity and location might reveal user current mood, this mood can be provided implicitly as an input, so AmI might take some actions as a response.

AmI is expected also to have the ability of learning and keeping track of human historical behavior. AmI embodies a high degree of personalization to human profiles and life styles. Software personalization is a standalone research now, but we might hardly consider AmI as a useful system if it behaves in the same way with different kind of people and characters. The social mobility of humans is another important issue an AmI application needs to consider. People normally play more than one social role; they should be accordingly supplied by tailored services and information considering their social context [16].

AmI arises many social issues that need to be studied and analysed before AmI can get acceptance in practice. The ubiquity of computing might relieve people mind in one hand and might have negative impacts as well. People will feel that they lost control, and might not trust technology. People have already lost some privacy providing that cellular phones enable other party of at least knowing their location, and the same for using credit cards. Instead of commanding computing, computing in AmI is supposed to control several aspects of people everyday life. An essential principle in this regard is that human do not feel that they lost control, and to enable them configuring their needs in a simple way, may be through some privacy patterns. However, we see many interesting practical domains that can benefit from AmI scenarios, such as the health care domain, in particular those specialized of caring old people, and supporting persons with dementia problems, where AmI might play the role of caregiver.

3 Agent Paradigm

Agent-based computing is currently becoming an important research area. This increased interest is motivated by the need for software can act on behalf of its user, software that is able to realize the concept of agency. Giving a definition for agent is not straightforward; there is no consensus about the main characteristics an agent should have to deserve this name. A well accepted definition of software agent is found in [6]:

"An agent is an encapsulated computer system that is situated in some environment and that is capable of flexible, autonomous action in that environment in order to meet its design objectives."

An agent is supposed to have its own control over its state and behavior, to percept the environment around and to affect it in turn. Being in an environment and sensing it implies the necessity that agent can react to environmental context changes. Moreover, agent is supposed to activate goals without external prompt and to tailor suitable plans to achieve them. The key characteristics an agent must have that are highly agreed upon include: autonomy, proactiveness, reactivity, situatedness, directedness, and social ability.

Being autonomous, an agent behaves independently according to the state it encapsulates. For example, an agent, by contrast to an object, can decide the way of how to respond to the incoming messages from other agents. Agents interact with each other without losing control if they do not allow that. Proactivity means that agent is able to take the initiative without external order. Agents have goals and act in order to achieve them. This is more complicated than reacting in timely fashion to direct environment stimulus. Situatedness means the ability of agent to settle in an environment that might contain other agents, to perceive it, and to respond to changes that happen in it. An agent might make changes and effect this environment in turn. Directedness means that agent has a goal, this goal represents the reason of the actions an agent has to take. An agent does not exist in vacuum; instead it lives in a society of other collaborative or possibly competitive groups of agents. Agents have the social ability to interact with other agents. This interaction might be motivated by collaborative problem solving.

A long discussion can be found in the literature about what formulates an agent and what differentiates it from object. We are here not concerned about such discussion, rather we believe that using agent as a kind of abstraction might enable us of viewing the world as an organization of autonomous entities, directed by goals, able to sense the environment changes and can learn by time. The use of agent paradigm as kind of abstraction might better help of analyzing and designing complex open systems, and presents more natural way to start with, and hopefully this will lead to more robust and flexible software systems in correspondence.

An agent is supposed to live in a society of agents; multi-agent system (MAS) is known as a system composed of several agents collectively capable of reaching goals that are difficult to achieve by an individual agent or monolithic system. The relation can be alternatively competitive one, like for example multiple agents responsible for advertising products in an open market on behalf of different producers, or a society of agents in an e-auction. Again, defining MAS is not that straightforward. MAS might help us decomposing the problem into components that are able to interact and deal with unpredictable situations that can happen in complex systems like AmI.

A MAS represents a natural way of decentralization, where there are autonomous agents working as peers, or in teams, with their own behavior and control. Each of these agents looks to the world from its own perspectives and has its own goals and intentions. Such MAS is expected to work well with open complex systems, and to scale well by time. It is one promising computing paradigm for implementing many application domains such as e-commerce, enterprise resource planning, and traffic control, and so on [5]. We consider AmI as a system that fits by its nature to agent and multi-agent system paradigm as we are going to discuss later.

4 Agent Oriented Software Engineering (AOSE)

Software engineering is different from other engineering disciplines in its dependability on engineer skills of analysing the problem, designing a suitable solution, and coming up with the final system [17]. Although software engineering is qualitative in nature, a serious research is being done to find more and more scientific methods, models, and criteria that assist developing the intended software. Problems are everywhere in software development process, engineering a software is an engineering for abstraction. For example, understanding precisely what a software is supposed to do and transforming this knowledge into abstract models readable by both of engineers and stakeholders is far of being easy as it seems.

Many large industrial projects failed because the final software was not the one needed or expected. The models used to describe software requirements and design need to be compact and expressive enough to replace usefully the natural language. The models need therefore to be precise enough to not lose the real concepts they are supposed to represent. The models might be formal or transformable into formal ones, so reasoning can be done over them with the purpose of discovering any anomalies, incompleteness, or inconsistencies. Software engineering methodology is concerned not only about inventing and using modeling languages that can express what the system has to fulfil, and the software design, but rather it has to provide a process model for creating such models in turn.

Software agent that persistently observes the environment, interprets it, acts, and might communicate with other agents is a promising computing paradigm for implementing open complex systems. AOSE methodologies tend to analyse and design such kinds of complex systems in order to arrive finally to an agent-based implementation. There are several research groups working in developing their own AOSE methodologies [7]. The orientation towards agent does not mean that these methodologies use agency concepts and agent mentalistic notions along with all phases of developing software, rather the goal is to analyze and design in a way that leads to multi agent system. Only Tropos [18], as an AOSE methodology, uses the notions of agent and the related mentalistic notions from the early analysis down to the actual implementation.

As the use of computing is becoming an essential part of individuals' daily life together with business and organizations, and as we increasingly need to combine between different computing ends and parties, the need for software that is dynamic, flexible, adaptable, situated is more critical. The need for software evolution is becoming faster than software development process itself. Solving these challenges is based to a large extent on the way such software has to be engineered. Agent oriented software engineering is trying to arrive methods that enable developing a software can resist against evolving requirements, a software that is flexible enough to adapt and change fluently according to the new environments and requirements.

Fortunately, agent oriented software engineering, by contrast to object oriented software engineering and structured analysis and design, is not restricted or deeply influenced by some existing programming paradigm [19][20]. Agent

oriented software engineering research is now taking the initiative towards programming languages and infrastructures that serve the concepts suitable for software development instead of using those of existing programming languages in reverse unnatural way. Being limited to programming languages has enforced those previous software engineering practices to focus on the solution domain, since the concepts used are not those describing naturally requirements and problem domain. Agent oriented software engineering is growing together with agent oriented programming and agent infrastructure, this might fill the gap between problem and solution domains. Hopefully such consistency will make software development process faster, and lead to software can be easily evolved and maintained, and can adapt to different environments and requirements.

5 Exploiting agent paradigm for engineering AmI

Agent paradigm fits well for implementing AmI scenarios due to the coincidence between agent characteristics and AmI needs. Agent paradigm as a kind of abstraction is also capable of giving a good contribution with regards to AmI systems development, including analysis and design phases, besides the security issues. Securing an AmI ecosystem means fulfilling the security requirements of the owners of the different elements such as hardware, software and information involved in these ecosystems. One of the most important points is the lack of a model that can appropriately describe this type of sets of interrelated Security and Dependability goals, except agent-oriented approaches to system engineering. This fact together with the capability of these approaches to be extended and to be used at runtime with the help of automated tools, enhances one of the main appeals of agent technology for AmI ecosystems. On this way Software Agents can also be the basis for new security solutions. e.g. content protection [38] or multicast streaming video distribution [39]. In this section we will state our initial view of the agent oriented AmI engineering and securing.

5.1 Agent-oriented AmI development

As we explained previously, AmI shows a degree of complexity and multiple inter-related disciplines that require using special engineering paradigm. This need is coming from the new nature of such systems, where behavior is not known in details, or adequately controllable. AmI is distinguished by its dynamicity, openness, and complex inter-relations amongst environment components. Compared with object oriented software engineering practice, agent paradigm offers a higher level of abstraction suitable for engineering complex systems [21]. Agent paradigm enables engineering software at the knowledge level; at this level we talk of mental states, of beliefs instead of machine states, of plans and actions instead of programs, of communication, negotiation and social ability instead of direct interaction and I/O functionalities, of goals, desires, and so on [22].

Tackling the complexity of developing complex software can be done through some techniques such as 1) Decomposing the problem into smaller sub-problems

that can be managed more easily. 2) Using abstract models to represent system focusing on some concepts and relations, and omitting others unrelated. Such models should be compact and expressive in order to usefully summarize and even formalize what can be alternatively expressed by the natural languages. 3) Defining and managing the inter-relationships between problem solving components as they were an organization of some hierarchy [23].

As shown in [5], agent paradigm is not only useful as software construct but rather it can be used as a new way for analyzing and designing complex systems. Using the decomposition, abstraction and organization techniques to tackle the complexity of such systems can be done following agent paradigm from the early phases. Decomposing complex systems into related subsystems, each with its own thread of control, and own objectives to be achieved autonomously can be seen as a society of interacting agents. Agent paradigm provides a sort of abstraction to model problem domain in terms that are too consistent with solution domain. Subsystems are viewed as autonomous agents, agent social ability implies the interrelation at high level amongst those autonomous subsystems. This interaction might model cooperation, coordination, or negotiation amongst agents. The evolution of inter-relationships between components of complex systems and the different aggregation these components can be classified at different levels of abstraction match closely to agent and multi-agent system paradigm. As for the dynamic organization structure, agent paradigm has the expressivity to represent these concepts due to its explicit structure and flexible mechanisms. A methodology called Gaia [24] was developed to reflect such ideas providing a methodological way for engineering some kinds of complex systems.

Another attempt for using agent paradigm as conceptualization construct is based on BDI agent architecture, the world is viewed as a society of actors each has its own autonomy, and might depend on each others for task to be performed, goal to be achieved or resource to be provided [21]. Agent beliefs are the world model at the conceptual level, agent desires are translated into goals to be achieved, while the intention an agent might commit is considered as a plan. The multiple plans an agent might follow to achieve the same goal give some degree of flexibility for dealing with different contexts. Goals are analyzed through means-end analysis to conclude the actual actions by which goals are achieved. These actions are the actual requirements of the intended final software [25]. Tropos is another methodology was developed on the basis of these ideas, it uses agent mentalistic notion along all the phases of software development [18].

For engineering AmI, like for example smart campus, we need to decompose it into autonomous subsystems, and to abstract using knowledge level conceptualization rather than the fine grained one used by OO which is useful for predicted behavior and relatively static systems. With AmI we are not talking about an organization with one well defined behavior, business process, and straight control. Here the ambient is always changing and in an unpredictable way sometimes, so we need high degree of adaptability to cope with AmI going to serve everyday life scenarios with a lot of alternatives. Considering AmI as complex open system, we believe that agent paradigm and agent mentalistic no-

tions can contribute well for analyzing, and designing AmI scenarios rather than only implementing them.

5.2 Securing AmI ecosystems

We have shown that Agent-systems can bring important benefits especially in application scenarios where highly distributed, autonomous, intelligente, self organizing and robust systems are required. Furthermore, the high levels of autonomy and self-organization of agent systems provide excellent support for the development of systems in which dependability is essential. Both Ubiquitous Computing and Ambient Intelligence scenarios belong to this category. However, despite the attention given to this field by research community the agent technology has failed to gain a wide acceptance and has been applied only in a few specific real world scenarios. Security issues play an important role in the development of multi-agent systems and are considered to be one of the main issues to solve before agent technology is ready to be widely used outside the research community. However, we will show in this section that solutions are available for most of these problems. Furthermore, very promising technologies are currently under development (in some cases in a quite advanced phase) for the remaining problems. Consequently, our view is that the main reason why agent-oriented approaches have not gained wider acceptance is the lack of appropriate application scenarios. Precisely, AmI ecosystems are perfect scenarios for the application of agent approaches. With regards to security, agents present the most appropriate solution because they facilitate concealing disparate security requirements from different points in order to achieve each parts' goals in a collaborative setting. Of course, as mentioned above, we need to solve the most important security issues for general multi-agent systems.

Some of the general software protection mechanisms can be applied to the *protection of agents*. However, the specific characteristics of agents mandate the use of tailored solutions. First, agents are most frequently executed in potentially malicious pieces of software. Therefore, we can not simplify the problem as is done in other scenarios by assuming that some elements of the system can be trusted. Then, the security of an agent system can be defined in terms of many different properties such as confidentiality, non repudiation, etc. but it always depends on ensuring the correct execution of the agent on agent servers (a.k.a. agencies) within the context of the global environments provided by the servers [26].

Some protection mechanisms are oriented to the protection of the host system against malicious agents. More relevant approach is Sandboxing, a sandbox is a container that limits, or reduces, the level of access its agents have and provide mechanisms to control the interaction among them. Another technique, called proof-carrying code, [27]. For this purpose, every code fragment includes a detailed proof that can be used to determine whether the security policy of the host is satisfied by the agent. Therefore, hosts just need to verify that the proof is correct (i.e. it corresponds to the code) and that it is compatible with the local security policy.

Other mechanisms are oriented towards *protecting agents against malicious agencies*. Sanctuaries [29] are execution environments where a mobile agent can be securely executed. Most of these proposals are built with the assumption that the platform where the sanctuary is implemented is secure. Unfortunately, for agent-based systems this assumption is not applicable.

Several techniques can be applied to an agent in order to verify self-integrity in order to avoid that the code or the data of the agent is inadvertently manipulated. Anti-tamper techniques, such as encryption, checksumming, anti-debugging, anti-emulation and some others [30] [31] share the same goal, but they are also oriented towards the prevention of the analysis of the function that the agent implements.

Additionally, some protection schemes are based on self-modifying code and code obfuscation [32]. In agent systems, these techniques exploit the reduced execution time of the agent in each platform. Software watermarking techniques [33] are also interesting. In this case the purpose of protection is not to avoid the analysis or modification but to enable the detection of such modification. The relation between all these techniques is strong. In fact, it has been demonstrated that neither perfect obfuscation nor perfect watermark exists [34].

In summary, all these techniques provide short-term protection; therefore, in general they are not applicable for our purposes. However, in some scenarios, they can represent a suitable solution, especially, when combined with other approaches. Theoretic approaches to the problem have demonstrated that self-protection of the software is unfeasible [35].

In some scenarios, the protection required is limited to some parts of the software (code or data). In this way, the function performed by the software, or the data processed, must be hidden from the host where the software is running. Some of these techniques require an external offline processing step in order to obtain the desired results. Among these schemes, function hiding techniques allow the evaluation of encrypted functions [36]. This technique protects the data processed and the function performed. For this reason it is an appropriate technique for protecting agents. However, it can only be applied to the protection of polynomial functions.

The case of online collaboration schemes is also interesting. In these schemes, part of the functionality of the software is executed in one or more external computers. The security of this approach depends on the impossibility for each part to identify the function performed by the others. This approach is very appropriate for distributed computing architectures such as agent-based systems or grid computing, but has the important disadvantage of the impossibility of its application to off-line environments

Finally there are techniques that create a *two-way protection*. Some of these are *hardware-based*, such as the Trusted Computing Platform. With the recent appearance of ubiquitous computing, the need for a secure platform has become more evident. Therefore, this approach adds a trusted component to the computing platform, usually built-in hardware used to create a foundation of trust for software processes [37]. Other techniques are software-based, for instance

Protected Computing [39] approach. Protected Computing approach is based on the partitioning of the software elements into two or more dependent parts, then a part of this code will be remotely executed in a different agent.

6 Conclusions

AmI implies a shift from appliances that provide some functionality and can be utilized by external entity, towards appliances that have their own autonomy and know how to behave on behalf of humans without explicit request.

Abstractly speaking, this shift can be seen similar to the shift from object oriented towards agent oriented software paradigm. When we described AmI as a multidisciplinary paradigm, we discovered the similarity between AmI needs and Agent paradigm primitives. In AmI, each ambient appliance will behave like an agent that has character and can decide. Each appliance needs to be autonomous, reacting to environment changes, and taking the initiative towards fulfilling human needs in the correct moment and way. Appliances also need to settle down within an open environment of other appliances and need to communicate with them, so it needs some kind social ability.

Moreover, we consider AmI, that is intended to serve unpredictable everyday life scenarios and includes a spread of interacting appliances, as an open complex system that needs to be engineered using more advanced techniques than those tailored for well defined systems. We believe that agent paradigm is promising for developing AmI systems during all the development life cycle phases and not only for implementing them. Agent oriented software engineering methodologies have a good potential with respect to AmI; so the next step could be adapting some existing methodologies, or creating a new one, in order to engineer AmI at all phases of development life cycle from requirement gathering until the final implementation.

References

1. N. Streitz and P. Nixon. The Disappearing Computer. *Communications of The ACM*, March 2005/Vol. 48, No.3.
2. Krogstie, J., et al., Research Areas and Challenges for Mobile Information Systems. *International Journal of Mobile Communication*, 2004. 2(3).
3. Krogstie, J. Requirements Engineering for Mobile Information Systems. In *Proceedings of the Seventh International Workshop on Requirements Engineering: Foundations for Software Quality (REFSQ'01)*. 2001. Interlaken, Switzerland.
4. EU Project Report. ISTAG Scenarios for Ambient Intelligence 2010. <ftp://ftp.cordis.lu/pub/ist/docs/istagscenarios2010.pdf>
5. M. Wooldridge and N. R. Jennings, 'Intelligent agents: Theory and practice' *Knowl. Eng. Rev.*, vol. 10, no. 2, 1995.
6. M. Wooldridge. Agent-based Software Engineering. In *IEE Proceedings on Software Engineering*, 144(1), pages 26–37, February 1997.
7. Paolo Giorgini and B. Henderson-Sellers (Eds.) *Agent-Oriented Methodologies*, Idea Group Inc., 2005

8. Philips Research. Ambient Intelligence Research in ExperienceLab. http://www.research.philips.com/technologies/syst_softw/ami/
9. MIT Ambient Intelligence Research Group. <http://ambient.media.mit.edu/>
10. Mark Weiser. The Computer for the Twenty-First Century. *Scientific American*, pp. 94-10, September 1991.
11. Remagnino, P. and Foresti, G.L. Ambient Intelligence: A New Multidisciplinary Paradigm. *IEEE Transactions on Systems, Man and Cybernetics, Part A, Volume 35, Issue 1, Jan. 2005* Page(s):1 - 6.
12. A. Schmidt. Implicit Human Computer Interaction Through Context. *Personal Technologies Volume 4(2&3)*, June 2000. pp191-199.
13. A. Schmidt, K.A. Aidoo, A. Takaluoma, U. Tuomela, K. Van Laerhoven, W. Van de Velde. *Advanced Interaction in Context. The International Symposium on Handheld and Ubiquitous Computing (HUC99)*, Karlsruhe, Germany, 1999 & Lecture notes in computer science; Vol 1707, ISBN 3-540-66550-1; Springer, 1999, pp 89-101.
14. Anind K. Dey and Gregory D. Abowd. Towards a Better Understanding of Context and Context-Awareness. In the *Proceedings of the CHI 2000 Workshop on The What, Who, Where, When, and How of Context-Awareness*, The Hague, Netherlands, April 1-6, 2000.
15. Jolle Coutaz , James L. Crowley , Simon Dobson , David Garlan, Context is key, *Communications of the ACM*, v.48 n.3, March 2005
16. K. Lyytinen , Y. Yoo The Next Wave of Nomadic Computing: A Research Agenda for Information Systems Research. *Sprouts: Working Papers on Information Environments, Systems and Organizations. Vol. 1, Issue 1, Article 1 - 2001.*
17. N.R. Jennings. On Agent-Oriented Software Engineering. *Artificial Intelligence* 117 (2) 277-296 (2000).
18. P. Bresciani, P. Giorgini, F. Giunchiglia, J. Mylopoulos, A. Perini. TROPOS: An Agent-Oriented Software Development Methodology. *Journal of Autonomous Agents and Multi-Agent Systems. Kluwer Academic Publishers Volume 8, Issue 3, Pages 203 - 236, May 2004.*
19. J. Mylopoulos, L. Chung, and E. Yu. From Object-Oriented to Goal-Oriented Requirements Analysis. *Communications of the ACM*, 42(1):31-37, Jan. 1999.
20. J. Mylopoulos, Information modeling in the time of the revolution, *Information Systems*, v.23 n.3-4, p.127-155, May 1, 1998
21. E. Yu. Agent Orientation as a Modelling Paradigm. *Wirtschaftsinformatik. 43(2)* April 2001. pp. 123-132.
22. A. Perini, P. Bresciani, F. Giunchiglia, P. Giorgini, J. Mylopoulos. A Knowledge Level Software Engineering Methodology for Agent Oriented Programming. In the *Proceedings of the Fifth International Conference on Autonomous Agents*, Montreal, Canada - May 29 - June 01, 2001.
23. G.Booch "Object-Oriented analysis and design with applications" Addison Wesley (1994)
24. M. Wooldridge, N. R. Jennings, and D. Kinny. The Gaia Methodology for Agent-Oriented Analysis and Design. In *Journal of Autonomous Agents and Multi-Agent Systems. 3(3):285-312. 2000.*
25. A. Dardenne, A. van Lamsweerde and S. Fickas. Goal-Directed Requirements Acquisition. *Science of Computer Programming Vol. 20, North Holland, 1993*, pp. 3-50.
26. S. Berkovits, J. Guttman, V. Swarup. Authentication for Mobile Agents. *Mobile Agents and Security. Springer-Verlag Publishers Volume 1419, 1998*, pp 114-136.
27. G. Necula G. Proof-Carrying Code. *Proceedings of 24th Annual Symposium on Principles of Programming Languages. 1997.*

28. A. Gunter Carl, P. Homeier, S. Nettles. Infrastructure for Proof-Referencing Code. Proceedings of the Workshop on Foundations of Secure Mobile Code. March 1997.
29. Yee, Bennet S. A Sanctuary for Mobile Agents. Secure Internet Programming. 1999.
30. I. Schaum, H. Müller-Bichl, E. Piller. A Method of Software Protection Based on the Use of Smart Cards and Cryptographic Techniques. Proceedings of Eurocrypt. Springer-Verlag. LNCS 0209, pp. 446-454. 1984.
31. J.P. Stern, G. Hachez, F. Koeune, J.J. Quisquater. Robust Object Watermarking: Application to Code. Proceedings of Info Hiding, Springer-Verlag. LNCS 1768, pp. 368-378. 1999.
32. C. Collberg, C. Thomborson. Watermarking, Tamper-Proofing, and Obfuscation - Tools for Software Protection. University of Auckland Technical Report 170. 2000.
33. P. Wayner. Disappearing Cryptography. Information Hiding, Stenography and Watermarking. Morgan Kaufman. 2002.
34. B. Barak, O. Goldreich, R. Impagliazzo, S. Rudich, A. Sahai, S. Vadhan, K. Yang. On the (Im)possibility of Obfuscating Programs. Proceedings of CRYPTO. Springer-Verlag. LNCS 2139. pp. 1-18. 2001.
35. O. Goldreich. Towards a theory of software protection. Proceedings of the 19th Ann. ACM Symposium on Theory of Computing, pp. 182-194. 1987.
36. T. Sander, C.F. Tschudin. On Software Protection via Function Hiding. Proceedings of Information Hiding. Springer-Verlag. LNCS 1525. pp 111-123. 1998.
37. S. Pearson, B. Balacheff, L. Chen, D. Plaquin, G. Proudler. Trusted Computer Platforms. Prentice Hall. 2003.
38. A. Maña, J. Lopez, J. Ortega, E. Pimentel, J.M. Troya A Framework for Secure Execution of Software. International Journal of Information Security, Vol. 3, Issue 2, Springer-Verlag, 2004.
39. A. Maña, A. Muñoz Mutual Protection for Multiagent Systems. Proceedings of the Third International 3rd International Workshop on Safety and Security in Multiagent Systems. 2006.

EuroTRUSTAmI workshop : European
R&D towards trusted Ambient
Intelligence

Introduction

The EuroTRUSTAmI workshop was organised by the Serenity, a European integrated project dedicated to “system engineering for Security and dependability” with the help of an Advisory Committee¹, and with the active participation and involvement of 27 other IST European research projects and platforms² funded by the European Union in the context of the Sixth Framework Programme.

EuroTRUSTAmI aimed at providing a comprehensive vision of the European Research focused on the Projects that deal with advancing the AmI vision and providing secure and dependable computing environments in a context of open, heterogeneous and dynamic networks. Several research projects funded by the European Commission have already started to work towards the realization of secure ambient intelligence ecosystems from different perspectives and focusing on different technical aspects of the aforementioned problems. The EuroTRUSTAmI workshops provided a comprehensive and rigorous insight into these problems at 2 levels:

1. **Cooperative issues** by fostering synergies, identifying connections and collaboration avenues, between the European projects invited and other external interested parties. This cooperative workshop was structured in 3 parallel streams covering different types of issues:
 - (a) Designing, modelling and engineering for AmI and SOAs,
 - (b) Infrastructural and support aspects of AmI and SOAs,
 - (c) Foundational and theoretical aspects of AmI and SOA.

¹ EuroTRUSTAmI Advisory Committee

- Richard Bricaire, STM, in charge of dissemination activities on the Serenity project,
- Jean-Louis Carbonero, ST Microelectronics, MINAmI project coordinator,
- Dr Jean-Claude Laprie, LAAS-CNRS, ReSIST project coordinator,
- Professor Antonio Maña, U of Malaga and AmI.d Programme Committee co-Chair,
- Professor Yoram Ofek, U of Trento, RE-TRUST project Coordinator,
- Domenico Presenza, Engineering Informatica, Serenity project Coordinator,
- Aljosa Pasic, Atos Research & Innovation, in charge of the Security WG, NESSI ETP,
- Dr Carsten Rudolph, Fraunhofer Institute, AmI.d Programme Committee co-Chair,
- Pedro Soria-Rodriguez, Atos Research & Innovation, ESFORS project coordinator.

- ² **The 28 European projects and platforms** participating in EuroTRUSTAmI: AmIGO, ASK-IT, Biosecure, Discreet, EmBounded, EPoSS, ESFORS, Gredia, GridEcon, GridTrust, Hagggle, HYDRA, MINAmI, MONAmI, NESSI, One, Prime, R4egov, ReSIST, re-TRUST, S3MS, SENSE, Sensoria, Serenity, SMEPP, SWEB, UbiSec&Sens and WASP.

2. **Dissemination objectives** towards the academic research and professional communities interested in AmI developments. At Fall 2007 many of the invited projects were in the middle of their planned execution, and therefore the presentation and comparison of their objectives, approaches, progress and results is particularly rich and stimulating.

This report covering the Dissemination workshop only, presents the objectives, structure , state of progress and results of most of the participating projects at Fall 2007.

The Networked European Software and Services Initiative

Speaker: Aljosa Pasic, Atos Research & Innovation.

Summary

NESSI is the European Technology Platform on Software and Services - the Networked European Software and Services Initiative.

Launched in September 2005 by 13 partners and enlarged in June 2006 to 22 partners and over 200 members, NESSI aims to address the major changes that are driving the IT services marketplace. Indeed, today this marketplace is changing dramatically, due to a series of factors:

- Businesses and the Public Sector, which require flexibility to keep up with the ever increasing pace of change caused by globalisation and technological innovation.
- A continuing shift toward increasingly made-to-order solutions, which changes the balance of demand from products to services and from monolithic do-it-all applications to ad hoc service components and customised software solutions.
- The clear emergence of Open Source Software, which nourishes the dynamics of the ICT marketplace and creates an 'eco-system' that fosters opportunities by: increasing options and competition, aligning to open standards objectives, positioning software as a public good, improving technological self-reliance, increasing transparency, minimising security risk while optimising costs.
- The broader uptake by end-users, which is gaining momentum, leads to new needs such as ubiquitous access, ease of use, personalisation and trusted transactional capabilities on all types of platforms, from embedded systems to distributed environments.

NESSI aims to provide a unified view for European research in Services Architectures and Software Infrastructures that will define technologies, strategies and deployment policies fostering new, open, industrial solutions and societal applications that enhance the safety, security and well-being of citizens.

You can obtain more information visiting: <http://www.nessi-europe.com/>

Project Serenity

Speaker: Domenico Presenza, Engineering Informatica.

Summary

The primary goal of SERENITY IP proposal is to enhance security and dependability for AmI ecosystems by capturing security expertise and making it available for automated processing.

SERENITY will provide a framework supporting the automated integration, configuration, monitoring and adaptation of security and dependability mechanisms for such ecosystems. Technically, SERENITY will be based on (i) the enhanced notions of S&D Patterns and Integration Schemes, and (ii) the support for run-time pro-active and reactive monitoring of requirements. SERENITY focuses on five key areas to provide security and dependability mechanisms: (i) Organization & Business, (ii) Workflow & Services, and (iii) Network & Devices levels, (iv) provision of integrated solutions for these mechanisms and (v) support for run-time monitoring.

The results coming from these areas will be integrated to produce the SERENITY framework.

The results will be driven by the scenarios and the industrial requirements that will influence the research results to make them ready to be exploitable. The SERENITY framework will be made available as open source while other project results will form the basis of contributions to relevant standardisation bodies. Exploitation of results will be achieved through different routes but with the common theme of partners incorporating these results in current or planned products.

SERENITY brings together software companies, application solution developers and research institutions and will be driven by the need for security and dependability solutions in e-business, e-government and communication domains. SERENITY is integrated in the following ways:

- technically, through complementary focus areas addressed by strong research teams,
- industrially, through multi-sectors application partners who share a common vision for the
- potential of security issues,
- managerially, through a strong management structure based on entrepreneurial practices,
- internationally, with partners from 9 different countries,
- personally, through strong existing working relationships between partners.

Technologies

The main technologies involved in this approach are the following:

- Analysis of S&D solutions at different levels

- Modelling S&D, not only solutions but also, requirements, properties, context ...
- Development time support: solution discovery, selection, adaptation and integration
- Runtime support: solution selection and dynamic management
- Runtime monitoring: in open , distributed and uncontrolled scenarios

Expected results

To develop mechanisms and tools for the semi-automated provision of security and dependability in Aml ecosystems

- by capturing the security and dependability expertise in the enhanced concept of Security and Dependability Patterns and Integration Schemes,
- with an approach cutting through and integrating from Business Organisation to Network levels.

Useful data

Project name	System Engineering for Security and Dependability
Acronym	SERENITY
Funded by	European Commission (VI FP)
Contract	IST-027587
Type of project	Integrated Project
Budget	Total cost: 13,1 Million euros / Funding: 7,8 Million euros
Contacts	Coordinator: Domenico Presenza (domenico.presenza@eng.it) Dissemination: Richard Bricaire (rbricaire@strategiestm.com) Scientific: Antonio Maña (amg@lcc.uma.es)
Projects websites	www.serenity-project.org www.serenity-forum.org
Duration	January, 2006 - December, 2009
Partners	Engineering Ingegneria Informatica S.p.A (Italy), Athens Technology Center (Grece), ATOS (Spain), City University of London (United Kingdom), Deep Blue (Italy), Fraunhofer Gesellschaft zur Frderung der angewandten Forschung e.V (Germany), Katholieke Universiteit Leuven (Belgium), NOKIA (Finland), Telefonica I+D (Spain), SAP AG (Germany), Security Technology Competence Centre (Slovenia), Stratgies Telecoms & Multimedia (France), Thales (France), Universit di Trento (Italy), University of Aegean (Grece) y University of Málaga (Spain).

Project SMEPP

Speaker: Jose Luis Serrano Martin, Tecnatom.

Summary

The main objective of this project is to develop a new middleware, based on a new network centric abstract model, specially designed for the above described scenario, and trying to overcome the main problems of the currently existing domain specific middleware proposals. The middleware will be secure, generic and highly customizable, allowing for its adaptation to different devices (from PDAs and new generation mobile phones to embedded sensor actuator systems) and domains (from critical systems to consumer entertainment or communication). Its suitability will be demonstrated by the development of two different innovative real-life applications in the domains of Home Systems, Mobile Telephony and Environmental Monitoring in Industrial Plants.

Technologies

The main technologies involved in this approach are the following:

- Abstract Models for Interaction and Service Orientation.
- Middleware Architecture and Infrastructure.
- Security.
- Peer-to-peer.
- Wireless Sensor Networks.

Expected results

The result of this project will be a new middleware, based on a new network centric abstract model, specially designed for the above described scenario, and trying to overcome the main problems of the currently existing domain specific middleware proposals. The middleware will be secure, generic and highly customizable, allowing for its adaptation to different devices (from PDAs and new generation mobile phones to embedded sensor actuator systems) and domains (from critical systems to consumer entertainment or communication). Its suitability will be demonstrated by the development of two different innovative real-life applications in the domains of Mobile Telephony and Environmental Monitoring in Industrial Plants.

Useful data

Project name	Secure Middleware for Embedded Peer-to-Peer Systems
Acronym	SMEPP
Funded by	European Commission (VI FP)
Contract	IST-5-033563
Type of project	STREP
Budget	Total cost: 4,4 Million euros / Funding: 2,9 Million euros
Contacts	Coordinator: Manuel Díaz (mdr@lcc.uma.es) Dissemination: Manuel Díaz (mdr@lcc.uma.es) Scientific: Manuel Díaz (mdr@lcc.uma.es)
Projects websites	www.smepp.org
Durantion	September 2006 - September 2009
Partners	University of Málaga (Spain), Tecnatom, S.A. (Spain), University of Pisa (Italy), Technical University of Graz (Austria), Siemens (Germany), Telefonica I+D (Spain), Institute for Info-comm Research (Singapur)

Project Discreet

Speaker: Giuseppe Bianchi, Università degli Studi di Tor Vergata.

Summary

Pervasive technology poses a serious risk on the user privacy rights. The collection of personal and contextual data, in particular when integrated over various information sources, and their disclosure to various infrastructure operators and service providers (not to mention malicious intruders), may turn out as a serious obstacle for the practical deployment of pervasive services. In this context, the IST-Discreet project is motivated by the following fundamental questions: Is pervasive technology forcing users to waive their privacy rights? And how much of our privacy can be traded for security and/or new service opportunities?

The Discreet project aims at contributing to break what we argue to be a false dichotomy, in which systems designers force their users to sacrifice some part of a fundamental right - their privacy - in order to gain some utility - the use of the application. Our belief is that ICT technology can play a crucial role in pushing forward the growth and spreading of new pervasive technologies, if it technically addresses privacy issues. A fundamental, and quite challenging, research task consists in designing tools and solutions that, in the same time, either provide advanced service opportunities and benefits to the end users, meanwhile not introducing threats on the users' fundamental privacy rights. This can be accomplished by designing technical solutions capable of minimize and control the amount, the type, and the way personalized information is made available to the equipments and/or entities involved in the service provision. Moreover, Discreet aims at further taking into account the many legal and regulatory issues emerging when dealing with the fundamental right of the users to their privacy, as well as the applicability of such technologies.

To face these challenges, Discreet challenges the multiplicity of privacy enhancement technologies and solutions deemed necessary, according to a "layered" view.

- At the bottom layer, environment enhancements are deemed necessary to protect the user personal data as soon as they are gathered. In fact, any well-designed intermediary brokerage system, despite its complexity and completeness, cannot solve the issue of protecting the data when they are acquired from the environment (e.g. active data acquired from RFID tags, indeed an important research area in the project, of passive data gathered from video-surveillance cameras) and when they are delivered through an access network or through a network of sensors.
- Protection of the delivered information against external threats and attackers is dealt with at another layer referred to as "layer 1". This includes enhancements of traditional widely employed communication security protocols to protect against communication address disclosure and, even more critical, against powerful statistical traffic analysis attacks which cannot be circumvented by "just" encryption.

- “Layer 2” aims at providing a number of techniques to manage the user identity and authorization credentials according to an user-centric fully distributed approach. As such it encompasses both a novel blind authorization approach based on a two-party-only protocol for both credential assignment and verification, as well as a distributed pseudonym system which does not rely on any centralized entity for pseudonym assignment and/or verification, but nevertheless retains the fundamental property of providing means to revert the assigned pseudonym when e.g., mandated by regulatory provisions.
- Finally, “layer 3” goal is to develop a distributed middleware framework devised to run-time control and regulate the disclosure/protection of data from entities that are internal to service provision and communication. The most critical function provided by the middleware is the detailed control exerted on how, to whom, and under which conditions and in which specific context, a specific information data should be disclosed. The approach taken to achieve this level of intelligence in Layer 3 is to express the information model as an ontology of personal data together with services, access restrictions, handling policies, protective measures and actors. Furthermore, a unique feature of Discreet is its attempt to incorporate in such an information model a semantic description of regulatory provisions concerning data protection.

Technologies

Discreet challenges a variety of different technologies.

- At the environment enhancement layer, key technologies are primarily RFID systems and video-surveillance technologies, plus some punctual privacy enhancements in both Sensor networks and Ad Hoc networks.
- Data communication protection at layer 1 is specifically focused on the backward-compatible enhancement of IPsec, specifically chosen because of its more general applicability with respect to transport-layer solutions (such as TLS), and because of its widespread deployment and its growing importance also on portable devices.
- Again with the goal of retaining backward compatibility, layer 2 pseudonymization and authorization solutions are developed over X.509 certificates, when necessary enhanced with proprietary extensions. The novel blind signature approach used in the authorization, to date, still relies on RSA (extensions over elliptic curves in progress).
- Layer 3 uses a customized XML language called DPL (Discreet Privacy Language). Widely adopted standards are used for the Ontology description (W3C OWL) and its querying (RDQL with a Pellet Reasoner). Finally, messaging is based on HTTP.

Expected results

The following results have been produced (or at late stage of implementation) by the Discreet activities:

- An RFID reader devised to protect the data delivery from the RFID tag with pseudorandom channel noise;
- A ContactLess Privacy Manager, namely an RFID tag similar to a blocker-tag, but selectively programmable to permit individual tag's reading;
- An original design of a lightweight public key encryption mechanism based on a variant of McEliece, and its application to multi-path transmissions;
- A probabilistic routing mechanism for location privacy in sensor networks;
- A Traffic Flow Confidentiality protocol extension for IPsec, developed as an "handler" (i.e. similarly to AH/ESP), and devised to masquerade the traffic pattern according to programmable profiles;
- An IPsec "telescope" extension to provide anonymous routing;
- A PKI-like X.509 certificate based distributed pseudonym assignment infrastructure;
- A novel RSA-based blind signature approach, called "marked blind signature", devised to include an unforgeable random value inside the signed message, and its application to a two-party authorization credential assignment and verification;
- A policy-based middleware infrastructure for the control, selective disclosure, and run-time filtering (obfuscating) of the data information conveyed by the end user;
- An ontology of Privacy providing the semantic description of the user data, services, access restrictions, and regulatory provisions, through which middleware policies are produced;
- An User Privacy Manager complementing the middleware framework and providing privacy protection wrappings (privacy locks) for the user data;
- A Graphical User Interface to allow the user to visualize and customize the level of privacy provided by the system;
- The integration of face blurring/de-blurring mechanisms into a video-surveillance framework controlled by the Discreet Middleware.

Useful data

Project name	Discreet Service Provision for Smart Environments
Acronym	DISCREET
Funded by	European Commission (VI FP)
Contract	IST-027679
Type of project	STREP
Budget	Total cost: 3,8 million euro; Funding: 2,3 million euro
Contacts	Coordinator: Giuseppe Bianchi (Giuseppe.bianchi@uniroma2.it) Dissemination: Francesca Gaudino (Francesca.gaudino@bakernet.com) Scientific: Giuseppe Bianchi (Giuseppe.bianchi@uniroma2.it)
Projects websites	www.ist-discreet.org
Duration	December, 2005 - February, 2008
Partners	Centro Nazionale Interuniversitario per le Telecomunicazioni (Italy), Baker&McKenzie (Italy), CEA-LETI (France), Cocalis & Psarras (Greece), Eyeled (Germany), Institute of Communication and Computer Systems / National Technical University of Athens (Greece), Thales Communications (France), Star-Beam s.r.l. (Italy), Ludwig Maximilian University (Germany), University of Surrey (UK).

Project EmBounded

Speaker: Kevin Hammond, University of Saint-Andrews.

Summary

Embedded systems form an increasingly important part of the European, and indeed the global, software economy. The aims of the EmBounded project are to identify, to quantify and to certify resource-bounded code in a domain-specific high-level programming language for real-time embedded systems. Using formal models of resource consumption as a basis, the project will develop static analyses for time and space consumption and assess these against realistic applications for embedded systems, including a vision-based control system for a RobuCar autonomous vehicle. The work is novel in combining analyses of both source and machine code into a single framework.

We envisage future real-time embedded system software engineers programming in very high-level functionally-based programming notations, whilst being supported by automatic tools for analysing time and space behaviour. These tools will provide automatically verifiable certificates of resource usage that will allow software to be built in a modular and compositional way, whilst providing strong guarantees of overall system cost. In this way, we will progress towards the strong standards of mathematically-based engineering that are present in other, more mature, industries, whilst simultaneously enhancing engineering productivity and reducing time-to-market for embedded systems.

The research builds on world-class expertise in four complementary and active research areas: high-level resource prediction (LMU and St Andrews); precise costing of low-level hardware instructions (AbsInt GmbH); domain-specific languages and implementation (Heriot-Watt and St Andrews); and the design and implementation of real-time embedded systems applications, in particular in the area of computer vision algorithms for autonomous vehicles (Universit   Blaise-Pascal and Heriot-Watt). It is especially timely in building on newly-emerging theoretical results in predicting resource usage, in exploiting state-of-the-art cost models of embedded hardware and in utilising recent developments in computer vision algorithms for controlling autonomous vehicles.

Technologies

The main technologies involved in the EmBounded project are:

- formal cost models capable of attaching time and space cost;
- formally derived static analyses, capable of producing guaranteed upper-bound cost information in the presence of advanced language features such as recursion and garbage collection;
- dependent type frameworks for associating formally verifiable safety and security information to program text;
- AbsInt’s aiT tool for producing guaranteed worst-case execution times;

- the domain-specific Hume language, which combines finite-state automata with purely functional programming, as a testbed for guaranteed program behaviour.

Expected results

We anticipate that the EmBounded project will enable several research advances to be made:

- i) it will develop compositional resource certificates for embedded systems;
- ii) it will synthesise resource cost models from both source and machine levels, so enabling more accurate modelling than is possible individually;
- iii) it will extend theoretical cost modelling technology to recursive, higher-order and polymorphic functions;
- iv) it will characterise software development using constructs with well defined formal and analytic properties in the context of realistic applications;
- v) it will represent the first serious attempt to apply modern functional programming language technology to hard real-time systems, including complex industrially-based applications.

As a minimum outcome, we expect to produce a set of certified models and analyses that will determine upper bounds on time and space costs for a range of useful primitive recursive function forms. We should also have determined the accuracy of these models both against some representative computer vision algorithms that have been adapted to the analyses, and against some representative, simple real-time control applications that have been written in Hume. In this way we will have made a step towards ensuring the practical application of functional programming technology in a real-time, hard-space setting.

Useful data

Project name	Automatic Prediction of Resource Bounds for Embedded Systems
Acronym	EmBounded
Funded by	European Commission (VI FP)
Contract	IST-510255
Type of project	Specific Targeted Research Project (FET-Open)
Budget	Total cost: 1,6 Million euros / Funding: 1,3 Million euros
Contacts	Coordinator: Kevin Hammond (kh@cs.st-and.ac.uk)
Projects websites	www.embounded.org
Duration	March, 2005 - February, 2008
Partners	University of St Andrews (UK); Heriot-Watt University (UK); AbsInt GmbH (Germany); Ludwig-Maximilians-Universität, München (Germany); Université Blaise-Pascal, Clermont-Ferrand (France).

Project HAGGLE

Speaker: Melek Önen, Institut Eurecom.

Summary

Haggle is a new autonomic networking architecture designed to enable communication in the presence of intermittent network connectivity, which exploits autonomic opportunistic communications (i.e., in the absence of end-to-end communication infrastructures).

We propose a radical departure from the existing TCP/IP protocol suite, completely eliminating layering above the data-link, and exploiting and application-driven message forwarding, instead of delegating this responsibility to the network layer. To this end, we go beyond already innovative cross-layer approaches, defining a system that uses real best-effort, context aware message forwarding between ubiquitous mobile devices, in order to provide services when connectivity is local and intermittent. We use only functions that are absolutely necessary and common to all services, but that are sufficient to support a large range of current and future applications, more oriented to the human way of communicating (and, more generally, the way communities of any type of entities communicate), rather than related other technological aspect of the communication.

The complex networking architecture adopted by the project suggests that investigation on system security will be performed in multiple stages. Security cannot be considered as an independent module of the system. Rather, it will be a feature that will support the whole infrastructure. The objective of this WP4 Security WorkPackage in HAGGLE is to provide secure communication means within communities using automated mechanisms for the creation of trust relationships and to foster collaboration among parties that are not necessarily bound by a joint management infrastructure.

A user can be part of multiple communities and may have different roles, preferences, and relations in each of them. To be able to create trusted relations among parties that do not share any a priori trust relationship, users rely on trust establishment protocols. Trust establishment protocols are crucial to the community concept that is the key building block in the proposal. A concept that nicely fits with the underlying opportunistic networking model is offered by optimistic security protocols whereby some communication with trusted third parties might be required but the correctness of the security protocol does not require on-line connectivity.

Providing support for secure communications between members of a community as well as incentive mechanisms to encourage peers to perform a fair share of basic networking operations like forwarding packets and requests are other key factors that need to be addressed in order to make the opportunistic networking paradigm realistic. Inducing cooperation between community members can be based on distributed reputation systems whereby only peers with a good reputation record are admitted by other peers.

Guaranteeing fairness in the community however does not protect against attacks aiming at corrupting the integrity and confidentiality of messages being forwarded between peers. However, if basic security services that provide message integrity and confidentiality can be based on traditional security mechanisms, forwarding requests and messages without accessing their content is a hard problem that relies on solutions for computing with encrypted functions and homomorphic encryption. Design of practical solutions amenable to applications such as opportunistic networking is an open problem that calls for a judicious blending between protocol complexity and realistic design choices imposed by the underlying communication model.

Expected results

The objectives of the Security Workpackage are as follows:

- 1) to provide automated mechanisms for the establishment of trust relationships among peer parties.
- 2) to foster collaboration among parties that are not necessarily bound by a joint management infrastructure.
- 3) to assure the security of the Hagggle communication mechanisms in the face of malicious attacks such as masquerade, eavesdropping and denial of service.

Useful data

Project name	An innovative paradigm for autonomic opportunistic communication
Acronym	HAGGLE
Funded by	European Commission
Contract	IST-027918
Type of project	Integrated Project
Budget	Total EC contribution = 4,400,000 euros
Contacts	Coordinators: Christophe Diot - Thomson SA Martin POTTS - Martel Consulting
Projects websites	http://www.hagggleproject.org
Duration	January, 2006 - December, 2010
Partners	- Thomson SA, The Chancellor, Master and Scholars of the University of Cambridge, Uppsala Universitet, Ecole Polytechnique Federale de Lausanne, Scuola Universitaria Professionale dell Svizzera Italiana, Consiglio Nazionale delle Ricerche, Institut Eurecom, Martel GMBH, INTEL (UK)

Project GridTrust

Speaker: Alvaro Arenas, STFC.

Summary

The overall objective of the GridTrust project is to develop the technology to manage trust and security for the Next Generation Grids (NGG). We propose to have a vertical approach tackling issues of trust, security and privacy (TSP) from the requirements level down to the application, middleware and foundation levels. Our emphasis is on models, tools and services to assist in reasoning about trust and security properties along the NGG architecture.

GridTrust develops a framework to enforce advanced TSP policies in Grids. The framework is based on a general model of security called usage control. The general usage control model can be tailored to implement well known access control policies such as role-based access control, or more advanced dynamic security policies such as Chinese walls and history-based access control.

GridTrust aims to overcome the trust and security risks in Grid environments bringing closer scientific and business worlds. The project output is a security framework to define, efficiently evaluate, and enforce security policies derived by the TSP requirements specified by the user. The set of GridTrust trust and security services will be compliant with the Open Grid Services Architecture (OGSA).

The Grid was initiated as a way of supporting scientific collaboration, where many of the participants knew each other. In this case, there is an implicit trust relation, all partners have a common objective and it is assumed that resources would be provided and used within some defined and respected boundaries. However, when the Grid is intended to be used for business purposes, it is necessary to share resources with unknown parties. Such interactions may involve some degree of risk since the users cannot distinguish between high and low quality resource providers on the Grid. GridTrust mitigates this risk by developing trust and security components.

The GridTrust framework will be validated in four scenarios: supply-chain systems for both the pharmaceutical and the fish-market domains; inter-enterprise knowledge management; and distributed authoring in the media domain.

Technologies

Usage Control Techniques: The UCON model developed by Park and Sandhu is central to the project, being adapted and extended for Grid computing.

- Security Requirements: A goal-oriented requirements engineering methodology (KAOS) is used to model security requirements for Grid-based applications.
- Model-Based Refinement: The formal specification language Event-B is used to model VOs and to refine them into more concrete/operational ones.

- Policy Refinement: One challenge in the project is policy design, covering derivation of policies from requirements, as well as refinement of abstract policies into concrete ones.
- Monitoring Services: Execution services will exploit monitoring services to monitor several aspects such as resource usage, or the behaviour of a computational application.
- Meta-Schedulers: Current meta-schedulers will be exploited to allocate resources according to security properties of the requested application.
- Eclipse: All design-level tools will be integrated into the Eclipse IDE.
- Globus Middleware: All services developed into the project will be integrated into the Globus middleware.

Expected results

GridTrust will produce a security framework that consists of the following components.

- Secure VO Requirements Editor and Policy Generator Tool.

This is a requirements-engineering tool tailored for Grid security requirements. The tool is based on the goal-oriented requirements methodology KAOS and gives a global and detailed view of the VO being developed by identifying the VO goals; the roles and responsibilities of the VO participants; and the services and resources used in the VO. The tool allows one to model an attacker at requirements level as well as security properties of a VO. The tool includes a library of security requirements patterns that a VO designer can use to express the required security properties. The output of the tool is an abstract model of a VO, its identified security requirements, and associated abstract policies.

- VO Model and Policy Refinement Tool.

This tool allows VO designers to refine an abstract VO model to more concrete and operational VO models. The tool takes as input an abstract VO model, such as the one produced by the Secure VO Requirements Editor, and produces a more concrete VO architecture close to implementation. Policies in abstract VO models are usually expressed in the language of the stakeholders (VO users, business modellers) and need to be transformed into an implementable computational policy language. The tool is based on the event-B specification language, exploiting event-B tools such as refine and model checkers.

- Usage Control Service.

The GridTrust Usage Control Service improves the security of the Grid by integrating into the security architecture a component that performs a continuous usage control of Grid services by monitoring the behaviour of the applications executed on behalf of grid users. This component enforces a fine grain security policy that consists in a highly detailed description of the correct behaviour of the applications executed on computational services. Only the applications

whose behaviour is consistent with the security policy are executed on the computational resource. The continuous usage control service will be integrated into the Globus middleware.

- Secure-Aware Resource Broker Service.

The secure resource broker service integrates access control with resource scheduling. In Grid systems, both resource owners and users define their resource access and usage policies. The resource broker schedules a user request only within the set of resources whose policies match the user credentials (and vice-versa). The service extends traditional VO management services with secure scheduling functionalities, and will be integrated into the Globus middleware.

- Reputation Management Service.

The GridTrust reputation management service collects, distributes, and aggregates feedbacks about entities' behaviour in a particular context in order to produce a rating about the entities. Entities could be either users, resources / services, service providers or VOs. The reputation service is based on ideas of utility computing, and can be used in both centralised and distributed settings. The reputation service will be also integrated into the Globus middleware.

Useful data

Project name	Trust and Security for Next Generation Grids
Acronym	GridTrust
Funded by	European Commission (VI FP)
Contract	IST-033817
Type of project	Specific Targeted Research Project
Budget	Total cost: 3,8 Million Euro / Funding: 2,2 Million Euro
Contacts	Coordinator: Philippe Massonet, CETIC, Belgium (p hm@cetic.be) Dissemination: Daniel Rodriguez, Moviquity, Spain (drp@moviquity.com) Scientific: Alvaro Arenas, STFC RAL, UK (A.E.Arenas@rl.ac.uk)
Projects websites	www.gridtrust.eu
Duration	June, 2006 - May, 2009
Partners	Centre d'Excellence en Technologies de l'Information et de la Communication - CETIC (Belgium), HP European Innovation Center (Italy), Istituto di Informatica e Telematica - Consiglio Nazionale delle Ricerche - IIT-CNR (Italy), Istituto Geografico De Agostini (Italy), Interplay Software (Italy), Moviquity (Spain), Science and Technology Facilities Council - STFC (UK), Vrije Universiteit Amsterdam (Netherlands).

Project ReSIST

Speaker: Jean-Claude Laprie, LAAS-CNRS.

Summary

ReSIST integrates leading researchers active in the multidisciplinary domains of Dependability, Security, and Human Factors, in order that Europe will have a well-focused coherent set of research activities aimed at ensuring that future 'ubiquitous computing systems', the immense systems of ever-evolving networks of computers and mobile devices which are needed to support and provide Ambient Intelligence (AmI), have the necessary resilience and survivability, despite any residual development and physical faults, interaction mistakes, or malicious attacks and disruptions. The objectives of the Network are:

- 1) Integration of teams of researchers so that the fundamental topics concerning scalably resilient ubiquitous systems are addressed by a critical mass of co-operative, multidisciplinary research.
- 2) Identification, in an international context, of the key research directions (both technical and socio-technical) induced on the supporting ubiquitous systems by the requirement for trust and confidence in AmI.
- 3) Production of significant research results (concepts, models, policies, algorithms, mechanisms) that pave the way for scalably resilient ubiquitous systems.
- 4) Promotion and propagation of a resilience culture in university curricula and in engineering best practices.

The current state-of-knowledge and state-of-the-art reasonably enable the construction and operation of critical systems, be they safety-critical (e.g., avionics, railway signalling, nuclear control) or availability-critical (e.g., back-end servers for transaction processing). The situation drastically worsens when considering large, networked, evolving, systems either fixed or mobile, with demanding requirements driven by their domain of application. There is statistical evidence that these emerging systems suffer from a significant drop in dependability and security in comparison with the former systems. There is thus a dependability and security gap opening in front of us that, if not filled, will endanger the very basis and advent of Ambient Intelligence (AmI).

Filling the gap clearly needs dependability and security technologies to scale up, in order to counteract the two main drivers of the creation and widening of the gap: complexity and cost pressure.

Research activities will be re-structured and re-shaped according to the resilience scaling technologies: evolvability, assessability, usability, diversity.

The move towards resilience scaling technologies will be accompanied and facilitated by resilience integration technologies: a) a resilience knowledge base, and b) a resilience-explicit computing approach.

First year results

The two major achievements of the first year of activity have been the production of a) the State of Knowledge in Resilience-Building Technologies, and of b) a prototype of the Resilience Knowledge Base.

The work for producing the State of Knowledge in Resilience-Building Technologies has been divided among five working groups (each with active participation from the ReSIST partners that work in the corresponding research area) dealing with different aspects of resilience building and the corresponding sub-disciplinary areas. The document is therefore made up of five parts, each produced by one of the working groups:

- Resilience architecting and implementation paradigms.
- Resilience algorithms and mechanisms.
- Resilient socio-technical systems.
- Resilience evaluation.
- Resilience verification.

This state of knowledge document is co-authored by 66 researchers and doctorate students. The Resilience Knowledge Base (RKB) is intended to provide a semantic web environment for effective access to a body of knowledge on resilience concepts, methods and tools. The current prototype RKB contains 40 millions basic facts.

In addition to the above facts, ground work has been performed on the preparation of a) coming events, such as the Open Workshop (21-22 March 2007 in Budapest) and the Summer School (24-28 September 2007 in Porquerolles island) or b) deliverable production, such as the Research Agenda (that will constitute a deliverable due in June 2007, entitled: “From Resilience-Building to Resilience-Scaling Technologies: Directions”), the Resilience-Explicit Computing approach, the Resilience Ontology, the Best Practice Document, the Curriculum in Resilient Computing.

Useful data

Project name	Resilience for Survivability in IST
Acronym	ReSIST
Funded by	European Commission (VI FP)
Contract	026764
Type of project	Network of Excellence
Budget	Funding: 4,5 Milion Euros
Contacts	Coordinator: Jean-Claude Laprie, LAAS-CNRS (laprie@laas.fr) Dissemination: Luca Simoncini, University of Pisa (luca.simoncini@isti.cnr.it)
Projects websites	http://www.resist-noe.eu
Duration	January, 2006 - December, 2008
Partners	LAAS-CNRS (FR), Budapest University of Technology and Economics (HG), City University (UK), Technische Universität Darmstadt (DE), Deep Blue Srl (IT), Institut Eurecom (FR), France Telecom Recherche et Développement (FR), IBM Research GmbH (CH), Université de Rennes 1 - IRISA (FR), Université de Toulouse III - IRIT (FR), Vytautas Magnus University (LT), Fundação da Faculdade de Ciências da Universidade de Lisboa (PT), University of Newcastle upon Tyne (UK), Università di Pisa (IT), QinetiQ Limited (UK), Università degli studi di Roma "La Sapienza" (IT), Universität Ulm (DE), University of Southampton (UK)

Project MINAmI

Speaker: Pascal Ancey, ST Microelectronics.

Summary

MINAmI project addresses challenges related to the implementation of Ambient Intelligence (AmI) applications, where the personal mobile device acts as a gateway. MINAmI will expand the open technology platform developed in MIMOSA project and will demonstrate and validate new Ambient Intelligence applications. The centre of interest and the major innovative work in MINAmI are focused on the final concrete demonstrators for AmI, based on the development of an innovative state-of-the art micro/nanotechnology technological platform.

The main technical innovations in MINAmI are in the development of:

- Mass-memory RF Tags based on low power innovative technologies.
- Event sensitive RF nodes including new-low-cost time reference for time stamping function.
- Thin film rechargeable batteries and a wide range of low-cost and low-power nano and micro sensors and actuators, including, 9D integrated Inertial Measurement Unit and 3D distributed vision system.

In MINAmI, a global platform taking into account the constraints of integration, industrialisation and compatibility with advanced CMOS platforms will integrate these technologies. MINAmI links demonstration, validation & exploitation.

MINAmI Vision:

With the MINAmI Ambient Intelligence system, the physical environment can be loaded with interesting and context-related information, easily and naturally accessible to the user. Information is in the tags and sensors embedded in physical surroundings and everyday objects, and it can be anything from sensor measurements from the environment or the user itself, to a piece of music or the latest news. The user can wirelessly access this information content by just touching or scanning close tags and sensors with their mobile phone. The phone also enables wireless connection to the internet. As the interaction can be tied to a specific place, object, and time, the user is served with context-related information and services.

Technologies

Demonstrators developed in MINAmI:

- Drugs monitoring and conditioning aims at developing a smart pill box offering to patients an alert service when their use of medication dangerously differs from the prescription.
- Health monitoring and homecare will demonstrate the feasibility of an ultra light EEG data logger that can be downloaded every 24 hours through a passive RFID link.

- Assistive listening device will show how smart acoustic sensor arrays may help hearing instruments users to focus on relevant audio data (voice recognition, sound localisation).
- Data downloading from passive tags will demonstrate that people can consume a large amount of off-line digital data such as music, videos, games etc. The data is downloaded from a memory tag module to a reader module. Reader technology will eventually be integrated in to various kinds of personal devices such as mobile phones and multimedia computers (PDAs). In the future, a multimedia memory tag can even be embedded in magazines.
- Ambient sensors for friendly home applications will explore the feasibility of extracting data from distributed vision sensors and other smart sensors to bring information to users in home services related to automation, security and homecare.
- Virtual optical user interface will demonstrate how small devices such as cell phones will be able to become gateways to AmI applications where bigger screens and faster input devices may be required. The demonstration will be based on a tiny projection system that activates an optical keyboard and/or a projected touch enabled display.

Expected results

Potential Impact

EU is confronted with significant changes arising from globalisation and the challenges of new knowledge-driven economy, information and communication technologies have the potential to enhance every aspect of people's lives. In this way MINAmI will contribute to the European competitiveness by developing new competitive technologies and components almost "mandatory" to realise the AmI vision. Moreover, the applications developed in MINAmI can help not only to modernise the European social model in terms of healthcare, leisure and work opportunities but also to promote and accelerate acceptance of AmI ideas in Europe. Last but not least, MINAmI will take a holistic view of AmI, considering not just the technology but the whole of the innovation supply chain from usage and ethical assessment to demonstration and validation of applications.

Ethical issues in MINAmI

Ethical concerns regarding the vision and products of the project as well as the user evaluations carried out within the project are dealt with the two-fold ethical management structure of MINAmI. The project's internal Ethical Committee reviews the user evaluation activities carried out within MINAmI with regard to ethical concerns. The Ethical Committee prepares and maintains an ethical guideline document for the user evaluations and deals with ethical problems that may come up during the project work. The ethical concerns which arise and their solutions are reported annually. An Ethical Advisory Board includes external experts of different fields of ethics. The Ethical Advisory Board assists the project to identify and evaluate broader ethical implications related to the project vision, goal, and forthcoming products. The Board contributes

to the Ethical guidelines for mobile-centred Ambient Intelligence that MINAmI project maintains.

Useful data

Project name	Micro-Nano integrated Platform for Transverse Ambient Intelligence applications
Acronym	MINAmI
Funded by	European Commission (VI FP)
Contract	34690
Type of project	Integrated Project
Budget	Total cost : 19,6 Million euros / Funding : 10,2 Million euros
Contacts	Coordinator: Jean-Louis CARBONERO (jean-louis.carbonero@st.com) Dissemination: Adrian IONESCU (adrian.ionescu@epfl.ch) Scientific : Pascal ANCEY (pascal.ancey@st.com)
Projects websites	www.fp6-minami.org
Duration	October, 2006 - September, 2009
Partners	AARDEX International Ltd (Switzerland), Alma Consulting Group (France), Centre Suisse d' Electronique et de Microtechnique SA (Switzerland), Commissariat a l'Energie Atomique - LETI (France), Ecole Polytechnique Fédérale de Lausanne (Switzerland), Fraunhofer-Institut für Siliziumtechnologie (Germany), GE Healthcare Finland Oy (Finland), HAGER security SAS (France), LUMIO Ltd. (Israel), NOKIA OYJ (Finland), OTICON A/S (Denmark), SONION MEMS A/S (Denmark), STMicroelectronics SA (France), STMicroelectronics S.l.r. (Italy), Telefónica Investigación y Desarrollo S.A.U. (Spain), VTT - Technical Research Centre of Finland (Finland)

Project MonAMI

Speaker: Antonio Kung, Trialog.

Summary

The overall objective of MonAMI is to mainstream accessibility in consumer goods and services, including public services, through applied research and development, using advanced technologies to help ensure equal access, independent living and participation for all in the Information Society.

As costs for society for support to elderly persons and persons with disabilities are growing and demographic changes ahead, the societal demand for care of elderly persons and persons with disabilities will increase over the coming years. There is now a general trend in Europe to move away from institutionalised care of elderly persons and instead support living at home. This trend is based on the preferences of many elderly persons and the fact that support for living at home is less expensive for society than institutional living. The MonAMI project will thoroughly examine the economic viability and long term sustainability of the services in order to facilitate real mainstream implementation.

Technologies

To facilitate use and user interaction, MonAMI will develop an innovative interface, involving an embodied conversational agent. All services and applications will be selected and developed together with potential users with a “Design for All” approach within the areas:

- health.
- safety and security.
- communication and information.
- activity planning.
- comfort applications.

The selected services will first be tested in six Feasibility and Usability centres with user tests in lab-like conditions and when found feasible, usable and appropriate to user needs, large-scale validation will be carried out in Validation centres. Hundreds of users will try out the services in their homes and the impact and consequences will be analysed.

Expected results

The MonAMI project will demonstrate that accessible, useful services for elderly persons and persons with disabilities living at home can be delivered in mainstream systems and platforms such as digital television, third-generation mobile telephones and broadband Internet.

MonAMI will strengthen social cohesion by providing efficient systems for inclusion, allowing elderly persons and persons with disabilities to play a full role

in society. It will enable sustainable growth and competitiveness for European businesses by facilitating access to a new large market, elderly and disabled persons in Europe.

Useful data

Project name	Mainstreaming on Ambient Intelligence
Acronym	MonAMI
Funded by	European Commission (VI FP)
Contract	IST-035147
Type of project	Integrated Project
Budget	Total cost: 13,7 Million euros / Funding: 8,7 Million euros
Contacts	Coordinator: Gunnar Fagerberg (gunnar.fagerberg@hi.se) Dissemination: Maria Suarez (Maria.suarez@hi.se) Scientific: Antonio Kung (antonio.kung@trialog.com)
Projects websites	www.monami.info
Duration	September, 2006 - August, 2010
Partners	Swedish Handicap Institute (Sweden), OpenHub (United Kingdom), University of Zaragoza (Spain), France Telecom (France), Electricité de France (France), The Royal Institute of Technology (Sweden), London School of Economics (United Kingdom), HMC International (Belgium), Siemens Business Services (Germany), Telefónica I+D (Spain), Trialog (France), Technical University of Kosice (Slovakia), University of Passau (Germany), Europ Assistance France (France).

Project ONE

Speaker: Mihaela Ion, CREATE-NET.

Summary

In order to be competitive in Digital Ecosystems, Small and Medium Enterprises (SMEs) will need to develop alliances and collaborate with each other to provide joint service offerings and also address large tenders. It is for this reason that the ONE project has been created. The main objective of the ONE project is to enrich Digital Business Ecosystems with an open, decentralised negotiation environment. The project's features will allow organisations to create contract agreements for supplying complex, integrated services as a virtual organisation/-coalition. The project is especially geared towards SMEs and it provides them with a trusted and secure technological environment that is free of charge. The project creates tactical and strategic alliances to pursue business opportunities and growth.

Current negotiation platforms, such as Business-to-Business electronic marketplaces and Internet trading systems are centrally managed, and not fully trusted by SMEs and/or too expensive and hence not widely used by European SMEs today. Without the support of proper tools, SMEs cannot easily find trustworthy partners to provide services or be found themselves. Also, access to information about SME reputation is not readily available and negotiations are time consuming.

To solve these problems, ONE project will provide a negotiation environment that is affordable, open sourced and not centrally controlled; the environment will support the sharing of knowledge via exible security and trust policies; and it will be able to learn and adapt to real user negotiation strategies and to changing market conditions.

Key features

- Provide tools allowing users to create negotiation protocols and negotiation strategies, and runtime mechanisms for executing negotiations using different negotiation protocols,
- Enable users to dynamically modify the negotiation during the negotiation process,
- Develop decision support tools helping the users to execute a negotiation taking advantage of the learning technologies and improvements proposed by recommender and optimising their negotiation strategies,
- Create trust mechanisms to enable the sharing of trustworthy knowledge between partners.

Technologies

The main technologies adopted in the project are:

- Factory Environment: Model Editor (Meta Object Facility, Graphical Modelling Framework, Eclipse Modeling Framework/ECORE and Graphical Eclipse Framework), UML based models (the Negotiation meta model), XMI standard format.
- Negotiation Portal and Web-based Application: Asynchronous Javascript And XML (Ajax).
- Negotiation Engine: Negotiation Console, Negotiation Behaviour State Machine (extending Jbpm), Transformation Module.
- Distributed Knowledge Base: Application Server/Container, Content Repository (JCR API).
- Recommendation and Learning: Negotiation Support Systems, Recommender Systems, Learning System.
- Identity and Reputation: Single Sign-On, SAML, X.509, Secure Profiling, Distributed Knowledge-based Reputation, Identity Management, Certification Authorities, Core Security Primitives as platform run-time discovery services.

Expected results

ONE's strategic objective is twofold.

On one hand, it wants to create a flexible negotiation environment and mechanisms that would decrease (hopefully eliminate) the several barriers hindering businesses to come to an agreement via an assisted negotiation process.

On the other, it wants to provide a technological medium, a negotiation platform, based on the open source paradigm and the "evolutionary" software concept that would reassure users of their technological choices.

The ONE main objectives may be summarised by the following:

1. To enable the European service market and especially SMEs to be competitive in the global service production market;
2. To provide an open, decentralised environment able to self-adapt to the needs and culture of local business ecosystem enabling trust and evolution in B2B negotiations;
3. To provide a system that could enable the above-mentioned actors to access new markets and partners through reduction of entry cost barriers while increasing collaboration.

Useful data

Project name	Open Negotiation Environment
Acronym	ONE
Funded by	European Commission (VI FP)
Contract	FP6-034744
Type of project	Specific Targeted Research or Innovation Project (STREP)
Budget	Total Cost: 2,87 million euros / Funding: 2,03 million euros
Contacts	Coordinator: L. Telesca (luigi.telesca@create-net.org) Dissemination: P. Avesani (avesani@itc.it) Scientific: P. Ferronato (pferronato@soluta.net)
Projects websites	http://one-project.eu http://sourceforge.net/projects/one-project
Duration	September, 2006 - February, 2009
Partners	CREATE-NET (Italy), Soluta.Net East Europe (Romania), Fondazione Bruno Kessler (Italy), Waterford Institute of Technology - TSSG (Ireland), University of St. Gallen - MCM Institute (Switzerland), University of Girona (Spain), COOPSERVICE S.COOP. P.A. (Italy), Service Management International Ltd (UK)

Project RE-Trust

Speaker: Alessandro Zorat, University of Trento.

Summary

Industrial concern with software integrity is mostly focused on the protection of static software modules (e.g., by verifying the signature of their originator). However, many applications would require that the software is authenticated dynamically and continuously, in real time. Dynamic software authentication in real-time. This stronger kind of protection is a known problem, to which at present there is no satisfactory solution. Specifically, an open research challenge is that of ensuring that the original, trusted code base (i.e., the software as specified and implemented) is running on an untrusted host at all times and that the original code functionality has not been modified prior to or during execution.

This project investigates novel methodologies, either solely based on software or with hardware assistance, to solve the problem mentioned above. Central to this approach is the presence of a network that links the trusted and untrusted hosts. By combining the execution of software modules on both hosts and by exchanging (encrypted) information between them, the trusted host can obtain an assurance that the software running on the untrusted host is original, has not been manipulated and provides precisely the functionality it is designed for. For example, an attempt by the untrusted host to modify the policy of a network transport protocol to achieve faster service at the expenses of the other users would be detected so that punitive actions can be taken. Another example could be that of a film that has been downloaded with a license to be viewed only once should not be playable on a modified movie player that makes an (illegal) copy of the file without the trusted host being able to detect such breach of the license.

The discussion about the background and the challenging problems of the RE-TRUST project showed how the project “breaks with convention” by introducing the novel paradigm of continuous remote entrusting during run-time. The project is indeed challenging and has the potential to facilitate the emergence of an improved converged computing and networking environment with higher level of trust and integrity.

Leadership in technology is usually achieved by the introduction of new paradigms that break with existing conventions. Obviously, breaking with convention has high risks of two types:

1. Technological risks - in attempting to realize new technology there is always the risk of encountering either unsolvable problems, or more often, ineffective (i.e., too complicated) solutions.
2. Compatibility risks - even if there are effective solutions, they may diverge too much from the existing paradigms. In the environment of computing and networking the need for maintaining what is known as “backward compatibility” has relatively high risk.

Nevertheless, overcoming such risks typically lead to high rewards both scientifically and commercially. The RE-TRUST project, while being exposed to the risks above, is paving the way toward the high rewards deriving from the numerous applications that require or benefit from remote entrusting.

The RE-TRUST project uses tamper-resistant code to contrast tampering with the protocol/application for a well-defined time interval by periodically replacing selected parts of the code running on an untrusted host with newly downloaded tamper-resistant code. The tamper-resistant code uses techniques such as obfuscation, white-box cryptography, smart card, etc. that aim to ensure that automatic reverse engineering is infeasible within the available time frame before the next code replacement.

Technologies

The RE-TRUST project calls for the use of several technologies, among which the following are the most representative:

- SW engineering (Defenses against reverse engineering, Periodically replacing parts of the code running on an untrusted host, Code slicing).
- Cryptography (Code obfuscation, White-box cryptography).
- Secure operating systems and secure network protocols (Self-checking code (monitors) and monitor replacement).
- Tamper resistance hardware (Smart card, Secure token, Trusted processing module (TPM)).

Expected results

The main results for this project will be the ensuring that a remote host can continuously entrust a software components that is executed on another (HW/SW) environment; an environment that could possibly be untrusted. In particular, the project intends to provide workable solutions to:

- Protecting network resources and servers from users employing untrusted/unauthorized software and protocols - specifically in critical applications, such as e-commerce, e-government, e-voting, etc.
- Ensuring data privacy and compliance with the expected behavior in grid computing.
- Ensuring adherence to digital right management (DRM) by assuring proper processing of untrusted (possibly misbehaving) hosts that receive private data and copyright protected content.

Useful data

Project name	Remote EnTrusting by RUN-time Software auThentication
Acronym	RE-Trust
Funded by	European Commission
Contract	FP6-021186
Type of project	Specific Targeted Research or Innovation Project (STREP)
Budget	Total Cost: 2,27 million euros / Funding: 1,55 million euros
Contacts	Coordinator: Yoram Ofek (ofek@dit.unitn.it) Dissemination: Alessandro Zorat (zorat@unitn.it) Scientific: Yoram Ofek (ofek@dit.unitn.it)
Projects websites	www.re-trust.org
Duration	September, 2006 - August, 2009
Partners	University of Trento (Italy), Politecnico di Torino (Italy), Gemalto (France), Katholieke Universiteit Leuven (Belgium), St. Petersburg Institute for Informatics and Automation, Russian Academy of Sciences (Russia).

Project SENSE

Speaker: Professor Demos T. Tsahalis, Laboratory of Fluid Mechanics & Energy University of Patras.

Summary

SENSE project will develop methods, tools and a test platform for the design, implementation and operation of smart adaptive wireless networks of embedded sensing components.

The network is an ambient intelligent system which adapts to its environment, creates ad-hoc networks of heterogeneous components, delivers reliable information to its component sensors and the user.

The sensors cooperate to build and maintain a coherent global view from local information. Newly added nodes automatically calibrate themselves to the environment, and share knowledge with neighbors.

The network is scalable due to local information processing and sharing, and self-organizes based on the physical placement of nodes.

A test platform for a civil security monitoring system will be developed as a test application, composed of video cameras and microphones.

The test platform will be installed in an airport (Krakow-Balice), to yield real data and performance goals from a realistic test environment.

Each sensor is a stand-alone system consisting of multiple embedded components:

- video system,
- audio system,
- central processor,
- Power source
- wireless networking.

The security application will implement object/scenario recognition (e.g. baggage left unattended, people “lurking” in an area). Nodes will recognize local objects, using a combination of video and audio information.

Neighboring nodes will exchange information about objects in a self-organizing network.

The result is a global overview of current objects and events observed by the network.

SENSE will address the following scientific and technological objectives:

- To understand how to build networked systems of embedded components that can dynamically and automatically re-configure themselves
- To understand how to convert low-level local information to semantic knowledge
- To understand how to use semantic-level knowledge for network-centric computation

- To understand how perception and information processing can be combined using low-level and high-level feature fusion
- To understand how to facilitate networks of heterogeneous devices using a high-level semantic layer

Technologies

The main technologies involved in the SENSE project approach are:

- object recognition from video input
- sound pattern recognition from audio input
- correlation in semantic level of the objects and patterns recognised from the video and audio
- wireless sensor communication

Expected results

The expected results of SENSE are to combine the aspects of:

- embedded intelligent middleware in smart devices
- adaptive configuration,
- flexible cooperation (among devices),
- high-level perception and adaptation and
- dynamic networking
- Common framework of semantic knowledge discovery and sharing.

The SENSE system will encompass aspects including:

- construction of a modality-neutral embedded test platform;
- raw sensory processing;
- transformation of sensory data into semantic knowledge;
- communication between nodes to produce a consistent world view;
- sharing of knowledge between intelligent nodes;
- automatic recognition of unusual and alarm situations;
- communication between the intelligent network and an operator; and
- automatic discovery and configuration of new intelligent nodes.

Useful data

Project name	Smart Embedded Network of Sensing Entities
Acronym	SENSE
Funded by	European Commission
Contract	IST-033279
Type of project	Specific Targeted Research or Innovation Project (STREP)
Budget	Total cost: 2,323,478.00 Euros / Funding: 1,698,059.00
Contacts	Coordinator: Dr. Wolfgang Herzner (Wolfgang.Herzner@arcs.ac.at) Dissemination: Professor Demos Tsahalis (tsahalis@lfme.chemeng.upatras.gr) Scientific: : Dr. Dietmar Bruckner (bruckner@ict.tuwien.ac.at)
Projects websites	www.sense-ist.org
Duration	September, 2006 - August, 2009
Partners	Austrian Research Centers - ARC (Austria), Universidad Politecnica de Valencia (Spain) PARAGON Ltd. (Greece), University "Dunarea de Jos" of Galati (Romania), University of Patras (Greece), Vienna University of Technology, Institute of Computer Technology (Austria), ZDANiA Sp. z o.o. (Poland), AGH - University of Science and Technology Krakow (Poland), Miedzynarodowy Port Lotniczy im. Jana Pawla II Krakow - Balice Sp. z o.o. (Poland)

Project SENSORIA

Speaker: Fabio Martinelli, University of Roma.

Summary

The core aim of SENSORIA is the production of new knowledge for more systematic and scientifically well-founded methods of service-oriented software development. SENSORIA is developing a service-based suite of tools for implementing the new service-oriented language primitives, the analysis techniques and the support for service development and deployment. The tool suite will give continuous feedback on the usefulness and applicability of the research results. It will also be the starting point for the design of new industrial support tools for service-oriented development. The software development techniques of SENSORIA range from requirements to deployment including reengineering of legacy systems and rely on mathematical theories and methods that, ensuring the correctness of each step, allow a semi-automatic design process. Realistic case studies for different important application areas including telecommunications, automotive, e-learning, and e-business are defined by the industrial partners to provide continuous practical challenges for the new techniques of services engineering and for demonstrating the research results.

Technologies

The main technologies involved in this approach are the following:

- declarative and operational modelling of services.
- semantic based composition of services.
- formal techniques for qualitative and quantitative analysis of service-oriented systems.
- model-driven development and deployment of services.
- re-engineering of legacy systems into service-oriented systems.
- tool support for engineering service-oriented architectures.

Expected results

Engineering methods and techniques and tools for the development of service-oriented systems, which comprise

- Definition of adequate linguistic primitives for modelling and programming global service-oriented systems, including: a UML extension for services systems, a formal Reference Modelling Language SRML inspired by the service component architecture, a Phoenix family of process calculi for services as a formal basis for programming and modelling and analysing dynamic aspects of service-oriented systems.

- Development of qualitative and quantitative analysis methods for global services, including: trust management and static analysis techniques for crypto-protocols, secure service composition, techniques for ensuring constraints on interfaces between, services, and quantitative analysis of performance requirements of service-oriented systems.
- Sound engineering techniques for development over model-based transformation and for deployment and re-engineering techniques for service-oriented systems.
- Case tool support,
- The validity of the SENSORIA approach is demonstrated by case studies of the automotive, finance, telecommunications and e-learning domains.

Useful data

Project name	Software Engineering for Service-Oriented Overlay Computers
Acronym	SENSORIA
Funded by	European Commission (VI FP)
Contract	IST-016004
Type of project	Integrated Project
Budget	Total cost: 10,0 Million Euros / Funding: 8,15 Million Euros
Contacts	Coordinator: Martin Wirsing (martin.wirsing@lmu.de) Dissemination: Nora Koch (koch@fast.de)
Projects websites	www.sensoria-ist.eu
Duration	September, 2005 - August, 2008
Partners	Ludwig-Maximilians-Universität München (Germany), Università di Trento (Italy), University of Leicester (United Kingdom), Warsaw University (Poland), Technical University of Denmark at Lyngby (Denmark), Università di Pisa (Italy), Università di Firenze (Italy), Università di Bologna (Italy), Istituto di Scienza e Tecnologie della Informazione "A. Faedo" (Italy), University of Lisbon (Portugal), University of Edinburgh (United Kingdom), ATX Software SA (Portugal), Telecom Italia S.p.A (Italy), Imperial College London and University College London (United Kingdom), FAST GmbH (Germany), Budapest University of Technology and Economics (Hungary), S&N AG (Germany), Politecnico di Milano (Italy), ATX Technologies SA (Portugal)

Project UBISEC&SENS

Speaker: Dirk Westhoff, Nec Europe.

Summary

Wireless Sensor Networks (WSNs) are an exciting development with very large potential to have a significant beneficial impact on every aspect of our lives while generating huge opportunities for European industry. What is needed to kick off the development and exploitation of WSNs is an architecture for medium and large scale wireless sensor networks integrating comprehensive security capabilities right from the concept stage. This would support the rapid development of sensor networks and would open up the application domain for commercial activities. UbiSec&Sens intends to solve this by providing a comprehensive architecture for medium and large scale wireless sensor networks with the full level of security that will make them trusted and secure for all applications. In addition UbiSec&Sens will provide a complete tool box of security aware components which, together with the UbiSec&Sens radically new design cycle for secure sensor networks, will enable the rapid development of trusted sensor network applications.

The UbiSec&Sens approach is to use three representative WSN scenarios to iteratively determine solutions for the key WSN issues of scalability, security, reliability, self-healing and robustness. This will also give a clearer understanding of the real-world WSN requirements and limitations as well as identifying how to achieve a successful rollout of WSNs. UbiSec&Sens will provide a comprehensive architecture for medium and large scale wireless sensor networks with the full level of security that will make them trusted and secure for all applications. The overall project goals are to:

- Focus the work on the intersection of security, routing and in-network processing to design and develop efficient and effective security solutions and to offer effective means for persistent and encrypted data storage for distributed (and tiny) data base approaches
- Provide a complete toolbox of security aware components for sensor network application development. We aim at extremely energy-efficient and condensed data transmission as well as highly robust and reliable solutions for concrete WSNs that, at the same time, still provide an appropriate level of security.
- Prototype and validate the UbiSec&Sens solutions in the representative wireless sensor application scenarios of agriculture, road services and homeland security.

Technologies

The main technologies involved in the UbiSec&Sens are the followings:

- Flexible routing and in-network processing.

- Concealed data aggregation.
- Basic security components.
- Secure distributed data storage.
- Enhanced key pre-distribution.
- Data plausibility.
- Provably secure routing.
- Resilient data aggregation.
- Pairwise/groupwise authentication or re-recognition.
- Energy-efficient components.

Expected results

The results of UbiSec&Sens are a necessary step to progress the field of security and communication research in Europe and, as well as advancing the competitiveness of the European industry, they assist the European Commission to develop more comprehensive programs for innovative socially and economically beneficial sens.

Useful data

Project name	Ubiquitous Sensing and Security in the European Homeland
Acronym	UBISEC&SENS
Funded by	European Commission (VI FP)
Contract	026820
Type of project	STReP (Specific Targeted Research Project)
Budget	Total cost: 2,9 Million Euros / Funding: 1,9 Million Euros
Contacts	Coordinator: Uwe Herzog (herzog@eurescom.de) Dissemination: Dirk Westhoff (dirk.westhoff@nw.neclab.eu)
Projects websites	www.ist-ubisecsens.org
Duration	January, 2006 - December, 2008
Partners	Eurescom - European Institute For Research And Strategic Studies In Telecommunications GmbH (Ger.), RWTH - Rheinisch-Westfälische Technische Hochschule Aachen (Ger.), INRIA - Institut National De Recherche En Informatique Et En Automatique (Fra.), IHP - Innovations For High Performance Microelectronics (Ger.), INOV - INESC Inovacao - Instituto De Novas Tecnologias (Por.), BUTE - Budapest University of Technology and Economics (Hun.), RUB - Ruhr University Bochum (Ger.), NEC Laboratories Europe (U.K.)

Project WASP

Speaker: Laurent Gomez, SAP Research.

Summary

An important class of collaborating objects is represented by the myriad of wireless sensors, which will constitute the infrastructure for the ambient intelligence vision. The academic world actively investigates the technology for Wireless Sensor Networks (WSN). Industry is reluctant to use these results coming from academic research. A major cause is the magnitude of the mismatch between research at the application level and the node and network level. The WASP project aims at narrowing this mismatch by covering the whole range from basic hardware, sensors, processor, communication, over the packaging of the nodes, the organisation of the nodes, towards the information distribution and a selection of applications. The emphasis in the project lays in the self-organisation and the services, which link the application to the sensor network. Research into the nodes themselves is needed because a strong link lies between the required exibility and the hardware design. Re-search into the applications is necessary because the properties of the required services will in uence the configuration of both sensor network and application for optimum efficiency and functionality. All inherent design decisions cannot be handled in isolation as they depend on the hardware costs involved in making a sensor and the market size for sensors of a given type. Three business areas, road transport, elderly care, and herd control, are selected for their societal significance and large range of requirements, to validate the WASP results. The general goal of the project is the provision of a complete system view for building large populations of collaborating objects. The system incorporates networking protocols for wireless sensor nodes to hide the individual nodes from the application. The impact on European industry and research comes from the provision of an European alternative to the wireless sensor nodes originating in the US. The WASP results will be well suited for adoption by SMEs. The consortium de

nes an active programme to approach the appropriate SMEs and to familiarise them with the WASP results.

Technologies

The main technologies involved in this approach are the following:

- The development of an autonomous and intelligent infrastructure, which incorporates a wireless sensor network.
- The development of a cost-efficient infrastructure that encourages application driven optimisation of the network composed of generic nodes.
- The deployment of the developed infrastructure within a prototype, based on selected applications, to validate both the sensor network design and the genericity of the offered design.

Expected results

The project aims at providing:

- A consistent chain of software components to support (dynamic) energy-optimisation, security, QoS guarantees, and the specification of trade-off preferences by the application.
- Sets of cross-optimised software stacks with each set optimised for a given set of application characteristics.
- Set of benchmarks and measurements to compare energy efficiency and code efficiency between existing and new alternatives.
- Design-rules for the configurable sensor nodes, and their applications and optimisation strategies.
- A prototype implementation in two of the three chosen business areas

Useful data

Project name	Wirelessly Accessible Sensor Populations
Acronym	WASP
Funded by	European Commission (VI FP)
Contract	IST-034963
Budget	Total Cost: 16.3 Million euros / Funding: 10.1 Million euros
Contacts	peter.van.der.stok@philips.com
Projects websites	www.wasp-project.org
Duration	September, 2006 - February, 2010
Partners	Philips Research Eindhoven (the Netherlands), CEFRIEL (Italy), IMEC-NL (the Netherlands), CSEM (Switzerland), TU Eindhoven (the Netherlands), European Microsoft Innovation Center (Germany), Health Telematic Network (Italy), Fraunhofer-Gesellschaft (Germany), ASG veehouderij (the Netherlands), Imperial College (United Kingdom), ST microelectronics (Italy), INRIA (France), EPFL (Switzerland), Philips Research Aachen (Germany), Centro Ricerche Fiat (Italy), TU Kaiserslautern (Germany), RWTH Aachen (Germany), SAP (France), University of Paderborn (Germany)

Project ESFORS

Speaker: Pedro Soria-Rodriguez, Atos Research & Innovation.

Summary

ESFORS is a Coordination Action that aims at bringing together the European stakeholders for security and dependability Information and Communication Technologies (ICTs) to address the security and dependability requirements of emerging software service platforms. This emergence of open service platforms such as web services provides major opportunities to position the European software industry at the heart of the emerging information society. However, the uptake of solutions based on software by industry is dependent on industry confidence in their security and dependability.

The project is positioned to support the emergence of a software and services platform architecture ensuring the incorporation of security and dependability best practice. The project will complement already existing coordination actions, e.g. SecurIST, to help shape the Security and dependability content within the European Strategic Research Agenda. It will co-operate with SecurIST to ensure that open service requirements are incorporated into the SecurIST security and dependability technology roadmap and that the roadmap is incorporated into the research agenda of the software and service research community. ESFORS will act as a bridge between these two communities: the software and services application community and the security and dependability community.

Technologies

The studies conducted in ESFORS are concerned with Service Oriented Architectures, and other related technology challenges. The project itself does not design or develop any technologies, but concentrates only on studies.

Expected results

ESFORS will act as a bridge between these two communities: the software and services application community and the security and dependability community.

The project will support the development of a secure web services framework for communications networks and information infrastructures in Europe by bringing together the key players from the web service and software and security and dependability communities.

The project is focused on coordinating the European activities to enable secure ICT services. The concept of Services represents a significant change in the way ICT will be delivered. An example of this is “web services”, which present a significant embodiment of the likely change.

By establishing links between projects in the services and security domains, ESFORS will articulate the security and dependability framework for the emerging industrial initiative on web services, software development and information infrastructure. This will include the FP7 technology platform instrument.

In particular, ESFORS will bring together all of the players that will contribute to a security and dependability framework required to support the establishment of a European Software and Services Technology Platform (see NESSI).

Finally, the project will produce a set of recommendation for future research objectives within E.C. framework programmes, and within the NESSI Strategic Research Agenda.

Useful data

Project name	European Security Forum for Web Services, Software and Systems
Acronym	ESFORS
Funded by	European Commission
Contract	FP6-027599
Type of project	Coordination Action
Budget	900,000 euros
Contacts	Pedro Soria-Rodriguez pedro.soria@atosorigin.com
Projects websites	www.esfors.org
Duration	November, 2005 - October, 2007
Partners	Leader: Atos Origin Partners: HP, SAP, Engineering, Waterford Institute of Technology, University of Lisboa.

Project PalCom

Speaker: Erik Gronvall, University of Siena.

Summary

The PalCom project aims to research and develop a new perspective on ambient computing named palpable computing. Palpable denotes that systems are capable of being noticed and mentally apprehended. Palpable systems support people in understanding what is going on at the level they choose. Palpable systems support control and choice by people. Often the default mode for a palpable application is to suggest courses of action rather than acting automatically. Thus palpable computing complements the effectiveness of ambient computing with a focus on making the means of empowering people intelligible.

The project applies a participatory design process, where technical possibilities and scientific analysis are balanced with usefulness and the development is given direction through user needs. Through this work the project contributes to the innovation of tools and techniques for user centred, participatory design of palpable applications.

As an important element in this process the project entails continuous involvement of a number of user sites.

Technologies

The various development processes in the PalCom project entail a large amount of different ambient computing technologies, both in terms of hardware and software. Some of the key themes for the common software architecture are:

- Service orientated architectures.
- Assemblies of services (Service composition).
- Generic runtime inspection mechanisms.
- Resource aware architectures.

Expected results

The two main objectives are to design:

- An open architecture for palpable computing.
- A conceptual framework to understand the particulars of palpable technologies and their use.

Secondary objectives include:

- Design and implementation of a (open source) toolbox for the construction of palpable applications.
- Development of a range prototypes of palpable applications
- Gaining a firm understanding of a range of practices into which palpable technologies may be introduced

Useful data

Project name	Palpable Computing: A new perspective on Ambient Computing
Acronym	PalCom
Funded by	European Commission, Swiss Government and partners
Contract	IST-002057
Type of project	Integrated Project
Budget	EU Funding: 7.004.000 euros Swiss funding: 1.400.000 euros Commercial partner funding: 1.600.000 euros University funding: 300 person months
Contacts	Coordinator: Morten Kyng (mkyng@daimi.au.dk) Dissemination: Gunnar Kramp (gkramp@daimi.au.dk) Scientific: Morten Kyng (mkyng@daimi.au.dk)
Projects websites	www.ist-palcom.org
Duration	January, 2004 - December, 2007
Partners	University of Aarhus, Denmark; University of Siena, Italy; Lund University, Sweden; Malmö University, Sweden; Lancaster University, UK; Aarhus School of Architecture, Denmark; Kings College, London University, UK; L'ecole Polytechnique Federale de Lausanne, Switzerland; 43D APS, Denmark; Siemens Aktiengesellschaft, Germany; Whitestein Technologies AG, Switzerland; Alexandra Instituttet A/S, Denmark

Project R4eGov

Speaker: Michel Frenkiel.

Summary

Putting eGovernment in place has become a priority throughout Europe over the past ten years. This is mostly thanks to people like André Santini, one of the first eGovernment pioneers.

eGovernment offers many advantages: it makes citizens' lives easier, it's a more cost-effective way to use taxpayers money, it encourages research, and it helps develop local economies.

eGovernment has become a reality for most of today's public administrations; and many different applications exist. Most of the applications were created as stand-alone applications. We now face a situation where these stand-alone applications need to communicate with each other. This brings a threefold challenge. First we need to make sure that communication is achieved without compromising the citizen's privacy. Then, that it does not break any of the rules implemented in the Member States. Finally, that it does not replace any of the systems already in place.

This is the challenge the R4eGov team faces.

Public administrations all across the EU have explained to us the specific problems they have. We decided to focus on a few selected cases. These involve prestigious administrations such as Eurojust, Europol, the Austrian Chancellery, the German Federal Court of Justice, the Paris Business Court, the ERASMUS programme, and consulates. In total, 20 of the best representatives from the research field and from the private sector work on the R4eGov project. Their collaboration in the areas of process control and security will generate the required new methodology and toolsets.

After one year of activity, we selected among these case studies two particularly well adapted problems to demonstrate the technology developed in the project. These two case studies will be further developed into full blown demonstrators. They are:

- BKA's Pilot of IOP gateway: information handling in a Legal Information System.
- Eurojust/Europol: Judicial and Law enforcement cooperation between EU Member States and EU agencies.

Technologies

- Workflows.
- IT security.

Expected results

- A model and associated IT tools to enable and control interoperability between European public administrations IT systems
- Two demonstrations running in large, demanding public administrations:
 1. linking Eurojust and Europol systems.
 2. linking several Austrian federal administrations.

Useful data

Project name	Towards e-Administration in the large
Acronym	R4eGov
Funded by	European Commission (VI FP)
Contract	IST-2004-026650
Type of project	Integrated Project
Budget	Total cost: 11,2 Million euros / Funding: 7,4Million euros
Contacts	Coordinator: Michel Frenkiel (michel.frenkiel@r4egov.info) Dissemination: Emmanuelle Martinot (Emmanuelle.Martinot@onenortheast.co.uk) Scientific: Adreas Schaad (andreas.schaad@sap.com)
Projects websites	www.r4egov.info
Duration	March, 2006 - February, 2009
Partners	Bundesgerichtshof (Germany); Bundeskanzleramt der Republik Oesterreich (Austria); Deutsches Forschungszentrum für künstliche Intelligenz GmbH (Germany); Eurojust (EU); Europol (EU); Greffe du tribunal de commerce de Paris (France); Hamburger Informatik Technologie Center E.V. (Germany); INFOCERT (Italy); Institut Eurecom (France); Karobas (France); Max-Planck-Gesellschaft z.f.d.w. represented by the MPI fuer Informatik (Germany); Metadat IT-Beratungs und Entwicklungs GmbH (Austria); North East Development Agency (UK); SAP (Germany); Service Public Fédéral Technologie de l'information et de la communication (Belgium); Thales Security Systems (France); UNISYS (Belgium); Universität Koblenz (Germany); University of Leeds (UK); Web Force (France)

EPoSS

Speaker: Sebastian Lange, VDI/VDE Innovation + Technik GmbH.

Summary

EPoSS, the European Technology Platform on Smart Systems Integration, is an industry driven policy initiative defining R&D and innovation needs and policy requirements related to Smart Systems Integration and integrated Micro and Nanosystems. EPoSS is contributing to the Lisbon Strategy aiming at boosting economic growth, creating more and better jobs and ensuring sustainable prosperity in Europe.

A group of major industrial companies based in different European Member States intends to co-ordinate their activities and to develop a vision for and to set-up a research agenda on innovative Smart Systems Integration. EPoSS brings together European private and public stakeholders in order to create an enduring basis for structuring initiatives, for co-ordinating and bundling efforts, for setting-up sustainable structures of a European Research Area on Smart Systems Integration. EPoSS embraces all key players, public and private, in the value chain so as to

- provide a common European approach on Innovative Smart Systems Integration from research to production outlining the key issues for a strategic European innovation process.
- formulate a commonly agreed roadmap for action (updating, assembling and completing existing material and approaches) and provide a strategic R&D agenda.
- mobilise public and private human, infrastructural and financial resources, and.
- define priorities for common research and innovation in the future.

The initiative is of immediate importance in view of defining research and technology priorities for the EU's VIIth Framework Programme, for raising more critical mass and resources and for coordinating between different initiatives (national, regional, EUREKA, European public funding and industry).

Technologies

- Smart Systems.
- Aeronautics.
- Automotive.
- Medical Technologies.
- RFID.
- Security.
- Information & Communication.

Expected results

Strengthen European competitiveness, increase the success of the partners in participating in the Framework Programme, Define Roadmaps and Strategies in the field of Smart Systems Integration. Facilitate Networking, etc...

Useful data

Project name	European Technology Platform on Smart Systems Integration
Acronym	EPoSS
Funded by	Members
Type of project	European Technology Platform
Contacts	Chairman: Klaus Schymanietz Office: Sebastian Lange (slange@vdivde-it.de)
Projects websites	www.smart-systems-integration.org
Duration	Open
Partners	EADS, Thales, Siemens, Bosch, Continental, Gemalto, NXP, Philips, EPCOS, etc ...

Project Hydra

Speaker: Atta Badii, University of Reading.

Summary

The first objective of the Hydra project is to develop middleware based on a Service-oriented Architecture, to which the underlying communication layer is transparent. The middleware will include support for distributed as well as centralised architectures, security and trust, reflective properties and model-driven development of applications.

The HYDRA middleware will be deployable on both new and existing networks of distributed wireless and wired devices, which operate with limited resources in terms of computing power, energy and memory usage. It will allow for secure, trustworthy, and fault tolerant applications through the use of novel distributed security and social trust components and advanced Grid technologies.

The embedded and mobile Service-oriented Architecture will provide interoperable access to data, information and knowledge across heterogeneous platforms, including web services, and support true ambient intelligence for ubiquitous networked devices.

The second objective of the HYDRA project is thus to develop a Software Development Kit (SDK). The SDK will be used by developers to develop innovative Model-Driven applications.

Technologies

- Embedded and mobile SoA.
- Semantic MDA for AmI.
- Ambient Intelligence support.
- Hybrid architectures.
- Wireless devices & networks.
- Trust and security.

Expected results

The project results consist of the following end products:

- HYDRA middleware for networked embedded systems - Adds AmI applications to new and existing embedded systems and components.
- HYDRA Software Development Kit (SDK) for middleware - Allows developers to rapidly create new networked embedded AmI applications.

Useful data

Project name	Networked Embedded System middleware for Heterogeneous physical devices in a distributed architecture
Acronym	Hydra
Funded by	European Commission (VI FP)
Contract	IST 2005-034891
Type of project	Integrated Project
Budget	12,8 Mill euros
Contacts	Coordinator: Dick Powell (dpowell@cinternational.co.uk) Dissemination: Heiz-Josef Eikerling (Heinz-Josef.Eikerling@c-lab.de) Scientific: Peter Rosengren (peter.rosengren@cnet.se)
Projects websites	http://www.hydra.eu.com
Duration	July, 2006 - June, 2010
Partners	C International, Ltd. (UK), CNet Svenska AB (Sweden), The Fraunhofer Institute for Applied Information Technology (Germany), The Fraunhofer Institute for Secure Information Technology (Germany), In-JeT ApS (Denmark), Priway (Denmark), T-Connect S.r.l. (Italy), Telefonica I+D SA (Spain), University of Aarhus (Denmark), Innova S.p.A. (Italy), University of Reading (UK), MESH-Technologies A/S (Denmark), Siemens Business Services (Germany), Technical University of Kosice (Faculty of Economics, Faculty of Electrical Engineering and Informatics) (Slovakia), University of Paderborn (Germany)

Project BioSecure

Speaker: Massimo Tistarelli, University of Sassari.

Summary

The main objectives of the BioSecure Network of Excellence are:

1. To strengthen and integrate multidisciplinary research effort in order to investigate biometrics-based identity authentication for the purpose of meeting the trust and security requirements in our progressing digital information society, through effective and dynamic technologies.
2. To disseminate and spread excellence using a number of dedicated tools that will strengthen the impact of scientific dissemination. Such tools include workshops, conferences, Residential workshops and similar events that are organised by the network. The international collaboration will also be enhanced by facilitating mobility across Europe through visiting researcher, Post-Doc.

The Network is composed of most of the excellent European institutes which have a great experience in the biometric field and are willing to work together in order to produce more effective and visible results. Two well known american institutes are also full partners of the network. The network has also some links with CASIA (China) which is in the process of becomming associate partner.

The network will thus become a durable and lasting virtual laboratory, with high visibility and interactions. It acts as a kernel of institutes aiming at widely disseminating information, results, data, and norms all through Europe, at creating excellence through training of researchers and doctoral students, which will enable the sustainability of Europe's excellence in this Biometrics field.

In operational terms, the envisaged objectives include the following ones:

1. Building of a common research infrastructure to avoid unnecessary duplication and splitting of resources. The classical investigation of monomodal biometric methods are pursued, with a special attention to emerging ones. An important stress will also be given to the combination of modalities.
2. Building of a common evaluation framework (that would include common database and protocols for technology evaluation). A particular focus will be on the integration of the existing material (databases and softwares) previously developed in different laboratories or in previous national or EC projects.
3. Organizing International Competitions such as NIST (National Institute of Standards and Technology) speech and face evaluation campaigns or the FVC (Fingerprint Verification Competition), which already takes place in Europe.
4. Promoting new European standards and common means of evaluation. Indeed, standards in the Biometrics area are mainly driven by the American

organization ANSI and a few other interested groups. However, the international ISO and CEN European standards have recently launched specific working groups in the Biometry area, to which BioSecure contribution will be beneficial.

5. Facilitating the practical usage and employability of the technology by identifying and addressing the technical challenges linked to applications.
6. Increasing training and mobility which represent essential tools for integration. A number of important initiatives have been identified to promote research personnel mobility (short-term missions, working seminars, Joint PhD supervision ...) and students or young researchers mobility (Post Docs, Joint PhD...). It is also one of the major goals of BioSecure to promote international training and several means are envisaged such as Residential workshops, European Master Program (distributed e-learning ...).

BioSecure also devotes a huge effort both in terms of initiatives and financial contribution to dissemination and excellence spreading since it is an essential mean to bring together all researchers across the full NoE and beyond. These activities include:

- large scale events that will either bring together the community (Annual BioSecure symposium/workshop, Special sessions at leading international and European conferences).
- Promotion of BioSecure (external forums or exhibitions such as Biometrics 2006, in general Media for public awareness and improving the science attractiveness for young students of both genders.
- Specific training (such as regular 'web seminars' broadcast over internet to members, short courses for industry).

Expected results

Specification and design of facilities for multimodal biometric algorithms evaluation, namely, databases, reference systems and assessment protocols.

Useful data

Project name	Biometrics for Secure Authentication
Acronym	BioSecure
Funded by	European Commission (VI FP)
Contract	IST-2002-507634
Type of project	Network of Excellence
Budget	Total cost: Funding 3 Million euros
Contacts	Coordinator: Caisse des Depots et Consignations (CDC) Scientific: Groupe des Ecoles des Télécommunications (GET) (Bernadette.Dorizzi@int-edu.eu)
Projects websites	www.biosecure.info
Duration	June, 2004 - September, 2007
Partners	Caisse des Dpôts et Consignations (France); Groupe des Ecoles de Télécommunication (France); Eurecom (France); Thales Research & Technology France (France); Université d'Avignon et des Pays de Vaucluse (France); Thales Security System (France); University of Kent (UK); University of Surrey (UK); University of Wales Swansea (UK); University of Magdeburg (Germany); Universidad de Vigo (Spain); Universidad de Zaragoza (Spain); Universidad Politecnica de Madrid (Spain); Universitat Pompeu Fabra (Spain); Fondazione Ugo Bordoni (Italy); Università Degli Studi di Bologna (Italy); University of Sassari (Italy); Joanneum Research Graz (Austria); Aristotle University of Thessaloniki (Greece); Stichting Centrum voor Wiskunde en Informatica (Netherlands); University of Twente (Netherlands); Halmstad University (Sweden); University of Ljubljana (Slovenia); University of Fribourg (Switzerland); Swiss Federal Institute of Technology (Switzerland); Institute of Information Technologies (Bulgaria); University of Zagreb (Croatia); Bogazici University (Turkey); San José State University (USA); Michigan State University USA)

Project GREDIA

Speaker: Dimitrios Sotiriou, Athens Technology Center.

Summary

Grid technology has achieved significant advances in the past few years, thanks in part to a considerable number of prominent organisations that have contributed to Grid middleware. This has opened horizons for new exploitation opportunities; however, these opportunities have not yet fully materialised in terms of the emergence of new applications for industry. Use of Grid technology is still primarily confined to scientific applications, which have been developed by scientific organisations with the necessary expertise in Grid principles. Many organisations developing IT applications for industry have been reluctant to leverage Grid technologies and concepts, due to perceived complications in their use and deployment.

GREDIA addresses this problem with the delivery of a Grid application development platform, a tool which will provide high level support for the development of Grid business applications through a flexible graphical user interface. This platform will be generic in order to combine both existing and arising Grid middleware, and facilitate the provision of business services, which mainly demand access and sharing of large quantities of distributed annotated numerical and multimedia content.

Furthermore, GREDIA will facilitate for mobile devices to exploit Grid technologies in a seamless way by enabling mobile access to distributed annotated numerical and multimedia content. The potential effects of the platform will be validated through two pilot applications, servicing the vital sectors of media and banking.

The objectives of the GREDIA project can be summarised as follows:

- Develop a reliable Grid application development platform with high-level support for the design, implementation and operational deployment of secure Grid business applications.
- Enable the efficient data management of mobile services for business applications.
- Ensure the protection of data and transactions at all levels through a dedicated security framework.
- Validate the platform by producing two pilot Grid applications to address real life scenarios, servicing the domains of media and banking.

The effectiveness and the reliability of the GREDIA Grid application development platform will be validated through the deployment of pilot applications in two operational domains:

- A media and journalism application is intended to allow journalists and photographers to make their work available to a trusted network of peers at the moment when it is produced, either from desktops or mobile devices. This

pilot will bring together the market orientation and pervasiveness of mobile communication technology with the promise of a dynamically concerted use of resources and services provided through Grid infrastructures.

- A banking application will enable the exchange of complex information between the customers and their bank(s) in a Basel II related credit scoring scenario. This pilot will utilize the advances in web services and other middleware developed in GREDIA to demonstrate how Grids can be accessed by many partners regardless of location, ensuring that the data sharing is consistent with the principles of the financial sector.

Expected results

From a technical point of view, GREDIA will focus on:

- Developing and maintaining a novel generic Grid middleware required for servicing business applications accessing distributed annotated numerical and multimedia content.
- Extending the notion of Grid middleware to the management of mobile data, thus allowing mobile devices to participate in a data Grid as service providers, in a peer-to-peer manner.
- Defining and analysing the appropriate interfaces to support the protection of data and transactions among peer-to-peer Grid based applications at all levels through a dedicated security framework.

Through the development of the Grid application development platform, GREDIA will contribute to the state of the art in several important areas:

- Innovative search and retrieval mechanisms for fast access of annotated numerical and multimedia content distributed over the Grid, based on P2P overlay network technology.
- A new notation for Grid application developers, allowing for easy definition of Grid application's static and dynamic aspects, hiding the complexity of semantic service matchmaking.
- Ontological services supporting interoperability in and across Virtual Organisations, building a semantic abstraction layer over available resources in the Grid.
- Implementation of information services that rapidly catalogue content on mobile devices, and design of agents that seek data caching and replication services based on QoS criteria.
- Protection of data and transactions through a secure framework for authentication of entities, confidentiality and integrity to access from remote resources.

Expected results

GREDIA will produce a reliable platform with high-level support for the design, development and operational deployment of secure Grid business applications. Through the successful deployment of the platform, GREDIA will:

- Build business applications upon a novel Grid middleware, enabling the access to distributed annotated numerical and multimedia content in a secure way.
- Define and specify services that will allow mobile devices to participate in the Grid Virtual Organisation in a seamless way.
- Analyse a security framework that will protect data at all levels of the Grid Virtual Organisation.
- Evaluate the framework by producing two Grid pilot applications, addressing real life scenarios servicing the areas of media and banking.

Useful data

Project name	Grid enabled access to rich media content
Acronym	Gredia
Funded by	European Commission (VI FP)
Contract	FP6 - 034363
Type of project	Specific Targeted Research or Innovation Project (STREP)
Budget	Total cost: 3,3 Million euros / Funding: 2,4 Million euros
Contacts	Coordinator: Nikos Sarris (n.sarris@atc.gr) Dissemination: Wilfried Runde (wilfried.runde@dw-world.de) Scientific: Nektarios Koziris (nkoziris@cslab.ece.ntua.gr)
Projects websites	www.gredia.eu
Duration	October, 2006 - March, 2009
Partners	Athens Technology Center S.A., SYMBIAN Ltd., Deutsche Welle, The Academic Computing Centre CYFRONET AGH, Institute of Communication and Computer Systems, City University of London, University of Malaga, Institute of Computing Technology, Chinese Academy of Sciences, DIAS Publishing Ltd, Banca Popolare di Sondrio.

Project GridEcon

Speaker: Dimitrios Sotiriou, Athens Technology Center.

Summary

The overall goal of the GridEcon project is to advance the functionality of existing Grid technology with respect to its capability to allow the economics-aware operation of Grid applications. GridEcon will propose the necessary solutions and extensions to this technology, so that new Grid business models can be implemented. The specific objectives that will be pursued are:

- Define and analyze economic issues that arise in the current and emerging Grid business models by using representative scenarios of Grid computing.
- Develop economic models for service provisioning and resource sharing across organizations.
- Design markets for services at various levels of service provisioning, from basic utility services to web services where buyers can express preferences for quality and reliability.
- Analyze new paradigms of revenue generation, accounting and settlement in the utility services model.
- Design the new components which will add the above functionality to the existing Grid middleware.
- Validate these findings by implementing specific components.
- Maximize the commercial impact of the project results by influencing existing technology trends and by explaining the important role of economics in the development of the new Grid applications.

Technologies

The main technologies involved in this approach are the following:

- Analysis from business perspective (business models).
- Economic analysis and economic models.
- Service Oriented Architecture for deploying Economic Enhanced Components.
- Middleware for existing Commercial Grid Infrastructure (i.e. Amazon EC2).

Expected results

Provide economic-aware components in the form of middleware for enhancing existing Grid Infrastructure and provide the opportunity for creating a dynamic Grid Market.

Useful data

Project name	Grid Economics and Business Models
Acronym	GridEcon
Funded by	European Commission (VI FP)
Contract	IST-033634
Type of project	Specific Targeted Research or Innovation Project (STREP)
Budget	Total cost: 3,5 Million euros / Funding: 2,4 Million euros
Contacts	Coordinator: Jörn Altmann (jorn.altmann@acm.org) Dissemination: : Derek McKeown (derek.mckeown@rtel.com) Scientific: : Jörn Altmann (jorn.altmann@acm.org)
Projects websites	http://gridecon.eu/
Duration	July, 2006 - December, 2008
Partners	International University (Germany), Athens University of Economics and Business (Greece), Ernst & Young - MSC B.V. (Belgium), Imperial College London (UK), LogicaCMG B.V.(The Netherlands), GigaSpaces (Israel), Real-Time Engineering Ltd (UK), Athens Technology Center S.A. (Greece), The 451 Group (UK)

Cyber-Security EU/US. Meet the pathfinders of our future

Jacques Bus¹ (organizer and moderator), Andy Purdy², Jody Westby³, Willem Jonker⁴, Michel Riguidel⁵, David Wright⁶, and Charles Brookson⁷

¹ ICT Trust and Security Unit, European Commission

² DRA Enterprises and BigFix, US

³ Global Cyber Risks LLC, US

⁴ Digital Lifestyle Technology, Philips Research, NL

⁵ Ecole National Sup. des Telecommunications, FR

⁶ Trilateral Research & Consulting, UK

⁷ OCG Security, ETSI

1 Introduction

The AmI.d'07 conference finished with a plenary panel debate focused on the different views of cyber-security aspects and the collaboration between the United States and the European Union.

The objective of the panel was to discuss the future networked world, based on many types of network infrastructure and a service-centric computing model. The debate was preceded by a series of presentations by each of the panellists. Jacques Bus conducted the panel, introduced the subject and the speakers and contextualized the objectives, which were condensed in the following questions:

- How secure and trustworthy will our lives be in the future networked world. Will we be able to protect ourselves against cyber crime (ID theft, phishing, hacking into critical infrastructures with criminal or terrorist aims). What are the vulnerabilities and how can we reduce the risks.
- What will be the level of privacy and data protection. How can users and content vendors be empowered to protect their own data and content. How does that relate to the data retention laws and data collection methods used for policing and intelligence gathering, as well as the data collection for personalised and interactive services. What are the dangers.
- How can research and technology development in ICT help solve these problems, particularly how can it be used to find the right balances.
- How can industry develop devices and services and propose valid business cases that stimulate trust, user acceptance, privacy protection and security.
- What are potential areas of cooperation between the EU and US that can stimulate progress at a global scale towards a secure future, whilst guaranteeing and further enhancing our values and human rights. Which steps can be taken towards such cooperation.

The selected speakers were composed by (i) two persons from the US: Andy Purdy, former acting director of the National Cyber Security Division/US-CERT

of the Dep. of Homeland Security and currently CEO of DRA Enterprises, who was a member of the White House team that helped to draft the US National Strategy to Secure Cyberspace; and Jody Westby, CEO of Global Cyber Risk LLC and Distinguished Fellow, Carnegie Mellon Cylab, who represented Carnegie Mellon University and presented the US research perspective on privacy and security; (ii) two researchers from Europe: Willem Jonker, head of the research sector on Digital Lifestyles of Philips (an important driver behind the concept of Ambient Intelligence), presenting the industrial view; and Michel Riguidel, professor at ENST, addressing in particular security and related subjects in future communication networks; and finally (iii) two speakers providing transversal views: David Wright, who played an important role in an EU funded project SWAMI (Safeguards in a World of Ambient Intelligence) that developed so-called dark scenarios in the future Information Society, and Charles Brookson, chairman of ETSI OCG Security, who provided a view with particular attention to practical problems and solutions, related to interoperability and standardisation that are of relevance in this context.

2 Individual statements

2.1 Introduction by Jacques Bus

Security (protection against violence and crime) is a worry of people since their existence. Circumstances and context make the difference of how to address it. A metaphor can be established between the protection of cyberspace and the protection of citizens. The situation in cyberspace has evolved in a similar way to the transition from the walled castle in the middle ages to the open metropolis now. The means to secure citizens have changed accordingly, and a similar development needs to take place with security on the Net. The traditional approach based on perimeter security is not appropriate any more. Firewalls and isolated systems will still play some role, but it will have to be combined with for example trust and reputation mechanisms to enhance security in the new generation of open and interconnected networks.

Having a protected, private environment which allows for individual creativity, dignity and protection of personal property and data, is similarly universal and of all times. Again the circumstances make the difference of how to address it. The future ambient intelligent environments will have dramatic effects on the openness and complexity of our communication and computing environment, raising enormous data management problems at all levels. In the past it was based on proximity, hiding in a personal place, or going to places where nobody knew you. In the Information Society, with CCTV, mobile phones with cameras, cell phones, Wi-Fi networks, Google searches and visiting Internet websites, one can track everyone's movements in physical as well as in cyberspace.

Living safe but also convenient, without daily confrontation with security controls, fear of arrests and long security queues is essential to ensure trust of citizens in the society. ICT should ensure acceptable and trustworthy security, but not be used for "big brother" or building the "intelligence state". It should

provide for intelligent (smart) and convenient, citizen friendly security, with accountable political and institutional control. This is the scene on which the panel discussion will focus.

Some of the questions to be answered are:

- What are the future and current challenges?
- Can we envisage dark scenarios?
- Do EU and US have different approaches in balancing citizen/societal security against personal freedom and privacy and user convenience?
- What are possible future solutions and which research should we prioritise to avoid dark scenarios and stimulate a development of our society to be prosperous, safe, convenient and stimulating creativity?
- What other means do we need by priority in the battle for a safe live in dignity?

2.2 Andy Purdy

The talk of Andy Purdy illustrated the perspective of preparedness planning and risk management, solidly founded on his experience in the Department of Homeland Security of the USA. He helped to draft the National Strategy to Secure Cyberspace and helped to form and then led the Dept of Homeland Security, National Cyber Security Division and US-CERT, etc. In particular he described the roles and responsibilities defined in the HSPD-7 (Homeland Security Presidential Directive 7) about identification, prioritization, and protection of critical infrastructures.

Regarding preparedness and incident response, processes and standards for certification and accreditation and statutory requirements such as the Federal Information Security Management Act (FISMA) he said these have made a valuable contribution, but significant work remains to be done in the assessment and mitigation of cyber risk to government systems and critical infrastructure. Other mechanisms such as the US-CERT of the National Cyber Security Division (NCSD), the Federal CONOPS (Concepts of Operations), the Information Sharing and Analysis Centers (ISACs) and the Joint Operations Centers were also introduced.

Mr Purdy described initiatives aiming at assessing and managing cyber risk such as the National Infrastructure Protection Plan (NIPP), which includes a formal public-private partnership called the Critical Infrastructure Partnership Advisory Council (CIPAC) established by the Department of Homeland Security to facilitate effective coordination between Federal infrastructure protection programs with the infrastructure protection activities of the private sector and of state, local, territorial and tribal governments. He also described the NIPP Base Plan and the Sector Specific Plans (SSPs) that will be implemented during 2008 to assess the physical and cyber risks to each sector. Finally he introduced the Strategic Homeland Infrastructure Risk Assessment (SHIRA), a classified terrorist-focused risk assessment.

Regarding international collaboration Mr. Purdy pointed at the existence of international watch and warning efforts as one key element that needs to be strengthened. He also highlighted the cyber risks to the global information infrastructure, such as the creation of a black market in attack tools that can exploit common vulnerabilities. All these require enhanced collaboration and information sharing efforts for assessing and mitigating risks due to vulnerabilities and available exploits due to the lack of borders. He mentioned that there are ongoing collaboration activities between the EU and the USA that should be strengthened in the future.

Research and Development were considered important elements that could enhance inter-agency coordination as identified in the Federal Cyber R&D Plan. The National Security Telecommunications Advisory issues recommendations regarding these R&D efforts. He recommended that there needs to be enhanced collaboration and information sharing internationally among governments, academic institutions, and private sector organizations and companies. He recommended the creation of an annual international conference series to promote progress on R&D.

Concluding his talk, Mr Purdy highlighted the important level of activity that one may perceive today, but doubted that the level of collaboration, both internationally and even nationally is yet sufficient. In his view, collaboration efforts can help identify and clarify requirements for action and a need for more adequate resources to meet those requirements.

2.3 Michel Riguidel

Mr. Riguidel discussed the protection of future large polymorphic networked infrastructures being built in society. He highlighted that research must seek to include human and societal values, and awareness of what is achievable (in terms of technical difficulties, cost constraints and 'affordable solutions') and what is acceptable (in terms of civilised ethics and democratic values). Cooperation between laboratories and research centres globally must therefore be built on these two tiers of work. It should not just be measured by what is do-able or saleable, but distinct cultures and a multi-faceted humanism, must be built in the communications and protection tools available to citizens in various global regions over the next couple of decades. This approach to design leads us to research that will bring citizens in a position to understand the security and intimacy stakes, and define and select, at least in part, the level that seems adequate to them. This implies transferring to them the knowledge and means for self-empowerment.

The citizen dimension is essential, at a time when technologies allow communications to be intercepted, to penetrate hard disks from remote, to film and listen to the private lives of people using their own fixed or mobile terminals, to identify and authenticate them, to recognise them morphologically or biometrically using software and sensors. The associated threats open up an enormous field of uncertainty for next generation citizens. The networked world is becoming interdependent, at the same time anonymous and traceable, falsifiable and

recordable, causing equally both illegal possession and computerised interference. This situation calls for more research aiming at location and time aware, adaptable technology solutions.

The approach using community's human values is the only way to set a frontier by consensus, between what will be permitted when using interconnection capabilities, increasing memories, data processing, calculations to break protection codes, and localisation. This concept of a frontier will have to be frequently defined as an arbitrage between sometimes-contradictory preoccupations in the short- and long-term.

Scientists must take the behavioural risks caused by the development of techniques and the appearance of new functionalities into account. The experience of people with e.g. avatars on the Internet, where the sense of privacy is absent, is dangerous particularly for the young who are ever more anxious to communicate. Such issues should be encountered within a framework of international cooperation, taking into account the societal values of different regions like the EU, US, Japan or China and including study of certain addiction phenomena.

Another example of the risk of disconnection between the perception of reality and the materiality of harm can already be found in phishing (the theft of a bank's identity), in identity theft of persons, in the growing feeling not to have committed a crime where you just store a video (police violence filmed on mobile telephones, storage of paedophile records). In respect of all these points the scientist who is involved in products, functions or services that will become operational in 5 to 10 years from now, has the task of working out, imagining and anticipating the effects on the behaviour of both individuals and groups.

In an international collaborative effort, a form of intercontinental thinking must be developed. It must encapsulate the differences, create models of otherness. We will see globally inventions, innovations as well as corruption. We must seek for standards, models, counter-models and alter-models that can bridge between societies, taking into account the arrival of other players (China, India, Brazil e.a.) on the information technology scene.

The 21st century will see a change in concerns, in demography and societal development, a change in power, which must be taken into account without naivety. We must also take into account different movements: e.g. pseudo-libertarians (the so-called 'Naives of the Internet') and those who see repression as the only solution.

A first condition of full cooperation between the EU and USA requires going beyond an idyllic, pre-scripted vision of future networks, and particularly of the Internet. A possible upheaval (in geo-strategic, economic and technological terms) is a variable that should be included, since an historic disrupture that is conceivable in the decades to come might lead to a major international disturbance.

The current vision, stamped with optimism like a Coué method, is based on ideas such as increasingly complex systems that are more interconnected, seamlessly intertwined, supporting broad heterogeneity, virtually self-administering, immersed in a mobile and intelligent environment, populated by ubiquitous

software, saturated with omnipresent information, and with users capable of connecting almost anywhere any time without the constraints of fixed bases, updating their IT programs on line, downloading security updates (anti-virus, anti-spam, error patches, etc.). With this technical system would come the confidence in its mechanisms for security (availability, reliability, and protection), communication (online payment), privacy, identification and authentication for each interlocutor or entity on this worldwide network.

Clearly, we run a huge risk of ending up with a situation in which the traditional implementation methods for security will become inoperable while we have not yet mastered the new forms of security. We must now work on new insights, such as those based on analogies with the bio-living world, and develop autonomic, evolvable and adaptive security mechanisms. It will require new cognitive techniques and semantic models managing the complexity of ambients where people/devices may jointly act and interact. We shall have to take into account a series of key criteria: security, assessability, dynamism of trust, management of complexity, heterogeneity, resilience, dependability, privacy, etc.

Several routes can be considered as a base for future cooperation.

First route: Changing the paradigm, taking account of future ICT pervasiveness with trillions of networked devices, leading to self-organising, self-healing and self-protecting systems. Development of such paradigm could benefit from bio-living world inspiration where such organised communities/populations exist and evolve. It will involve a proper understanding of the ecology of these interactions and interconnections.

This route leads us towards the vision of incremental development and deployment of systems; evolution is incessant, upgrades, changes in functionality, new features are being added at a continuous pace; systems are expected to be able to respond to the changing circumstances of the ambient where they are embedded.

Second route: Rethink the system from the users' point of view. This second possibly disruptive route would seek to change the current asymmetry between users and suppliers/publishers/service providers. The users, whether private individuals or professionals, must take back control (at least in part) of their personal, digital space. Current confidentiality and privacy is fragile, both in respect of commercial service providers and in terms of risks of intrusion and interception by private and public players. This represents a manifest risk of massive availability of digital traces representing behavioural, personal and even biological information (such as DNA, fingerprints, etc). The choice of tools present in this personal data space eludes the control and the knowledge of these users.

It is essential to return users to driving role, by seeking subsidiarity and independence, arriving at developing methods for user-oriented risk assessment; developing methods, tools and repositories to help developers analyse security implications of their code, and more generally to develop verifiably secure software that will guarantee through verifiable evidence to end users that software to be installed on the systems they use is secure.

In this vision, future user-centric systems will offer users personalisation and smooth interaction, a protected and private individual or community 'sphere'. It will also offer trustworthy authentication, anonymity, secure data storage, data matching or exchange, and trusted execution.

Finally we need mechanisms and tools for assessing and proving the security and dependability of a complex system.

The above suggestions are not exhaustive and could be extended with others that touch on the emergence of new types of terminals, biometry and questions of nomadism and mobility.

Mr Riguidel proposed 6 themes for successful cooperation

- definition criteria of true forecasting, free from the immediate imperatives of commercial adaptation of what exists.
- an initial convergence between technical research and research into the social sciences.
- a further convergence between technical research and research into the legal sciences.
- criteria for cooperation between the US and EU.
- adaptation of research into security to European requirements.
- the dissemination of the results: for whom is the research intended?

2.4 David Wright

The talk by Mr Wright was based on the work performed in the FP6 project: SWAMI (Safeguards in a World of Ambient Intelligence (AmI)), funded by the European Commission. This project identified, analysed and described in detail four main 'dark' scenarios to highlight the threats and vulnerabilities in AmI, along with socio-economic, technological, political and legal safeguards¹.

Mr Wright indicated that in order to catch terrorists and criminals it is necessary to know aspects such as who he or she is, what he looks like, how he behaves (his history), where he works, what he is doing and buying, with whom he communicates, etc. In order to achieve this, he described tools that can be used currently, like biometric ID cards with personal data, biometric passports, facial recognition technology, DNA databases, surveillance cameras, location tracking, passenger name records, or data-mining and profiling.

This may take us to what could be called surveillance societies. For instance, in the UK there are 4.2 million CCTV cameras (one for every 14 citizens) and more than 2.4 million DNA samples have been collected already. Likewise the US is believed to perform eavesdropping without a warrant. Finally, on a European level, the use of biometric passports and the EU data retention directive are tools for this purpose.

Mr Wright described possible scenarios in five to ten years from now. In five years, everyone will have a biometric ID card with personal data (China

¹ For more details, see Wright, D., et al., *Safeguards in a World of Ambient Intelligence*, Springer, Dordrecht, 2008.

leads this trend), the DNA databases will be populated with everyone's DNA and surveillance cameras and microphones will be everywhere. Other devices such as 'talking CCTV' ('Hey you, stop that, right now!') and spy drones may have appeared. The Internet of things will be advancing and the trials of Project Hostile Intent (based on monitoring micro-physiological & behavioural cues) will be successful. In ten years, his vision is that we will be able to know who everyone is, what he looks like, how he behaves, with whom he communicates, where he is and when, what he is doing and buying and ... We will be close to knowing what he is thinking. Tracking devices (e.g., implants) will be mandatory and brain scans will show great promise for revealing intentions, types of thinking & behaviour. The project Hostile Intent will be widely deployed and the Internet of things with intelligence will be a reality. At this point no one will have any privacy left.

We can conclude that the existing situation is not adequate to bend these trends and avoid the above scenarios. The UK Information Commissioner, for example, has said that the UK is sleepwalking into a surveillance society. He has said that the number of banks, retailers, government departments, public bodies and other organisations that have admitted serious security lapses is frankly 'horrifying'. The UK House of Lords Science & Technology (S&T) Committee has criticised the 'laissez-faire attitude' towards Internet security by government, manufacturers of hardware and software, retailers, ISPs, banks, police and the criminal justice system.

The main safeguards that we have in order to deal with the current challenges are:

- Legislation (but this can be protective or intrusive), with consultations beforehand
- Privacy impact assessments
- Stronger penalties
- Codes of practice
- Stronger powers to inspect and audit organisations suspected of privacy breaches
- Trust seals with guarantees of standards compliance
- Vendor liability
- Designing privacy into new technologies
- More resources and skills available to the police and criminal justice system to catch and prosecute e-criminals
- Centralised and automated system for reporting e-crime
- Obligation on companies to report data breaches

Mr Wright remarked that the role of 'guardians' is crucial. Among these guardians he included the media, the data protection authorities, the OECD, associations such as Privacy International, ACLU, EPIC, social and other scientists, opposition parties and dissenters in the police, but that the most important one is the citizen him/herself.

Unfortunately, it seems that for the average citizen privacy is not a big issue (except for those who have suffered ID theft). This is illustrated for instance

by the fact that citizens are currently happy to give away privacy for access to websites, or loyalty programs, etc. Many are not aware of security risks and don't use firewalls or other security software and some prefer the security offered by CCTV cameras to privacy. After all, they consider that having their wallet or purse stolen is more intrusive than a camera taking their picture.

2.5 Willem Jonker

Mr Jonker centred his talk on the consumer perspective. He analysed the increasing dependence of citizens on information and communication services.

In his presentation he related the concepts of Ambient Intelligence and Ambient-assisted living, highlighting the importance of safety and protection aspects of the latter. He presented the architecture of a system for remote patient monitoring and highlighted the aspects of heterogeneity (of devices, data connections, authorities, etc.), personalization, safety and responsiveness.

In the previous context, Mr. Jonker concluded that the main challenge for Ambient Intelligence technologies is to overcome the conflict between personalisation and privacy. Although this conflict may be perceived as inherent to these two requirements, such perception is based on current technologies and may therefore be solved with the aid of new underlying technologies. In fact, the current base technologies for information processing were not designed for dealing with the current mix of requirements, in particular with regards to privacy and protection of digital assets.

As a consequence, in the opinion of Mr. Jonker, the main challenge of the network society is to restore the trust that users have gradually lost. He based his position on an interview with David Clark, published on 'Technology Review' in December 2005 1. In this interview it is argued that the Internet is now broken due to the patchwork applied to it during the last years, which has transformed it from a network designed to do a few things well and fast to a dynamic network of embedded systems. One crucial difference is that at the time the Internet was designed, the number of users and their profiles were such that trust could be put on them. This is not the case any more.

To conclude, Mr. Jonker proposed a shift in the focus of the security research. Moving away from approaches centred on systems and information which are focused on the protection against intentional harm, to approaches centred on people focused on creating safety and trust.

2.6 Jody Westby

The talk by Ms. Westby addressed the legal aspects of cyber security research and how they impact cyber security research and development (R&D), differences in the way EU and US address security and privacy issues, and problems that should be addressed through collaboration.

Ms. Westby discussed several security R&D priorities and explained how, in order to deal with these problems, the analysis of traffic data was necessary. She

stressed the point of the identifiability of Internet users and the way the EU Article 29 Working Party (Working Party) has addressed this. A June 2007 Opinion (4/2007) from the Working Party highlights the legal and cultural aspects of privacy and security that differ from the American perspective. She praised the Working Party's Opinion for its clarity and explanation of how personal data should be viewed by national data protection authorities. She also explained some differences between the EU and U.S. approaches, e.g. in the treatment of IP addresses and the mandatory logging of the access information for ISPs. The treatment of IP addresses as personal information is a clear example of 'personal data' in the sense of the EU Data Protection Directive and the privacy personal data should be afforded that IP addresses are not viewed as such under US law.

Pseudonimization was discussed as a possible solution, and a set of criteria for acceptability was discussed. Likewise, other alternatives such as key-coded data and anonymous data were described and discussed.

Ms. Westby compared the EU legal framework with the corresponding US laws and concluded that data and privacy protection is better regulated in the EU and is impacting operations globally. Finally, she concluded that Policy, Legal, & Technical needs in this must converge globally. In her opinion, there is a strong need for the U.S. and the EU to collaborate in order to create a culture of privacy awareness and compliance in the community.

2.7 Charles Brookson

Mr. Charles Brookson addressed the role of standards in the materialisation of the Ambient Intelligence vision. He presented the mission of the European Telecommunications Standards Institute (ETSI) and described the three roles of ETSI, namely: (i) an European Standards Organisation; (ii) a Global Standards Producer; and (iii) a Service Providing Organisation.

He described some of ETSI's activities relevant to Ambient Intelligence, such as Next Generation Networks (NGN), Ultra wideband (UWB), Grid, RFID, Low Power Devices, Emergency communications, Security, Lawful Interception, etc.

He highlighted the importance of security standards, as a crucial element to ensure interoperability. He described how security standards help in guaranteeing adequate levels of security and compliance with the law. Moreover, he explained how these standards contribute to economic realisation and cost reduction. Mr. Brookson provided his view on other reasons for having security standards and presented the catalog of security standards that are developed by the ETSI.

Mr Brookson gave a short overview of the standardisation efforts currently underway in ETSI concerning data protection and identity management. He concluded that, although work is being done, much more is needed, in particular in relation to privacy protection and protection of the personal sphere.

3 Panel debate and audience comments

The panel debate was conducted by Jacques Bus. Taking the emerging trends described above, the main questions asked in this panel were:

- How secure and trustworthy will our lives be in the future Information Society. Will we be able to protect ourselves against cyber crime (ID theft, phishing, hacking into critical infrastructures with criminal or terrorist aims). What are the vulnerabilities and how can we reduce the risks.
- What will be the level of privacy and data protection. How can users and content vendors be empowered to protect their own data and content. How does that relate to the data retention laws and data collection methods used for policing and intelligence gathering. What are the dangers.
- How can research and technology development in ICT help solve these problems, particularly how can it be used to find the right balances.
- How can industry develop devices and services and propose valid business cases that stimulate trust, user acceptance and security.
- What are potential areas of cooperation between the EU and US that can stimulate progress at a global scale towards a secure future, whilst guaranteeing and further enhancing our human values. Which steps can be taken towards such cooperation.

Mr Purdy recognised important risks and emphasised the need for stronger cooperation between countries, not only on a bilateral basis but also at a more global level.

Mr Wright argued that we will not be more secure in the future because it goes against the human nature. There will always be some protection measures that will be broken. He also expressed his view about the future degradation of our level of privacy. One of the reasons for this is the fact that privacy will be sacrificed in the interest of national security. He emphasised the need for the introduction of vendor liability as a mechanism to introduce more security.

Mr. Riguidel focussed on the need for international cooperation and the joint development of a research roadmap, which would include technology, human values, governance and legislative aspects, aiming at a holistic system approach.

Mr Jonker pointed again at the development of personalised services (e.g. interactive TV) and the risks for privacy in its use. He emphasised the need to develop a viable business case that would stimulate the right balance between privacy and data collection and use.

Ms. Westby commented on the need for common traffic data sets for research, and alluded to the difficulties in legal frameworks that need to be resolved. She emphasised that the U.S. could learn from the EU DP regulation and Art 29 WP framework and noted how collaborative cyber security R&D possibly could help resolve some of the legal differences.

Mr Brookson concluded that still much work has to be done on security standards, to protect revenues of enterprises and built an infrastructure that would create trust with consumers.

The audience comments were focused on the privacy aspects and methods for identification. It was stated that indeed the federated identity approach promoted by Liberty is needed, but is not sufficient. There is a need of tools for user empowerment as regulation on use of identity data by enterprises and gov-

ernment is difficult to enforce without such tools. There was general support for the panellists' opinions.

Author Index

- Abdel-Naby, Sameh, 103, 166
Albert, Jérémie, 156
- Badii, Atta, 13
Bajo, Javier, 68
Beun, Robbert-Jan, 23
Bremond, F., 79
Brookson, Charles, 240
Bus, Jacques, 240
- Chaumettea, Serge, 156
Compagna, Luca, 143
Corchado, Juan M., 68
Corvee, E., 79
- El Khoury, Paul, 143
Engberg, Stephan, 13
- Fabry, Johan, 2
Fante, Stefano, 103
- Giorgini, Paolo, 103, 166
- Hoffmann, Mario, 13
Hosaka, Hiroshi, 133
- Javier, Muñoz, 114
Jonker, Willem, 240
- Khalil, Karim, 133
Kung, Antonio, 55
- Labidi, Wael, 92
- Maña, Antonio, 34, 166
Maret, Pierre, 133
Matthess, Manuel, 13
- Mizuno, Hiroshi, 133
Muñoz, Antonio, 34, 143, 166
- Noguera, Carlos, 2
- Paradinas, Pierre, 92
Patino, J.L., 79
Pelechano, Vicente, 114
Purdy, Andy, 240
- Raian, Ali, 166
Renjith, Nair, 13
Rhelimi, Alain, 125
Riguidel, Michel, 240
- Sánchez, Juan M., 68
Sánchez-Cid, Francisco, 143
Sasaki, Ken, 133
Schütte, Julian, 13
Serral, Estefanía, 114
Serrano, Daniel, 34
Setton, Michael, 92
Streitz, Norbert, 47
Susini, Jean-Ferdy, 92
- Tapia, Dante I., 68
Thiemert, Daniel, 13
Thonnat, M., 79
- Valderas, Pedro, 114
van Diggelen, Jurriaan, 23
van Eijk, Rogier M., 23
- Werkhoven, Peter J., 23
Westby, Jody, 240
Wright, David, 240