THE MULTILEVEL JAVA CARD GRID

by

Jonathan Ouoba

with Pr. Serge Chaumette

Report submitted to the University of Bordeaux 1

for the degree of Master of Science

June 2007

Departement of Computer Science

University of Bordeaux 1

- **Abstract**

- **Introduction**

- **Part 1: Background information**

  1. MANets concepts
  2. Grid and purposes
  3. Smart cards and Java Cards
     - 3.1 Smart Cards
     - 3.2 Java Cards

- **Part 2: Existing projects**

  1. MADNESS
  2. Terminode

- **Part 3: Java Card Grid and its variations**

  1. Presentation of the Java Card Grid

- **Part 4: Necessary technologies**

  1. Bluetooth
  2. WIFI
  3. USIM
  4. GSM/3G
  5. APDU

- **Part 5: Research question and solutions**

  1. The Multilevel Java Card Grid
  2. The Chat Application
     - 2.1 Objectives
     - 2.2 Functional description
     - 2.3 Implementtion procedures

- **Conclusion**

- **References**

LIST OF FIGURES

Figure 1.1 – Mobile Communications
Figure 1.2 – Representation of a MANet
Figure 1.3 – Representation of a grid
Figure 1.4 – Smart Cards Categories
Figure 1.5 – A Smart Card
Figure 1.6 – A Java Card
Figure 1.7 – The JCVM Architecture
Figure 1.8 – Development cycle of Java Cards applets
Figure 2.1 – MADNESS Architecture
Figure 3.1 – Java Card Grid Architecture
Figure 4.1 – Possible Communications
Figure 4.2 – Bluetooth Logo
Figure 4.3 – WIFI Logo
Figure 4.4 – (U)SIMs
Figure 4.5 – Command initiaded by Smart Card
Figure 4.6 – Command initiaded by Handset
Figure 5.1 – Multilevel Java Card Grid
Figure 5.2 – Multilevel Java Card Grid
Figure 5.3 – Multilevel Java Card Grid Chat
Figure 5.4 – A Level 0 Group
Figure 5.5 – Communications in the Multilevel Java Card Grid
Figure 5.6 – The Process of sending a message in a level 0 group

ABSTRACT

Mobile Ad hoc Network (MANets) are more and more widespread because of the raising of many reliable wireless means of communication. It leads to the taking into account of security problems and management of nodes in this type of versatile and nonheterogeneous network, which are really difficult to solve. The mobility of nodes and the variety of wireless technologies in MANets context demands a new approach in the global solutions that could be found for these networks, networks that can also contain different wireless means of communication.

The use of smart cards, and especially java cards is very interesting as they are considered as secured devices because of their structure and robustness. Java cards have been used as basic secure bricks in some projects dealing with security like the Java Card Grid.

The question that naturally raises is the following: how can we take advantage of the various and interesting possibilities (in the security field for instance) offered by the java cards in a MANet context integrating different wireless technologies (WIFI, Bluetooth, GSM, 3G for instance).

We think that it is necessary and possible to build a new framework, the Multilevel Java Card Grid, in order to bring some interesting responses to all the main points raised by the association of MANets (with various wireless technologies) and the secured devices that we believe java cards are.

To define the main aspects of our framework, we chosed the option to conceive specific applications such as a secured chat to easily deal with the general structure of the framework and discover what is needed.

Through all this, we were able to clearly identify interesting issues that are to be solved in order to really describe the targeted framework. These problems include identity management, application deployment, commnucation security, multilevel broadcast. Some of them could be solved, but more researches must be done for the others.

A clear definition of the multilevel java card grid could imply the possibility of exploring new application domains in a mobile context and interesting researches on specific problems related to the MANets.

Keywords: MANets, smart cards, wireless technologies

INTRODUCTION

In the context of my Master of Science and Technology option Computer Science speciality Distributed Systems Network and Parallelism at University of Bordeaux 1, I was given a topic of research: the Multilevel Java Card Grid with Professor Serge Chaumette of LaBRI, University of Bordeaux 1.

This subject leaded to have a major study on how it could be possible to bring security and robustness in a MANet context dealing with different wireless technologies (based on mobile phones) by using specific smart cards, the java cards. Thus we choose to develop a new framework, the Multilevel Java Card Grid Framework, object of this paper.

Security is one of the most important aspect of MANet because of the mobility and volatility of the nodes, especially with mobile phones, and java cards are considered as particularily secured devices. It was then important to think about the association of these two elements and what is implied.

This work relies on projects made by the SOD team of LaBRI (Laboratoire Bordelais de Recherche en Informatique), University of Bordeaux 1 and others researchers: first the original project, the Java Card Grid and second the Mobile Java Card Grid.

We will first have a brief review of specific concepts that must be understood to clearly identify and define the problems. These concepts include definitions of MANet, smart cards, java cards. Secondly we will present the Java Card Grid (on which our work is based) and all its variations to be able to correctly understand what could be new in the definition of our multilevel java card grid. We will also make a clear statement of the problem and research question before showing the way we tried to solve the difficulties by the building of the framework through applications conception and the new problems that raised. Finally we will conclude, point the other issues we have to deal with and give the perspectives in future researches.

PART 1: BACKGROUND INFORMATIONS

The development of mobile communications (via GSM or 3G for example) allowed the massive presence of mobile phones in the all day life. It is an interesting idea to try to make them communicate by using all their capacities (WIFI or Bluetooth connectivity) in this dynamic context (where the phones connect and disconnect themselves from the network at every moment) and even collaborate to share their ressources in a secure way. All this goes through a correct and clear understanding of some notions and concepts like MANets and grids. The terms MANet, grid, will then be presented and some stakes that come from these definitions will be explained. A good comprehension of the smart cards in general and particularily Java Cards is also a necessary as we could use it as a the security brick in our work.

1. MANets concepts

figure 1.2 – Representation of a MANet

MANet, which stands for Mobile Ad hoc network, is the name of an IETF work group created in 1998 to make standardizations for the routing protocols using IP technology in ad hoc networks. Since the beginning of this work group the acronym MANet has always been used to identify specific ad hoc networks.

Thus, a MANet represents a particular kind of ad hoc network, a mobile network, where nodes can move around and modify the network topology. To explain it more clearly, MANETs are composed of a set of communicating devices which are able to spontaneously interconnect without any pre-existing infrastructure, in these cases the network configured itself on the fly.

Because of the mobility in MANets, wireless connections are used to connect the nodes with each others. This can be a standard WIFI connection, or another medium, such as a cellular or satellite transmission. It is also important to notice that, due to the dynamic nature of MANETs, they are typically not very secure, so it is important to be cautious about data sent through these networks.

Some MANETs are restricted to a local area of wireless devices (such as a group of laptop computers), while others may be connected to the Internet. An example of MANets is the VANET (Vehicular Ad Hoc Network), which allows vehicles to communicate with roadside equipment. While the vehicles may not have a direct Internet connection, the wireless roadside equipment may be connected to the Internet, allowing data from the vehicles to be sent over the Internet. The vehicle data may be used to measure traffic conditions or keep track of trucking fleets.

In MANets, broadcasting becomes an operation of capital importance for the own existence and operation of the network. MANETs are highly fluctuating networks since they are composed of mobile devices, and both the localization and the number of these devices are continuously changing along time. This dynamic and unpredictable behavior is one of the main obstacles for making efficient communications. Optimizing a broadcasting strategy in the MANETs is a multiobjective problem targeting three goals: reaching as many devices as possible, minimizing the network utilization, and reducing the duration time of the broadcasting process.

2. Grid and purposes

The origin of the grid concept may be established in the early 90's. In a global way a grid must be able to deal with a number of resources ranging from just a few to millions. As we are in the computer science field, *"a computational grid is a hardware and software infrastructure that provides dependable, consistent, pervasive, and inexpensive access to high-end computational*

capabilities." . A grid is then an infrastructure that bonds and unifies globally remote and diverse ressources in order to provide computing support for a wide range of applications.

In other terms a grid:

- makes the coordination between ressources that cannot be centralized in the way they are controled
- uses specific, general-purpose protocols only built for it
- delivers a special quality of service

In order to achieve all its goals a proper grid must meet some specific requirements that can be seen as challenges to solve:

- the capacity to share the available hardware possibilities of the grid with different organizations
- the geographical distribution meaning that the grid's resources may be located at different distant places
- the fact that a hardware can be shared with other organizations must not disturb its normal operations
- the possibility for each organizatiton to keep the control on who gets access to its hardware
- the fact that each organization may establish different security and administrative policies
- the operations in the grid must be performed anonymously

As we can understand from the definition and the objectives of a grid, its management deals with many important concepts: ressource allocation, authentication and authorization, protection, control and accounting.

figure 1.3 – Representation of a grid

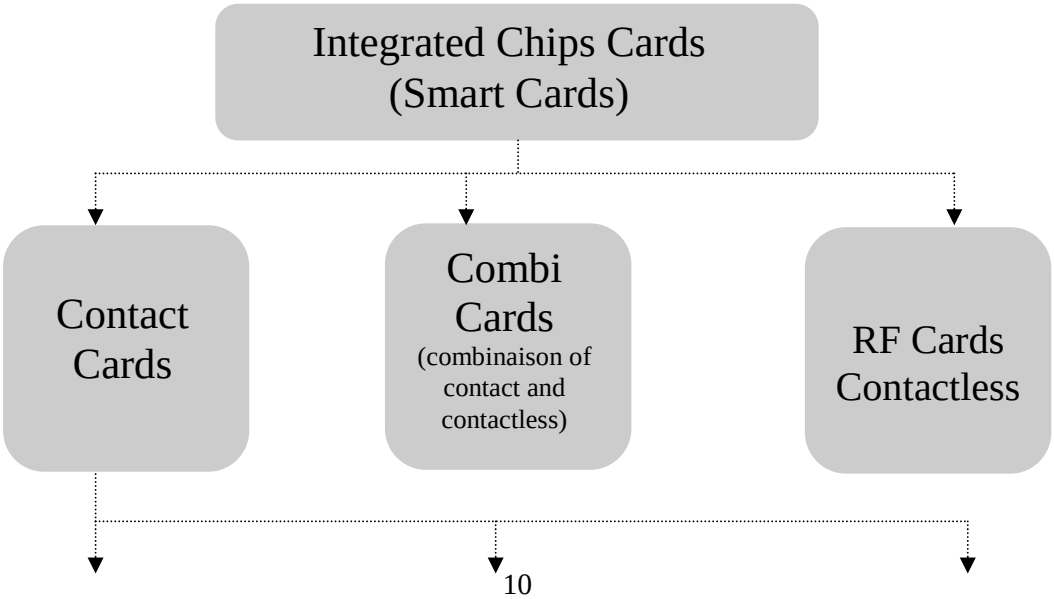
3. Smart cards and java cards

3.1 Smart Cards

A smart card is a piece of plastic containing an integrated electronic circuit and which is able to handle data. It can be programmed to perform tasks and store information. The first smart card was developed in 1974, by the independent inventor Roland Moreno. A smart card can either have a microprocessor and a memory chip or only a memory chip with non-programmable logic which implies that there are different types of cards:

- **Integrated Circuit (IC) Microprocessor Cards.** Microprocessor cards, generally called "chip cards", offer best memory storage capacity and security of data than usual mag stripe cards. Chip cards also can process data on the card.
- **Integrated Circuit (IC) Memory Cards.** IC memory cards can manage up to 1-4 KB of data, and do not contain a processor. Thus, they are dependent on the CAD (the card-accepting device) which is the card reader and are generally used when the card performs a fixed operation.
- **Optical Memory Cards.** It has a piece of a CD glued on top and can store up to 4 MB of data. Once written, the data cannot be updated or modified. Thus, this type of card is ideal for record keeping.

Another interesting category of smart cards is the contactless smart cards which includes secure microcontroller, internal memory and a small antenna, and communicates with a reader through a contactless radio frequency (RF) interface.



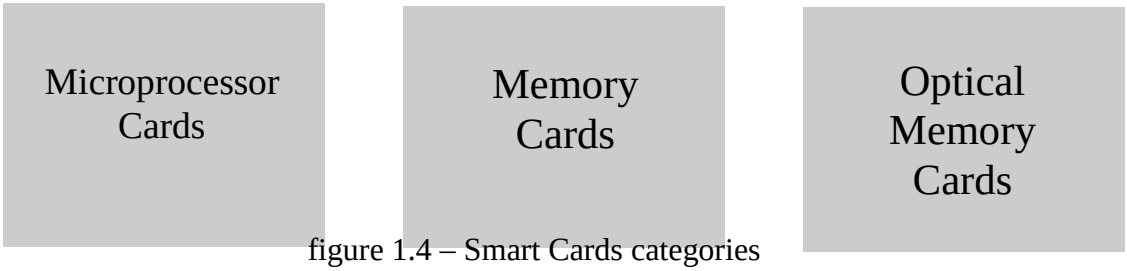


figure 1.4 – Smart Cards categories

One of the most interesting developement in smart cards is the domain of operating systems where we can find two primary categories: the fixed file structure systems and the dynamic application systems. The fixed file structure is used for cards that are considered as secure computing and storage device and which has a fixed structure and functions that will not change. The M.O.S.T. (Microprocessor Operating System Technoloy) Card Family from CardLogix and the FIPS2000 system are products in this style. In the other hand the dynamic application system enables developers to build, test, and deploy different applications securely. Because the operating system and applications are more separated in this second case, updates can easily and repeatedly be made. MULTOS (), CardLogix M.O.S.T. and JAVA card varieties are good examples of this second smart card OS type.

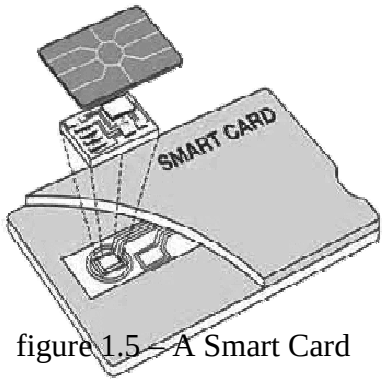


figure 1.5 – A Smart Card

The most common smart card applications are:

- Credit cards
- Electronic cash
- Computer security systems
- Wireless communication
- Loyalty systems (like frequent flyer points)
- Banking
- Satellite TV
- Government identification

Another interesting point is that there is some problems in the smart card world (lack of universal card platform, difficulty in testing cards implementations, difficulty in dynamically updating cards) and the GlobalPlatform standard tries to solve them. GlobalPlatform is thus *designed as a cross-industry standard for the entire smart card infrastructure include card, devices, and systems technology that will increase the total market by facilitating access to and use of smart cards and decrease the costs of implementation. GlobalPlatform is a secure and flexible technology standard that organizes and focuses the single and multi-application initiatives of the many participants in the global smart card industry*.

The next generation of smart cards technology, referred as "connected smart card", will witness the integration of smart cards into the Internet world. The smart card enhancements currently taking place within the marketplace truly represent the next generation technologies in this field, by engaging new markets such as federated identity management and 3G/4G. All this has been initiated by the dynamic advancements of the telecoms sector, and its increasing desire to offer end users innovative services. However, all sectors deploying smart cards will benefit from connected smart card functionality, which fundamentally will have an impact on the interaction smart card end users have with issuers and application providers.

3.2 Java Cards

The java card is a specific multi-applicative smart card using the java card technology. The specificity of the java card lies in the possibility to load and executes program written in a derivative of the Java language and of course get the advantages related to the java technology. It is then capable of running Java byte codes. Like seen before, smart cards do not have a lot of memory so the challenge was to meet all these technologies requirement (java possibilities, card operating system) and provide a card where there is enough space to get programs installed. The applications that run on java cards are called applets.

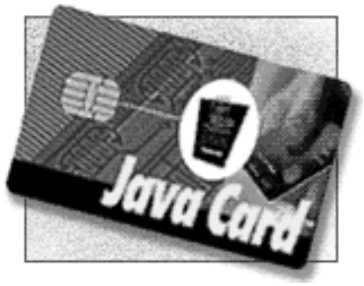


figure 1.6 – A Java Card

In a practical way, the virtual machine in java card technology, the JCVM (Java Card Virtual

Machine) is divided into two parts: the one containing the byte code interpreter which is on the card and the one containing the other functionnality of a classical virtual machine (converter, classes loading, bytecode checking) whom operations are done outside the card, on a work station for example. The JCVM offers portability and platform independency, vendor independency of development and applications, and advanced security mechanisms.

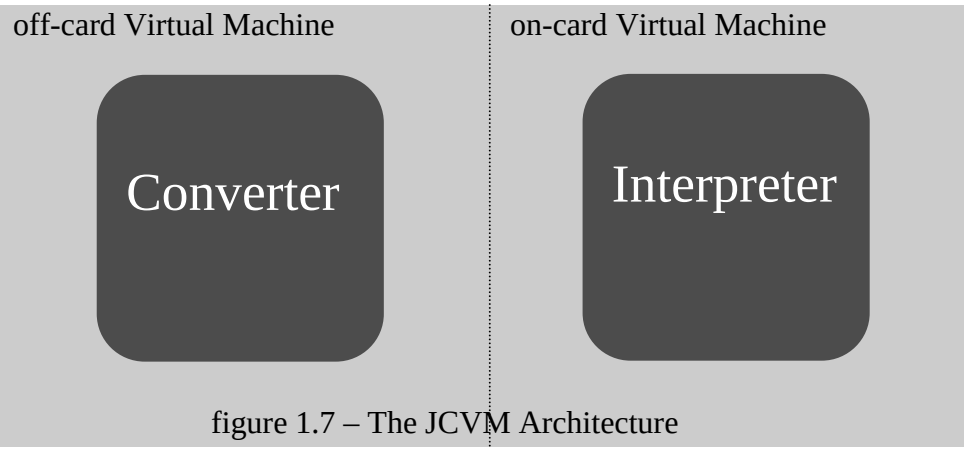


figure 1.7 – The JCVM Architecture

On being given a class file that comes from a Java compiler, the converter of the JCVM produces an executable binary CAP (Concerted Aplet) file that can run on the interpreter, and an export file, after all the necessary checks and byte code optimization. Once it has received a CAP file, the interpreter is responsible for executing the byte code, controlling memory allocation and object creation ensuring runtime security.

Because of this division of the JCVM, the java card contains a JCRE (Java Card Runtime Environment) which gives security mechanisms in order to allow separation (through what we can call a firewall) between the smart card system and the application that run on it. The JCRE manages the card ressources, the network communications, the executions of applets, the security of applets. The JCRE is loaded onto the Java Card at the factory and remains there till the card is destroyed The applets interacts with the JCRE via specific APIs. Each applet on a Java Card is isolated form the others by the « firewall », meaning that an applet has its own independant runtime context.

It is also important to notice that due to the limited capacity of smart cards in general, the language used to develop applets is a kind of subset of the java programming language. There are for example many caracteristics of the original java language which are not supported in the java cards:

- simple data type of big size such as long double or float
- multi dimentional array
- char and strings
- dynamic class loading
- threads

- objects serialization

The development cycle of java cards applets can be summarized in four steps:

- the compilation of the java code source to get the class files
- the debugging and the test of the targeted applet in a java card simulator that runs on a work station
- the conversion of the class files into the necessary CAP files
- the complete test of the applet in a java card emulator (that emulates the JCRE on a work station) and loading on the real java card

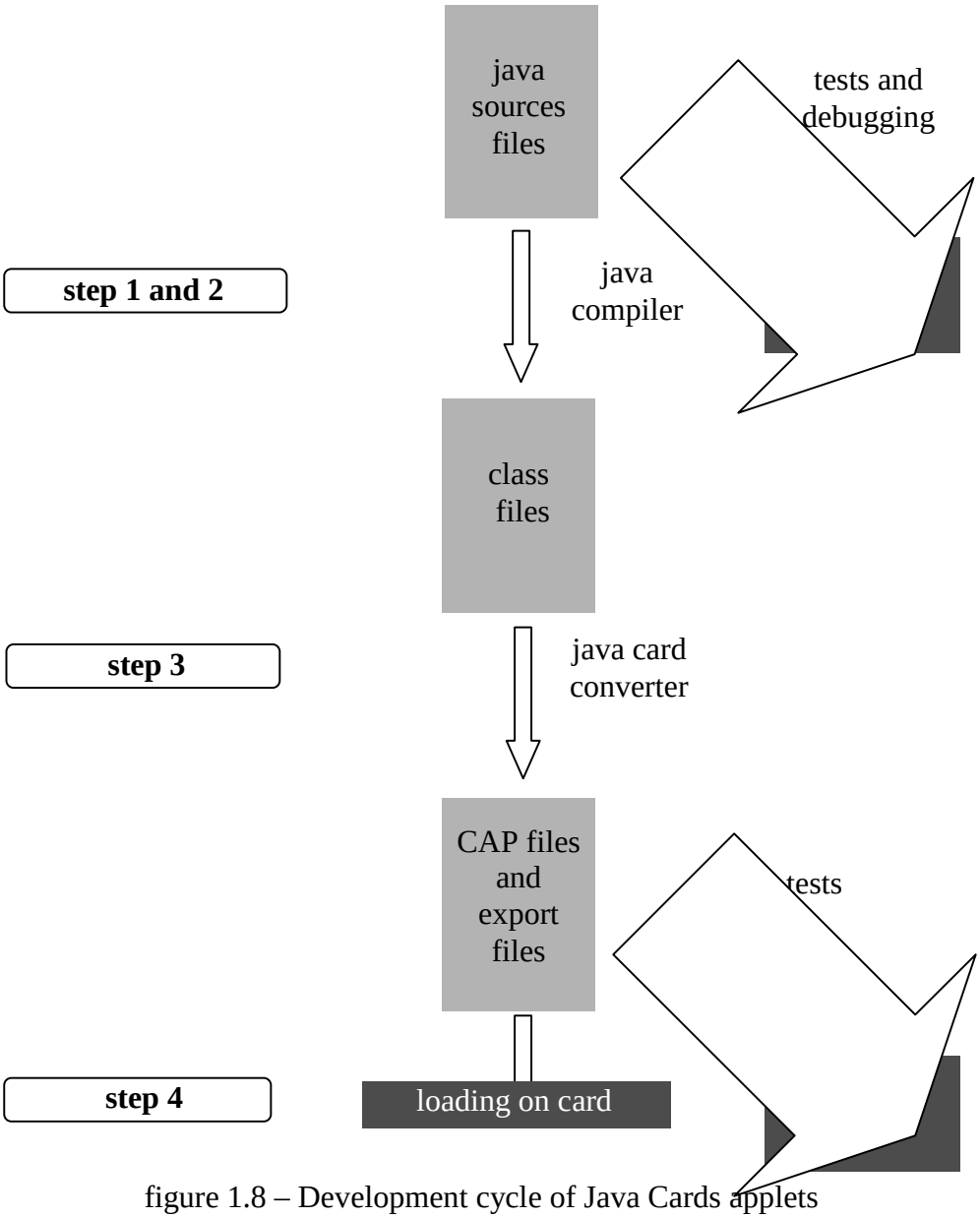


figure 1.8 – Development cycle of Java Cards applets

Nowadays, industries use java card technology in many applications domains such as SIM (Subscriber Identity Module) cards in GSM networks for the mobile phones, financial cards, cards to protect acccess to sensible enterprise ressources. This is due to all the benefits java cards can bring:

- interoperability => applets developped using java card standards will run on any Java Card technology- enabled smart card
- security => java cards use the inherent security of the Java programming language to provide secure execution environment
- multi-application capable => different applications can co-exist on a single smart card
- dynamicity => there is the possibility to install new applications after the issuance of the card
- compatibility with existing standards => it is compatible with the ISO 7816 international standard for smart cards, and important industries standards like GlobalPlatform refer to it.

PART 2: EXISTING PROJECTS

In this part we will focus on interesting (in our context) projects that have been developped or projetcts dealing with the combinaison of smart cards (particularily java cards) and MANets. It is hard to find works that associate mobile networks and the security possibilties of smart cards. It is nethertheless possible to present some intersting researches like MADNESS and Terminode.

1. The MADNESS framework

It is a framework proposal for securing work in ad hoc netwoks. MADNESS (Mobile AD hoc Network with Embedded Secure Systems) is a framework to secure ad hoc networks thanks to secure processing environment such as smart cards. It is assumed that to work in an ad hoc network, a trusted framework is necessary to ensure the co-operation of the mobile codes (so-called agents) and the security of the execution for the global platform. The project is developed at LMSI (Laboratoire Methodes et Structures Informatiques) of University of Limoges.

In a practical way, the framework was deployed on PDAs (MyPal A620BT from ASUS) with built-in Bluetooth communication capabilities and Compact Flash support. On each PDA in the CF slot, we use a smart cards reader (SpringCard-CF from Pro-Active) to exchange with the trusted applications installed on smart cards. The software framework is developed in C# with Visual Studio and based on the .NET Compact Framework. The communications with the smart cards reader and thus the smart cards inserted are realized through the SpringCard .NET API.

On card side, the Java Card technology is used because of its multi-application and dynamic application loading features. The use of Smartcard.NET instead of java cards in the future is more than possible. The cards are JCOP 31 bio from IBM and GemXpresso Pro from Gemplus.

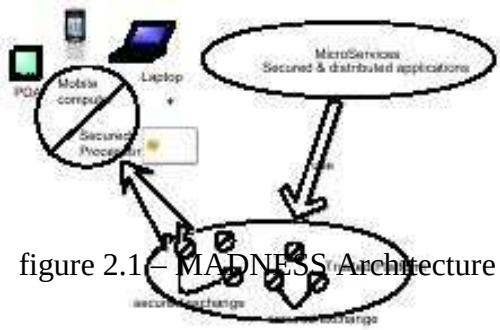


figure 2.1– MADNESS Architecture

2. The Terminode project

The Terminode project follows a system approach to investigate wide area, large, totally wireless networks that we call mobile ad-hoc wide area networks. A network of terminodes is an autonomous, self-organized, wireless multimedia network, independent of any infrastructure. In this project, a radically distributed approach is followed in which all networking functions are embedded in the terminals themselves. Because they act as nodes and terminals at the same time, we call these devices terminodes. A network of terminodes is an autonomous, self-operated network, completely independent of any infrastructure or other equipment. All this work is done at the Swiss Federal Institute of Technology at Lausanne.

Any of the projects presented above, deals with a multilevel aspect in a MANet (integration of multiple wireless technologies) what we want to improve in our works.

PART 3: JAVA CARD GRID AND ITS VARIATIONS

As our work comes from the Java Card Grid project, it is quite interesting to have a presentation of this framework and the variations it produced.

1. Presentation of the Java Card Grid

The goal of the Java Card Grid project developed at LaBRI, Laboratoire Bordelais de Recherche en Informatique, is to provide a secure hardware and software environment to experiment and thereafter propose innovative high level security solutions for distributed and mobile applications. The Java Card Grid is a grid-like hardware platform composed of a number of Java Cards (readers) connected together through USB hubs. Several grids can also be connected through the Internet.

figure 3.1 – Java Card Grid Architecture

Actually the general architecture of the Java Card Grid includes:

- two smart card servers, about fifteen cards readers are connected to each one through USB hubs.
- a data server which hosts a database where the informations related to the cards are saved.
- a proxy server, gateway between the Java Card Grid and others environment. The users of the Grid are connected through this server.

In the Java Card Grid, there is two kinds of communications depending on the device and destination of the message:

- extra-grid communication when an user want to get access to a specific smart card and communicate with it
- intra-grid communication, involving the components of the grid architecture

In the extra-grid communication, all the messages go through the proxy server which is a gateway between the users of the grid and the smart cards. To allow the users to contact the proxy server, the RMI (Remote Method Invocation, a Java API) technology is used, so it is possible to call remote methods in the process of communication. In the other hand, the Call Back mechanism (derivative of the RMI) is useful to allow the server to initiate communications with an user.

Concerning the intra-grid communication three types are possible:

- communication between the proxy server and the smart card servers. As the server proxy is a gateway, it must be able to communicate with all the components of the grid. Like in the

extra-grid communication RMI and Call Back procedures are used to develop these communications.

- communication with the database which is used to update the informations related to the smart cards of the grid (through SQL requests). The data server gives services allowing the remote access to the database for the smart card server and the proxy server, through the DBMS (Database management System).
- communication with the smart card. It represents the communication between the smart card and the smart card server. The APDU (Application Protocol Data Unit, ISO 78164) protocol using the API PC/SC (standard communication PC – Smart Card, the smart card and the card reader) allows it.

PART 4: NECESSARY TECHNOLOGIES

A detailed diagram of the communications that can take place in our projects will be presented and the useful technologies which must be known will be briefly explained.

The diagram of the possible communications in our work can take this form (as our network is composed of mobile phones):

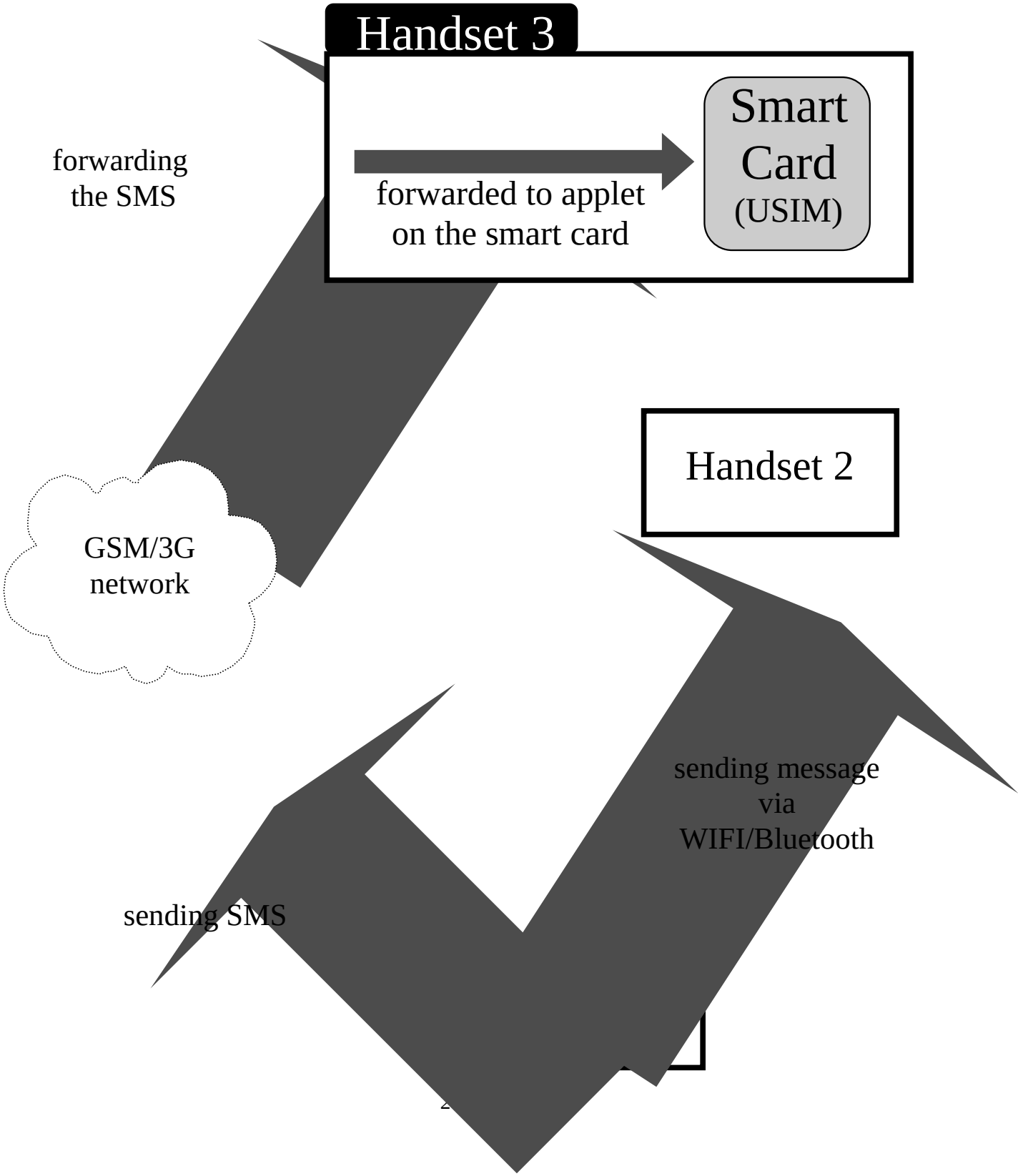


figure 4.1 – Possible communications

1. Bluetooth

Bluetooth is communication protocol via radio waves defined by Ericsson, IBM, Intel, Nokia and Toshiba. The goal of this protocol is to standardize short distance wireless communications between computers, PDAs, mobiles phones and others peripherals in an operating range of 100 meters. It was designed to be used with portable peripherals and lower power consumption. It is a kind of wireless equivalent to the USB (Universal Serial Bus) and consequently can not be used to build networks or connect several computers. Bluetooth is a IEEE standard under the reference 802.15, the maximum transmission flow is about 1 Mbit/s and it uses the frequency band of 2.4 Ghz. The name bluetooth comes from a nickname given to the Swedish king who gathered and federated the Scandinavian countries.

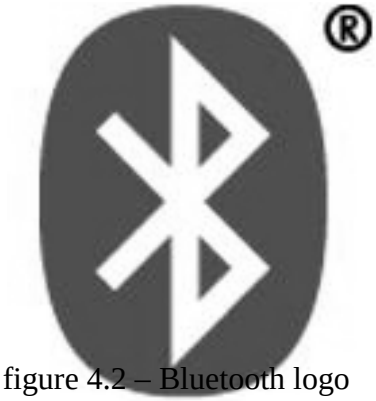


figure 4.2 – Bluetooth logo

2. WIFI

WIFI (Wireless Fidelity) is a wireless network technology able to allow communications between computers, PDAs and even cell phones (that have the WIFI capacity). It is defined as the 802.11 IEEE standard, the transmission flow is about 11 Mbits/s (802.11b norm) and 54 Mbits/s (802.11a/g norms) and it uses the frequency band of 2.4-2.4835 Ghz. The operating range is about several tens of meters, and in and open environments it can goes up to several hundred meters even kilometres in the WiMax variation. In a concrete way, it is possible to create a local network using the WIFI protocols. There is two connection mode to a WIFI network:

- the infrastructure mode where there is an AP (Access Point) that plays the role of a hub or a switch
- the ad-hoc mode where there is a direct connection between the equipments (in the case of an ad-hoc network for example)

The WIFI is kind of wireless equivalent to the Ethernet network and deals with the low layers of the

OSI model (data link layer and physical layer).

figure 4.3 – WIFI logo

3. USIM

USIM stands for Universal Subscriber Identity Module and is used with third-generation (3G) mobile phones. It is a removable smart card which is inserted in the mobile phone and keeps the subscriber and the authentication informations. For authentication purposes, the USIM stores a long-term preshared secret key, which is shared with the Authentication Centre (AuC) in the network, it can also provide storage space for text messages and phone book contacts.
The equivalent of USIM on 2G (second-generation) networks is the SIM (Subscriber Identity Module) in the GSM case. SIM cards securely store the service-subscriber key used to identify a cell phone. With SIM cards, users can easily switch phones by inserting it into another mobile phone.

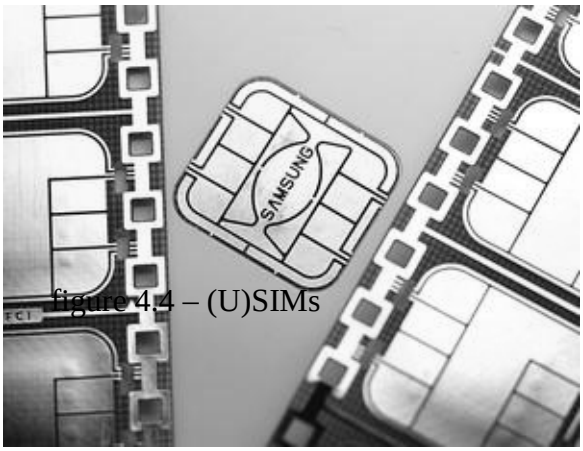


figure 4.4 – (U)SIMs

4. GSM/3G

The GSM is the Global System for Mobile communications and represent the standard network for mobile telephony (the most used in Europe) defined by the ETSI (European Telecommunications Standard Institute). It is a 2G, second-generation, standard because the communications function

according to an entirely numerical mode. The GSM became an international norm in 1991. In Europe it is the 900 Mhz and 1800 Mhz frequency bands that are used and in the United States the 1800 Mhz one. The GSM norm allow a maximum transmission rate of 9.6 kbps, which make possible the exchange of text messages (SMS, Short Message Service), multimedia messages (MMS, Multimedia Message Service) and of course the sending of voice.

3G, which stands for third-generation, is the telephony standard which comes after the 2G. It is build on the UMTS norm (Universal Mobile Telecommunications System) and permit transmission flows that can go up to 2Mbps. 3G include the possible use of IP (Internet Protocol) but it will be totally achieved in the 4G, fourth-generation, mobile phones networks.

5. APDU

The communication protocol between a smart card and the CAD (Card Acceptance Device) use the APDU (Application Protocol Data Unit) which is a data package. A CAD can be a card reader or a mobile phone for example. The dialogue between the card and the CAD is made of commandAPDU (which contains a command for the smart card, the applet on the card executes it) and responseAPDU (containing the answer to the sent command). The ISO norm ISO 7816-4 defines the way to use the communications APDU.

For instance in a mobile phone the command sent can take two forms:

- commands initiated by the smart card => the card indicates to the handset that it has an instruction to execute, the phone fetches the list to get the ready command in the card and processes it, then a result message is sent to the card

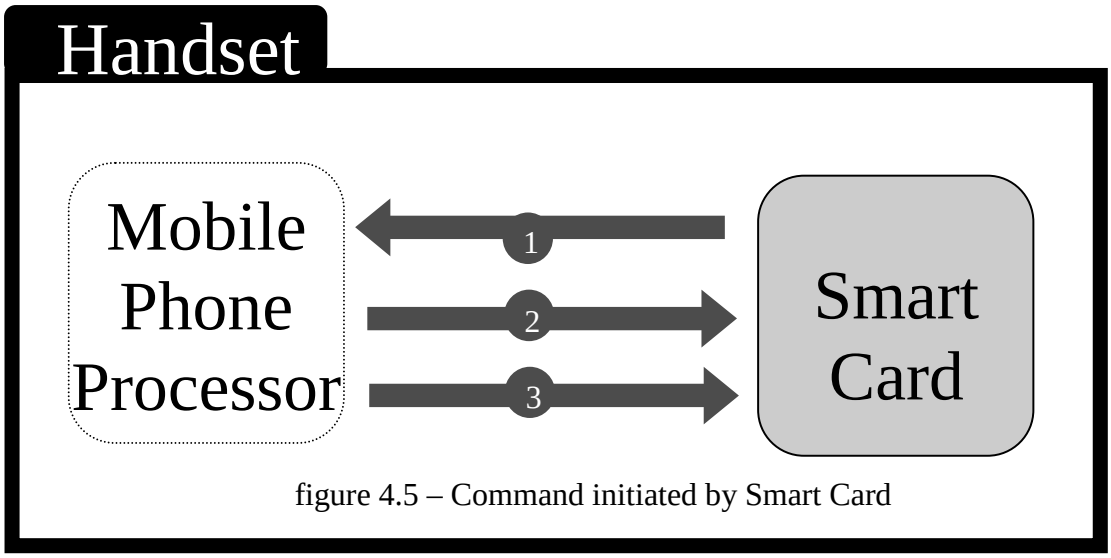


figure 4.5 – Command initiated by Smart Card

1=>indicates a ready command (status word)

2 =>fetches to get the ready command and executes it

3 =>sends a responseAPDU (result of the command)

- commands sent by the handset => the phone sends a message containing the command to the smart card which executes it and sends the result

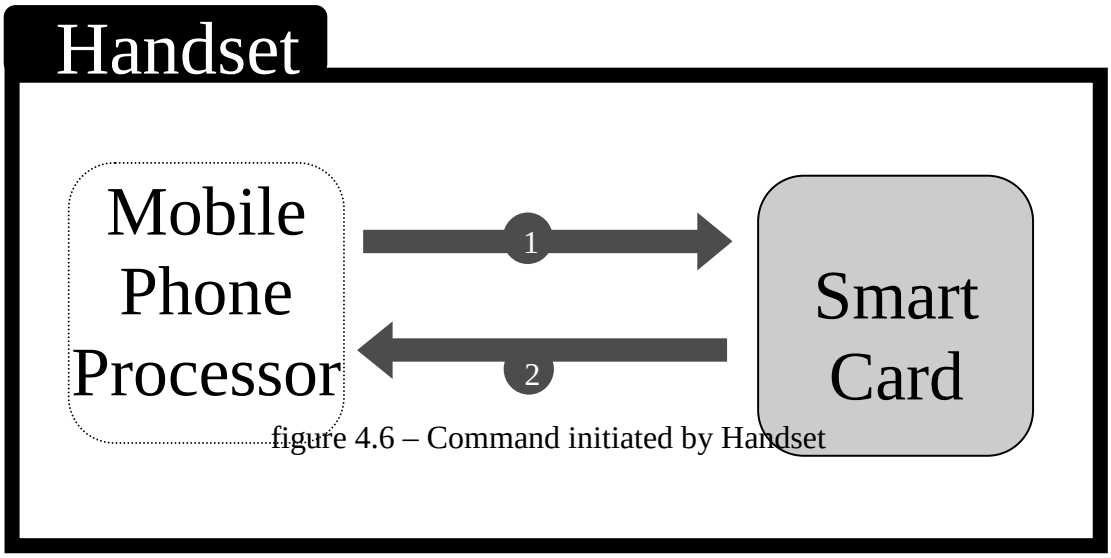


figure 4.6 – Command initiated by Handset

1 => sends APDU message with the command
2 => sends response APDU (result by a status word)

PART 5: RESEARCH QUESTION AND SOLUTIONS

A presentation of the answer to the research question will be presented through the description of the Multilevel Java Card Grid, a chat application which would illustrate the building of the framework will also be described.

1. The Multilevel Java Card Grid

The goal of the Multilevel Java Card Grid project is to explore new application domains, by extending to a mobile context based on mobile phones the possibilities offered by the original Java Card Grid (cf. Presentation of the Java Card Grid) developed at LaBRI, Laboratoire Bordelais de Recherche en Informatique. This project is therefore an extension of the Java Card Grid, defining a multilevel framework which could bring security and robustness in communications in a mobile environment.

In a practical way the multilevel grid will be composed of (U)SIM (with Java Card technology) cards embedded in a set of mobile phones, so that it will be possible to use the properties of the Java Card Grid and extend them in this new context.

The framework architecture is divided into two levels, allowing us a management of the communications between devices depending on the destination of a message. The first level of communication (level 0) will use the Bluetooth and/or Wifi connectivity of the phones when the destination of a message can be reached by this way. The second level of communication (level 1) will be supported by the GSM/3G network possibilities and will be used when the destination is not in the direct environment (reachable via Bluetooth or Wifi). The principe is quite simple to understand:when a message has to be sent, it is checked to verify which level of communication to use, the GSM/3G network or the Bluetooth/Wifi possibilities.

The challenge to solve is to be able, through this multilevel framework, to deploy applications which will work with security and robustness in the mobile multilevel network context. We must obtain a high level of confidentiality regarding the binary code, the input data handled, and the results produced; we also need to get the ability of the system to maintain function even with the changes in internal structure or external environment.

Through the definition of the Multilevel Java Card Grid Project we can assume that it shares some aspects with the MADNESS (Mobile Ad Hoc Network with Embedded Secure System) project developed at the XLIM (Unite Mixte de Recherche UNIVERSITE de LIMOGES).

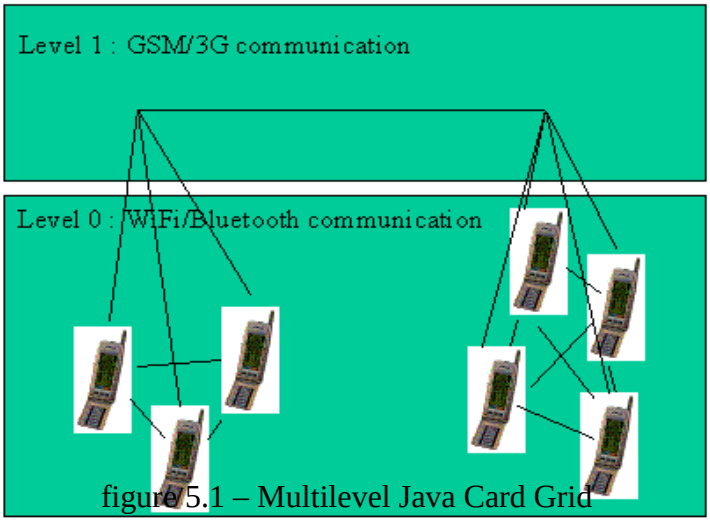


figure 5.1 – Multilevel Java Card Grid

2. The Chat Application

2.1 Objectives

To illustrate the development of the multilevel javacard grid framework, an application taking advantage of all its possibilities must be conceived. To achieve this goal we try to develop a secured chat program, an instant messaging application where each node of our grid will be able to commnicate with others using the multilevel aspect of the framework. The grid is composed of (U)SIM cards embedded in a set of mobile phones, so the program will be developed through midlets (on the handsets) and applets (on the javacards) which communicate with each other through specific protocols (APDU).

An instant messaging application or a chat is a program allowing client to exchange text messages. It differ from e-mail in that conversations are able to happen in realtime mode. Each client has a contact list, showing the peoples it may able to talk to and if they are connected or not to the network. This mean of communication gives many advantages such as the possibility not to immediatly answer to an incoming message (making it less intrusive than communication via phone), the realtime aspect, an easy collaboration between the clients.

The added value of the multilevel javacard grid chat stands in the fact that it takes benefit of the multilevel aspect of the framework. The messages exchanged by the clients will use a path or a mean of transport depending on the destination they must reach. When a message is sent, it is checked to see if the recipient is in the direct environment (reacheable easily via WIFI/Bluetooth), in that case the WIFI/Bluetooth protocols are used, in the other cases the information (text message) goes through SMS via the 3G/GSM network.

In addition the applicationwill be totally secured, using the javacard technologies and trying to handle the nodes identities and the control of message privacy during communications.

To achieve all these objectives, many problems are to be solved in the MANet context where the program relies:

- multilelevel management
- communications
- identities of management
- security of communications
- application deployment in each node of the grid

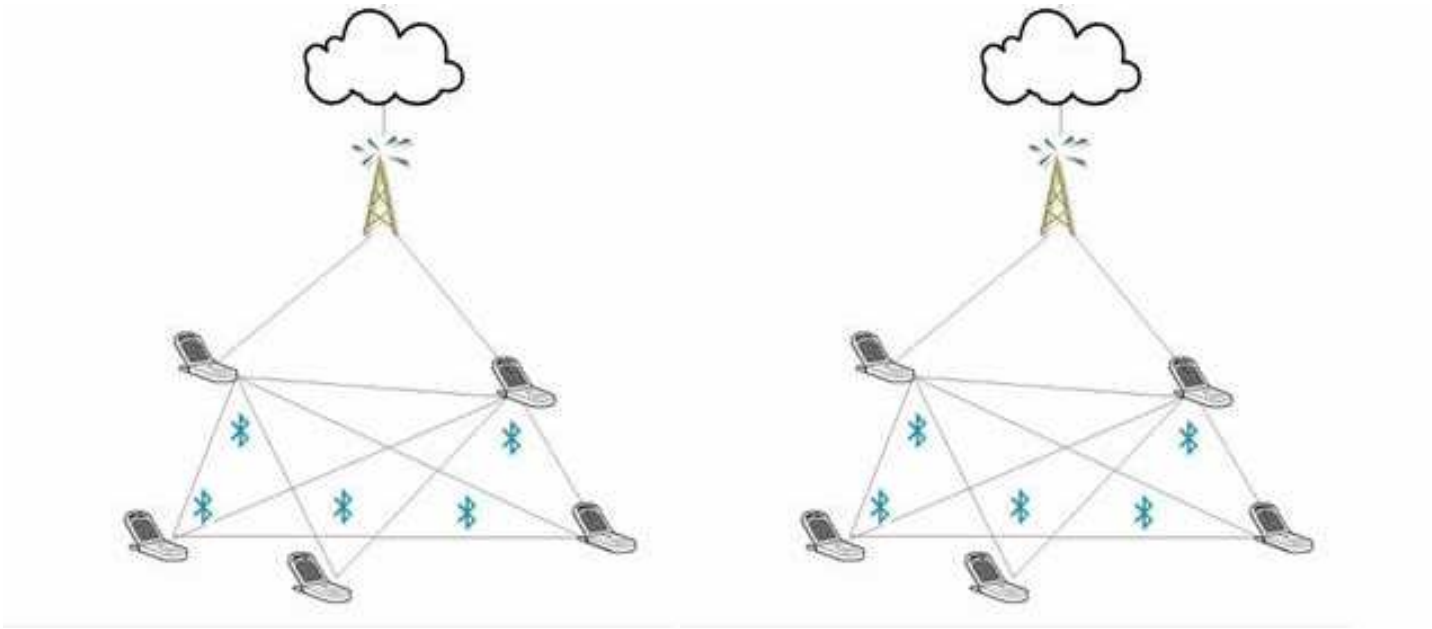


figure 5.2 – Multilevel Java Card Grid

2.2 Functional description

The goal of the chat is to allow the nodes forming the grid to communicate with each others through text messages. In the context of the multilelvel project the nodes of the grid are mobile phones with javacards. In this chat application the nodes will then be able to send and receice messages from correspondents whom the identity is known.

The exchange of the messages during the conversation can have different forms, depending on the situation and position of the nodes. Indeed the grid is distributed into two levels.

In the first level (level 1) are gathered in the same area the devices that can reach each others directly via bluetooth and/or WIFI, in that case the communications uses these protocols. Consequently the chat allow the members of the same level group and who know each others to discuss through text messages.

The second level (level 0) handles the communications that take place betweeen nodes which are not in the same first level group, which do not belong to the same WIFI/Bluetooth area. In this situation the nodes participating to the discussion send and receive the text messages by using the 3G/GSM network. The SMS (Short Message Service) is used for this purpose and for simulating the instant messaging application.

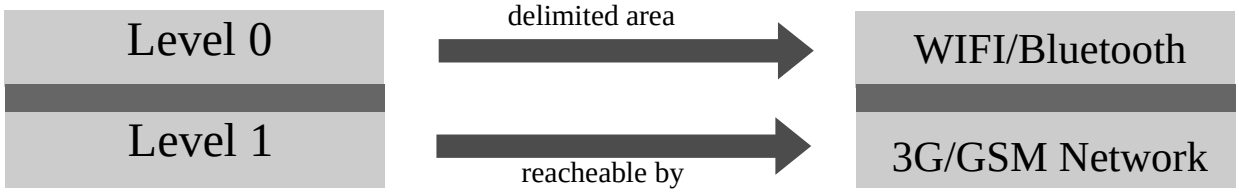


figure 5.3 – Multilevel Java Card Grid Chat

To the user all the elements described above are transparent. It is the application which manages and evaluates the position of the recipient before using the appropriate mean of communication to

deliver the message.

As already told in the objectives, the achievement of the installation of all the features of the chat application presents many problems that we need to solve. The functional description leads to the implementation procedures where we try to give some solutions concerning the security management, the communications mangement and other importants aspects of the multilevel javacard grid chat.

2.3 Implementations procedures

***multilevel management**

As explained in the functional description, the multilevel framework uses two level to manage the sending of messages between the nodes of the grid. At the level 0 we consider the nodes which are in a delimited area, covered by WIFI/Bluetooth networks. Consequently at this level (0), many groups can be formed.

At this point a definition of the meaning of a group in our understanding and in our conception is necessary. A group is represented by a complete graph which means that each node of the group is able to directly get access (through a direct link) to the other nodes.

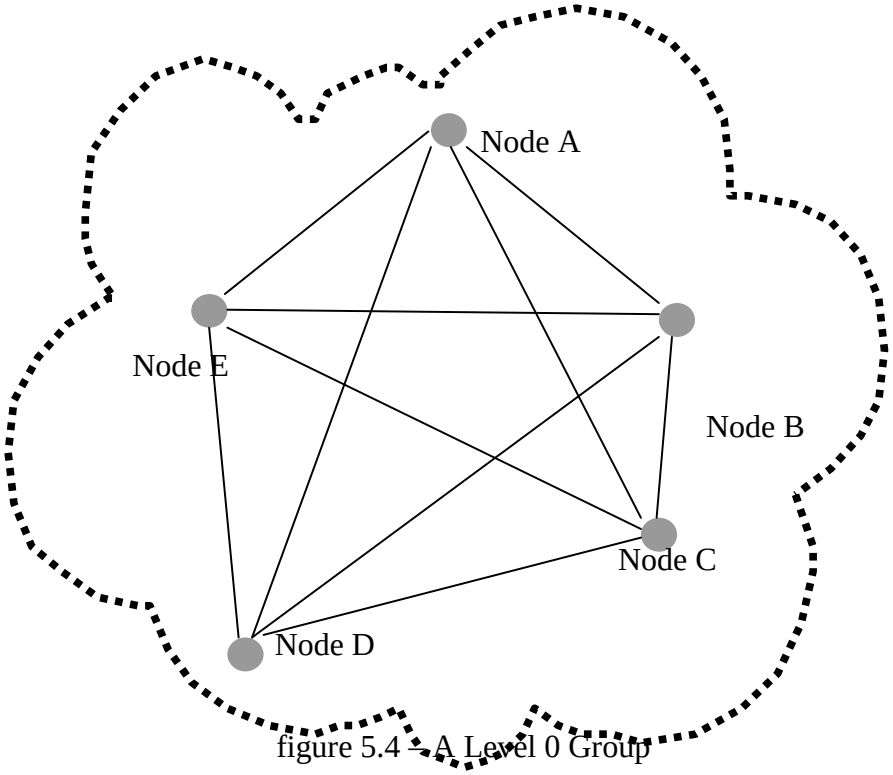


figure 5.4 – A Level 0 Group

In the other hand the level 1 is used when the recipient node is not the current group of the one which want to send the message. In this case the text is sent via a sms.

After all this description a question raises: how do I know that the node I want to contact is a local one (in my level 0 group) or a remote one ? This is the most important issue we have to deal with to easily and correctly manage the multilevel aspect of the grid.

The concept is quite easy to understand. At the connection, a node browse the neighborhood to get the identities of other peers which are present (in his level 0 group) and built a list of it. When it has to send a message to a specific client, it checks the list to see if the recipient is in the local area (listed in the contacts informations). If the recipient is in the level 0 group, the WIFI/Bluetooth technologies are used to send the message and an acknowledgement information is expected.

In the case the recipient is not in the local area or the confirmation of the reception of a sent message is not received, the level 1 of the framework is activated by sending a sms (through the 3G/GSM network) to reach the specified destination. All the tests to see which way (by level 0 or by level 1 of the multilevel grid) a message has to take are carried out in the local area, in the level 0 group of the concerned node.

It is important to notice that a filter is necessary on each node of the grid to avoid the reception of a duplicate message (for instance when an acknowledgement message is expected).

*** communications**

By analyzing the precedent descriptions, it is evident to consider that two kind of communications are possible:

- local communication, involving nodes in the same level 0 group (WIFI/ Bluetooth area)
- remote communication through the 3G/GSM network

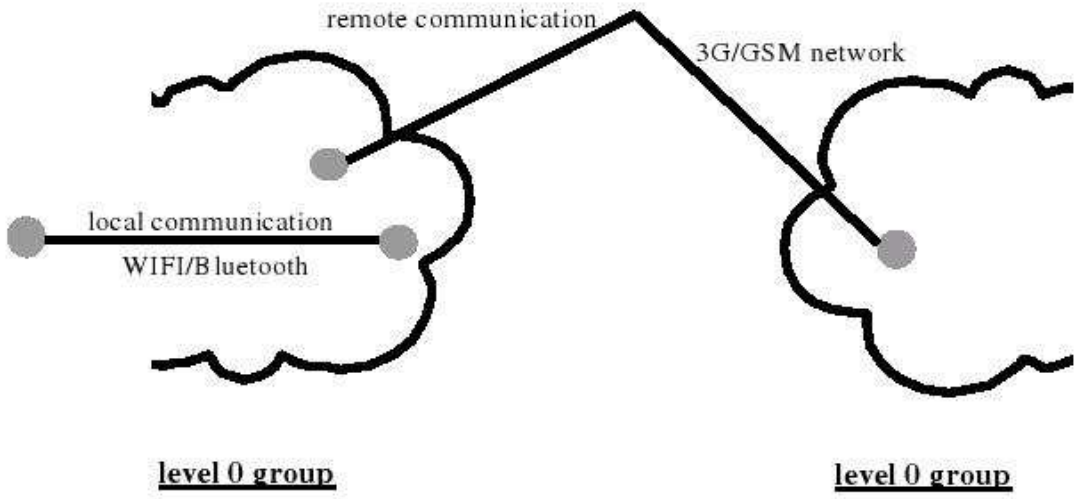


figure 5.5 – Communications in the Multilevel Java Card Grid

A local communication can also takes two forms: targeted messages and non targeted messages depending on the goal of the action.

In the targeted form, the identity of the recipient is known and all theses informations allow us to reach the required node directly. In this case a specific strategy of communication is necessary, using the multilevel management system. When we want to send a targeted local message, it implies that the identity of the recipient is known. We get address of the node to contact (by the list) and we send the message. If a confirmation of the reception of the message is not returned, a new discovery of the neighbor is done (to check if there is no address change) and we try to send the message again. If that fails, the sending of the message in the local area is impossible and we must use the remote communication.

In the non targeted form we use a kind of broadcast to reach all the nodes constituting a group (using the contact list built after the discovery of the neighbors). The question of a common identifier arises, to send a broadcast in the best way we need to know the precise definition of a group in the terms of identities.

A remote communication takes place when no local communication is available to reach one or many recipients of a message. In the targeted form of a remote communication we use the number alloted by the GSM network to the card of a node to send a sms message.

The non targeted form, in the broadcast way, poses some problems we neeed to resolve.

*** identities management**

The problems of the identity of each node and its diffusion to the other components of the grid is a central point of the framework.

The multilevel grid is composed of smart cards embedded in a set of mobile equipments which is connected to the GSM network (to be able to send and receive sms). It is thus possible to consider that the identity of each node is represented by the number attributed by the GSM operator to the (U)SIM card, as this number is supposed to be unique and not variable. The identity of each node is then linked to the smart card, so there is no problem when the equipement containing the card changes, the identity remains the same.

The diffusion of identities in a level 0 group is done when a node discover all his neighborhood. It receives the names (GSM number) of the neighbors and the MAC address of the mobile equipements in order to be able to communicate with them directly. To contact a node which is in another level 0 group, its identity must be known (given), as to call somebody its phone number should be known.

*** communications security**

Communications security tries to insure message confidentiality and authenticity, to deny unauthorized persons to have access to exchanged informations betweeen two sources. It includes transmission security, emission security and physical security.

First of all, it is interesting to focus on communications that take place between nodes of the same level 0 group (using Bluetooth/WIFI tehnologies). It is not dangerous to affirm that smart cards are quite secured devices, so are javacards which is an important point in the search of security.

The protocol used here, in the context of the multilevel javacards grid chat is completly inspired by the work of Eve Atallah and Serge Chaumette on «A Smart Card Based Distributed Identity Management Infrastructure for Mobile Ad hoc Networks » at LaBRI, University of Bordeaux 1.

The identity of each smart card of the grid is defined at its creation in factory, making it unique ; it also contains a global public key, a unique asymmetric key pair whom the public key is signed by a global private key (related to the global public key). At the beginning, when a node discover his neighbors, it receives from them (each of them) a message with their identities and their public keys signed by the global private key. Consequently, in his contact list, a node has the identities of the people his can access and their public keys. This method can also be used between two nodes to exchange a session key in order to iniate and achieve a secure communication.

So during a communication, the involved nodes encrypts each message with their private key before sending it. In the other side, the recipient, at the reception decipher the message by using the public key of the sending node (which must be in his contact list he built in the discovering of his neighbors).

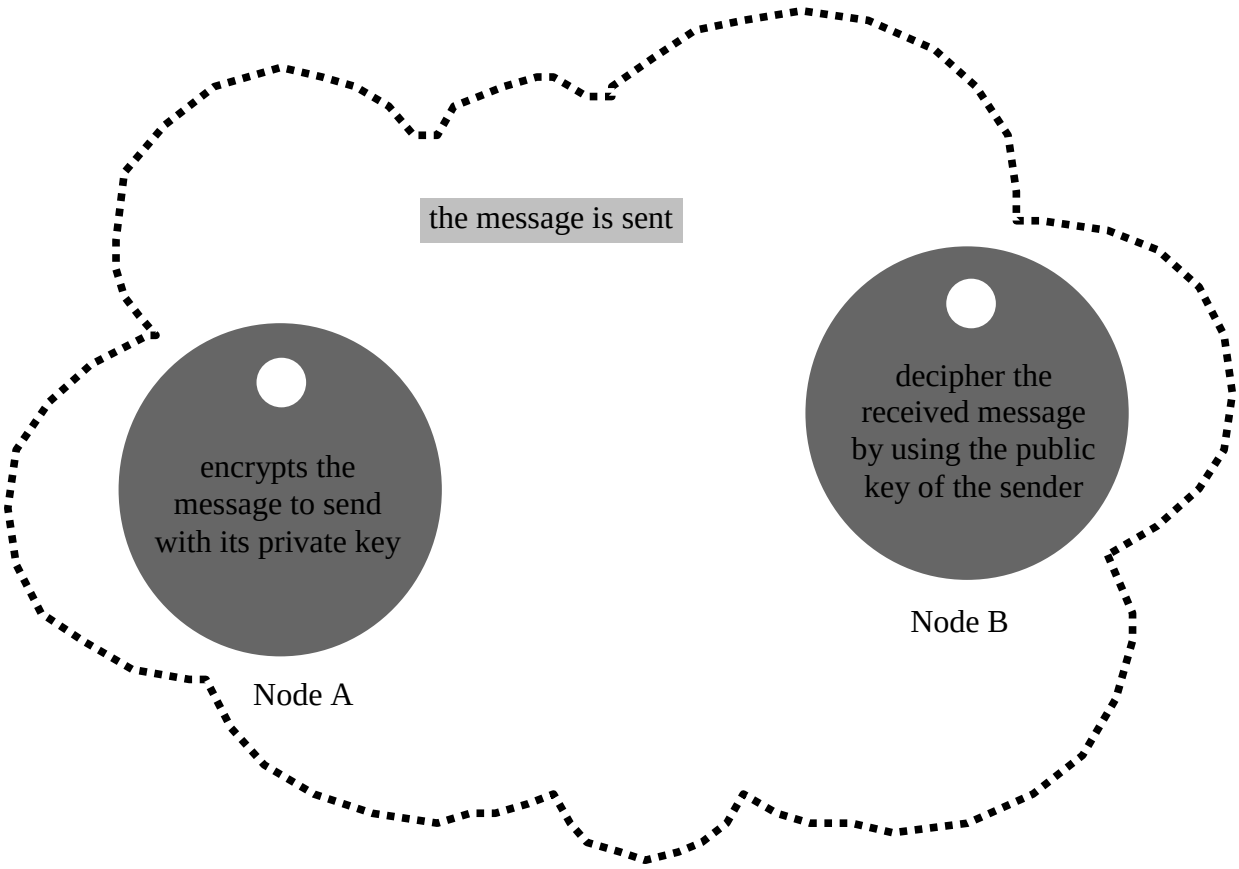

the message is sent
encrypts the message to send with its private key
Node A
decipher the received message by using the public key of the sender
Node B

figure 5.6 – The process of sending a message in a level 0 group

*** application deployment**

If we want our application to be used in a large scale, we need to find a way to allow users to install it on the smart card.

The solution could be to have a server where the application download will be possible and then the installion on the smart card as it supports post-issuance applications installations. It is also important to be sure that the application developed can be deployed in a safe way for each node of the grid. The problem is then to authenticate an application source before allowing it to be put on the smart card through the CAD (the mobile phone in our context).

In this case it is interesting to use the architecture build by William G. Sirett in his thesis work at the Royal Holloway University of London on "Temporally Aware Behavior-Based Security in Smart Cards". This solution can be described in four points:

- the server encrypts the byte code application with a shared (with the smart card) pair of keys. the server must know the unique identifier of the smart card to use the corresponding keys
- the server packs the encrpyted data as a device application and signs it with using the security measures developed between the server and the device
- the package is transfered on the device which anthenticates the source of the application before installing it (as it considered it as a device application). As the device does not have the secret used to protect the smart card application, it just stores it
- the installation on the smart card can be initiated by the server or by the user, anyway before starting the real intallation process the card wait to receive the server authentication. The encrypted bytes are then decoded and installed when all the necessary verifications are done through the shared secret between the smart card and the device

CONCLUSION

With the development of mobility in the networks and the big need of security that raise, it was important to start a reflexion on the combinaison of theses two elements, with the use of smart cards. In this context the Multilevel Java Card Grod project is a very interesting and innovative project as it deals with two concepts which are really widespread in nowadays information technologies: MANets and Smart Cards. The conception of this framework is a try to build a new structure allowing secure communications in a mobile ad hoc environment with different wireless technologies by using Java Cards. The Multilevel Java Card Grid is the natural continuation of the works developed at LaBRI (and others research institutes) since the publication of the results given by the Java Card Grid original project.

It was possible, through the conception of a chat application, to identitfy the main points causing some difficulties with the MANets approach in the framework:

- communications security
- multilevel management
- identites management
- application deployment

The studies also allow us to discover and apply new techniques in bringing solutions to the problems raised by the utilisation of MANet (in our context) especially in the fields of identities, deployment of applications, and integration of multiple wireless technologies.

There is still a lot of work to do since many others problems need to be solved. It will be interesting to continue the conception of the secure chat for our framework, and also try the implementation of new applications such as a virtual money management system to be able to discover other aspects of the Multilevel Java Card Grid we have to deal with and get functional prototypes. It is also important to continue the reflexion on the solutions found during the work. Another essential point will be to include in the future researches the use of 3G network IP possibilities, the security in 3G/GSM networks (for SMS for instance), and the definition of a multilevel broadcast in th e framework.

REFERENCES

1. Java Card Technology: java.sun.com/products/javacard

2. The Terminode project: http://citeseer.ist.psu.edu/update/235272

3. The Pleex project: http://maeglin.com/pleex.php

4. Multilevel Java Card Grid: http://www.labri.fr/site/formation-doctorale/Sujets-2007/MultilevelJavaCardGrid/mljcg.htm

5. MANets definition: http://www.techterms.org/definition/manet

6. Bluetooth: http://www.dicodunet.com/definitions/reseaux/bluetooth.htm

7. WIFI: http://fr.wikipedia.org/wiki/Wi-Fi

8. USIM: http://en.wikipedia.org/wiki/USIM

9. S. Chaumette, K. Markantonakis, K. Mayes et D. Sauveron.: The Mobile Java Card Grid Project. e-Smart 2006. 20-22 septembre 2006, Nice, France.

10. P-F. Bonnefoi, P. Poulingeas et D. Sauveron. MADNESS: A Framework Proposal for Securing Work in Ad Hoc Networks. International Conference on Computer, Communication and Control Technologies: CCCT'05. 24 – 27 juillet 2005, Austin, Texas, USA.

11. D. Sauveron. La technologie Java Card : Présentation de la carte à puce. La Java Card. RR-1259-01, LaBRI, Université Bordeaux 1, 2001.

12. W.G. Sirett, Temporally Aware Behavior-Based Security in Smart Cards.Thesis, Royal Holloway University of London,septembre 2006.

13. E. Atallah, S. Chaumette, F. Darrigade, A. Karray et D. Sauveron. A Grid of Java Cards to Deal with Security Demanding Application Domains.

14. E. Atallah, S. Chaumette. A Smart Card Based Distributed Identity Management Infrastructure for Mobile Ad hoc Networks. WISTP 2007, Greece, may 2007.

15. D. Sauveron, K. Markantonakis, A. Bilas, J.-J. Quisquater. Information Theory and Practices. International Workshop, WISTP 2007

16. L. Buttyan, J.-P. Hubaux. Security and Cooperation in Wireless Networks: Thwarting Malicious and Selfish Behavior in the Age of Ubiquitous Computing. may 2007