Multilevel and Secure Services in a Fleet of Mobile Phones: The Multilevel Secured Messaging Application (MuSMA)*,**

Serge Chaumette and Jonathan Ouoba

LaBRI, University of Bordeaux, France
{serge.chaumette,jonathan.ouoba}@labri.fr

Abstract. The level of guarantees that can provide systems leveraging MANets cannot reach that of more traditional networks due to their highly dynamic nature. Real MANets (based on mobile phones in our case) operate in an environment without any infrastructure where the nodes are intermittently connected over short or long periods of time. Solving the traditional problems that are identification, security of communications, content delivery and localization, therefore requires specific approaches. In addition, the mobile phones that make the MANet, offer different communication technologies that must be efficiently exploited in multilevel perspective, from the shorter range wireless radio standards to the longer range ones. This multilevel perspective must also integrate issues related to user preferences, energy saving and limited financial means. In this paper, we first propose a preliminary model taking into account all the elements previously mentioned in the context of a mobile phone oriented MANet. Next, we focus on two aspects that are the secure exchange of profiles and the choice of the transmission technology. We then describe the mobile application that we have developed based on this model and the first performance analysis that we have conducted. Finally, we detail the remaining challenges that must be solved in this novel approach and that will constitute the next steps of the research described in this position paper.

Keywords: MANet, multilevel communication, mobile phone, security.

1 Introduction

A MANet (Mobile Ad hoc Network), as considered in this paper, is composed of a set of communicating devices which are able to spontaneously interconnect without any pre-existing infrastructure and that configures itself on the fly. The devices (or nodes) can move around, appear, disappear what thus leads to modifications of the network topology.

* This paper presents a Work-in-Progress.

** This work is partly supported by the Smart Urban Spaces European project.

D. Uhler, K. Mehta, and J.L. Wong (Eds.): MobiCase 2012, LNICST 110, pp. 169–185, 2013.

It is then difficult to ensure certain properties in terms of security and authentication. We must decrease, compared to more conventional (infrastructure-oriented) networks, the level of guarantees we expect from the applications running on top of these networks. This is described in [1] where it is stated that it is impossible, for example, to maintain a single (connected) overlay over a MANet (what is a key feature in usual approaches to create services on top of mobile networks). Let us for instance consider authentication. Assume that within a MANet, two nodes meet, share their identities and communicate. Without the help of an external infrastructure, it is complex to authenticate the identities that were exchanged. However, it would be realistic to think of a system that would allow the two nodes, if they meet several times, to recognize each other. In some sense, to design systems adapted to MANets, we must mimic the behavior of people in real life. For instance, to get back to the previous example, people can talk to other people they meet in a crowd, even if they are not sure of their respective identities, and later recognize each other.

Existing mobile devices and mobile phones in particular, are endowed with several types of wireless technologies that expand and diversify their communication skills. The combined use of these technologies, while offering a variety of possibilities in terms of services and applications, requires a thorough analysis regarding security and the choice of the communication mode to use based on a number of criteria to be defined (for example energy cost, financial cost or privacy).

There are some noteworthy issues in this context of (mobile phones based) multilevel MANets. For example, in the context of the Smart Urban Spaces (SUS) European project [2] the goal of which is to propose new e-services, we intend to deploy what we call a Multilevel Museum Quest. The principle of the quest is to allow participants to answer, using a mobile application, series of questions disseminated inside a given museum. Some questions of the quest will concern pieces of art located in remote museums. For each question, either the player knows the answer and can go further in the quest, or he does not know the answer and then contacts others players (that may be in its immediate neighborhood or not) whose profile can suggest they might be able to answer the question he is trying to solve. So, the service must offer a player the possibility of: (i)discovering on the fly appropriate participants; (ii)determining the best way to contact them (Bluetooth, Wi-Fi, GSM, etc.). This application illustrates two of the basic problems to be solved within multilevel MANets. The question is thus how to allow a set of mobile phones to communicate securely using the most appropriate technology depending on the context? In order to contribute to solve this problem, our goal is to define a multilevel platform taking into account the different technologies available on the terminals that will, for the purpose of illustration, allow the secure exchange of messages. We study the theoretical and practical elements to consider in the design of the platform, model these elements, offer a reference application (secure exchange of messages) and validate the relevance of the proposed solutions.

The rest of this paper is organized as follows. First, we present our definition of the platform to implement and the key concepts to focus on. Then, we describe the first reference application that we have developed and the initial analysis that has been performed to evaluate it in terms of security, efficiency and energy consumption. We eventually present the remaining issues to address to make the platform effective, the extensions we propose for the platform and the future research work we plan to achieve, and we finally conclude.

2 Multilevel Framework

2.1 Overall Description

We first describe how we model the framework. The platform consists of a set of nodes equipped with certain types of wireless technologies (short, medium and long range) that can directly exchange messages (in a peer-to-peer manner with no routing procedures - one hop -). Each node has a profile (this will be discussed later) that contains its personal data, and we assume that the nodes have limited resources in terms of energy and storage capacity (these are mobile electronic devices). Our goal is to develop a flexible system that ensures the security of communications and the management of the multilevel aspect (choice of the most suitable technology to exchange messages depending on the context) still conveniently handling the personal data of the nodes.

Figure 1 shows a way of representing the global architecture and below we refer to it to describe the different entities and processes that are involved.

First, there are *the nodes and the communication technologies*. Each node supports a set of communication technologies and this set varies depending on the node. For example, in figure 1, n_1 is equipped with $Technologies$ 1 and 2 while n_3 is equipped with $Technologies$ 2 and 3. It is to be noted that the technologies have specific attributes, from the costs (energetic and financial) of transmitting a message, to their range and their transmission rate. In order to enable interactions between entities, the profile of each node specifies the characteristics through which it wishes (or does not wish) to be found, known or recognized by others. For example, in the Multilevel Museum Quest application that we have presented in the introduction, a participant may state he is an expert in a particular field of painting and thus express his willingness to help other players. Second, we have *the process related to the search for communication partners*. The search operation is based on the public information contained in the profiles. According to its needs (the case of the call for help in the Museum Quest for example) a node can specify with precise criteria the target node(s) it wishes to reach. Thus, for an efficient operation of the system, each node must publish as much as possible (in a coordinated manner in its different neighborhoods so that the duplications are minimized) the information it wishes to provide the others with. Hence, a node searching for a particular resource can explore the profiles that are accessible to it and try to find a node (or a set of nodes) that meets its expectations. In addition, when two nodes physically meet, the system must provide them with a way to exchange (if they wish) initial information in an easy

and secure manner (see section 2.2). This information is intended to allow the two nodes to recognize each other if they meet again (physically or virtually) or are private data (direct connection procedures for instance) in order to simplify any future communications between them.

Third, when a specified peer has been identified, *the communication between partners* can take place. In figure 1, the dotted lines, within each technology bus, represent the possible communication links that can be tied between nodes. We call a set of nodes capable of communicating with each other, at a given time, by means of the same technology (short or medium range) an *islet* of the system. One of the issue is to retrieve the technologies that are available on a node and that it can use to exchange messages. This is achieved using the information available in the profile of the considered node and by initiating *ping* procedures. *The technology to use for sending a message* to the node can then be chosen according to the constraints of the system (minimize the different costs) and the preferences of the involved entities.

It should be noted that we want to support not only direct communication but also another mean of communication, called *gateway mode* that allows a node to communicate with other nodes located in different *islets*. Concretely we call a *gateway node* (or gateway for short) a special node that authorizes the others to use it as a bridge to get access to remote *islets*. In figure 1, n_1 makes use of g_1 to reach the nodes of islet B. In order to use a gateway, a node must first subscribe to it.

The model of the framework highlights two essential elements within the system: the search for communication partners which is completed thanks to the information contained in the profiles; the absence of explicit localization of the nodes.

We can more precisely model the platform, which is graphically represented in figure 2, as follows:

- N is the set of nodes (mobile terminals) of the system. N contains the nodes n_i with $i = 1 \dots m$.
- T is the set of all available wireless technologies in the system. T contains the technologies t_j with $j = 1 \dots u$. The functions $rate$, $costE$, $costF$ are defined over T_{n_i}: $rate_{n_i}(t_j, t)$ = transmission rate for technology t_j at a given time t for the node n_i, $costE_{n_i}(t_j)$ = energy cost for sending a message via technology t_j for the node n_i and $costF_{n_i}(t_j)$ = financial cost for sending a message via technology t_j for the node n_i. It is particularly important to take into account the notion of time for the transmission rate due to its fluctuating nature. The function adr is also defined over T as follows $adr_{n_i}(t_j)$ = connection address to communicate with n_i through the technology t_j for the different entities of the system[1].
- $V_{n_i,tj}$, at a given time t, is the set of neighbors of n_i via technology t_j.
- $I_{t_j}(t)$, at a given time t, is an islet of the system. Each node n_i of I_{t_j} can directly send a message to another node of the islet by means of technology t_j. More formally, if $n_i \in N,\ n_i \in I_{t_j}(t) \Leftrightarrow V_{n_i,t_j} = I_{t_j}(t) - \{n_i\}$.

[1] We assume that this value does not change with time.

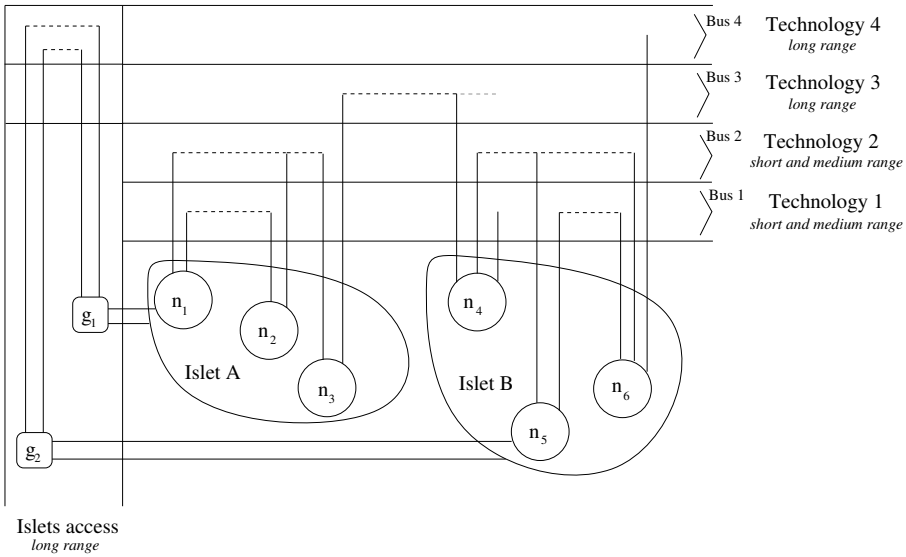

Fig. 1. Multilevel platform presentation

- G is the set of gateways, available in the system, allowing a node to communicate with remote islets (not directly accessible by using its embedded technologies). G contains gateways g_k with $k = 1 \dots b$.
- $n_i = (profile_{n_i}, techno_{n_i}, sub_{n_i}, pubKey_{n_i}, priKey_{n_i})$ with $profile_{n_i}$ the individual profile of the node, $techno_{n_i}$ the set of technologies it supports, sub_{n_i} the set of gateways (belonging to G) the node has subscribed to and $pubKey_{n_i}/priKey_{n_i}$ a RSA pair of public/private keys.
- we also define $kernel_{n_i}$ which are the minimal information to be exchanged (for node n_i) in case of physical meeting with another node.

  $kernel_{n_i} = (kernelprofile_{n_i}, adr_{n_i}(t_j), pubKey_{n_i})$ with $kernelprofile_{n_i}$ a subset of $profile_{n_i}$ and $adr_{n_i}(t_j)$ the connection information regarding the technology t_j (e.g. Bluetooth MAC address).

2.2 Concepts to Focus on

In this paper we will focus on two features of the platform. These are the elements that we were able, as of today, to test on a real application.

Secure Exchange of Minimal Information between Two Nodes. The goal of this process is to allow two nodes (n_i and n_j in the example), that physically meet and do not know each other, to securely exchange their kernel information (respectively $kernel_{n_i}$ and $kernel_{n_j}$). Figure 3 details the process that can be set up. The node (n_i) that initiates the action sends, through a dedicated channel, its public key and personal connection information (for a communication technology t_j it is equipped with, $adr_{n_i}(t_j)$ contained in $kernel_{n_i}$) to the

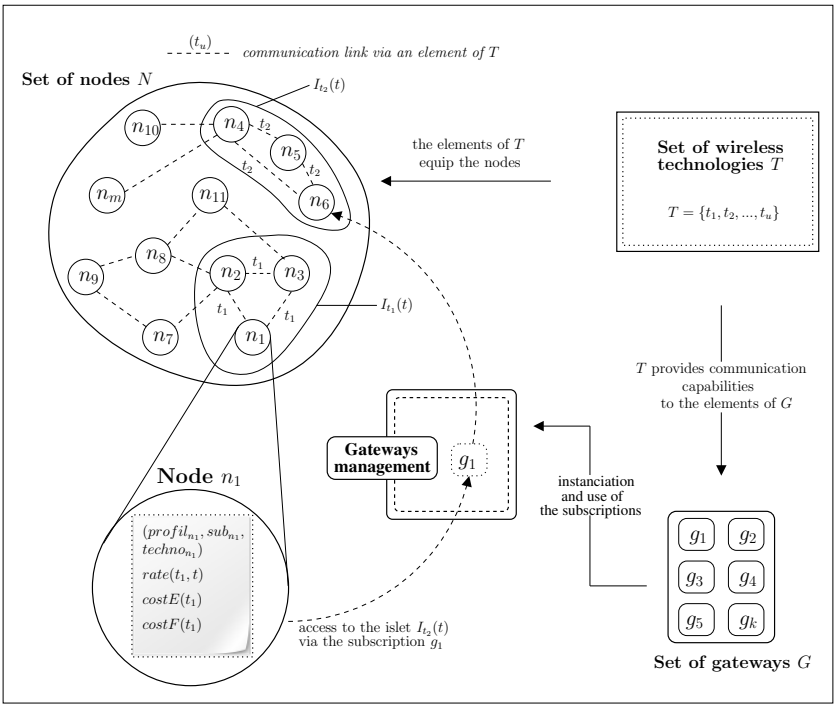

Fig. 2. Modeling of the platform

target node. The target node (n_j) transmits the information it wishes to share ($kernel_{n_j}$), ciphered with the public key included in the data that it just received, by using the personal connection information of the initiating node. In return, the initiating node sends the relevant information of its minimal profile ($kernelprofile_{n_i}$), ciphered with the public key of the recipient, through the same communication technology. The point to highlight is how the exchange process is initiated. The initial dedicated channel must enable a rapid and secure exchange of a limited amount of data while ensuring that the nodes are close to each other (in our prototype, it is achieved using Near Field Communication [3]). It is also important to note that due to the limitations of the dedicated channel (concerning the amount of data it can carry), it mainly serves to send the public key which will then help to secure the exchange of private information. Thus, apart from the dedicated channel, the protocol requires the use of another communication means. This is why the initiating node, in addition to its public key, sends its personal connection information for a communication technology, which communication technology must also be available on the second node. At the end of the exchange, n_i has received $kernel_{n_j}$ and n_j has received $kernel_{n_i}$. Following, the involved nodes will therefore be able to securely communicate with each other in order to share any kind of information, for instance information regarding their whole respective profiles.

It is worth mentioning that this exchange is not connected to the publication of profiles (that each node must perform) as described in section 2.1. Indeed, the publication of profiles was defined as a requirement for *the process related to the search for communication partners* to be effective. It is the dissemination of the profile of an entity to a set of nodes which can be contacted directly or through a gateway. In this case, the nodes do not physically meet and the published information is supposed to be public.

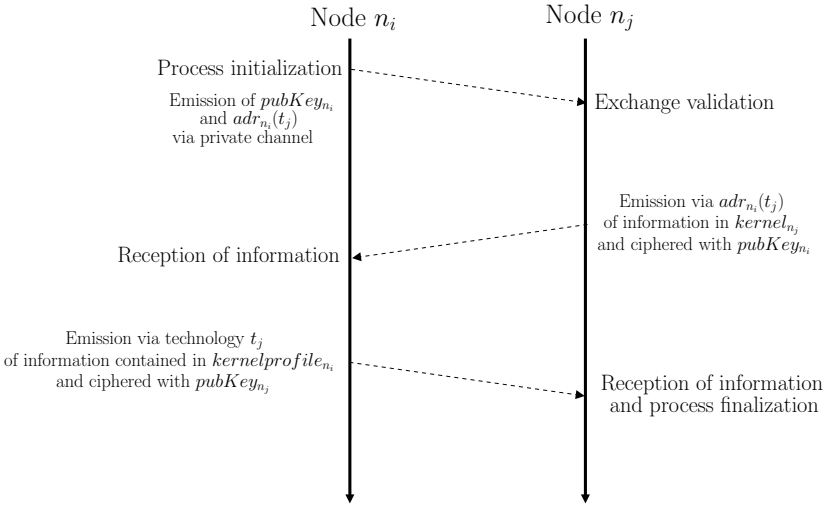

Fig. 3. Profile exchange process

Choice of the Transmission Technology. The problem to be solved at this level is: what technology t_j must be used by node n_i, at a given time t, to issue a message to another entity of the system so that the combination of $costE_{n_i}(t_j)$ and $costF_{n_i}(t_j)$ are minimal and $rate_{n_i}(t_j, t)$ maximal according to the different constraints? The constraints to take into account are those related to the profile of the considered sending node and the constraints of the entity to which the message must be sent. Indeed, a node can set in its profile some preferences in terms of energy and financial consumption or even have a limited number of technologies what impacts the way it sends or receives a message. Furthermore, the past activity of the system can also have an impact. It may be more appropriate to contact an entity of the system through technologies used in previous communications.

We thus need to compute the minimum of a cost function C (defined over T) with parameters representing the weighted factors to consider.

$C = \sum_{k=1}^{a}(w_k.cMin_k(t_i)) + \sum_{l=1}^{b}(\frac{w_l}{cMax_l(t_i)})$ with:

- $\sum_{k=1}^{a} w_k + \sum_{l=1}^{b} w_l = 1$ with w_k and w_l the weights of the factors
- $cMin_k(t_i)$ is a parameter to minimize (like $costE_{n_i}(t_j)$ and $costF_{n_i}(t_j)$) while $cMax_k(t_i)$ is a parameter to maximize (like $rate_{n_i}(t_j, t)$)

To compute $\min(C)$, we define three independent cost options: the *green option* where the node favors the situations with low energy consumption; the *cheap option* where the node minimizes as much as possible its financial costs; the *efficient option* when the transmission speed is essential. We could imagine, in the computation of $\min(C)$, that the weight 0.5 is assigned to $costE(t_j)$ if the node chooses the green option, to $costF(t_j)$ if the cheap option is selected and to $rate(t_j, t)$ in the case of the efficient option (for each option, the other parameters distribute the remaining weight (0.5) based on the different constraints).

Of course, a sending node must also be offered the possibility to arbitrary select the technology it wishes to use in order to send a message (thus bypassing the cost function based process) provided that the technologies in the corresponding entity are available.

2.3 Related Work

The multilevel platform model that we propose deals with many research issues that have often been explored but from different points of view. We have identified a few of them that are particularly relevant in the context of this paper.

Let us first consider the domain of network selection and cost functions where the goal is to be connected, depending on the context, to the most appropriate network in a seamless manner. In [4] and in [5] the authors present network selection strategies based on normalized utility functions that take into account parameters like bandwidth, power consumption and financial cost. Other network selection methods, with a policy specification model still based on cost functions, put more emphasis on specific issues such as the power-friendly aspect as in [6] or the user requirements as in [7]. Some authors also identify the handover decision (network selection) as a fuzzy MADM (Multiple Attribute Decision-Making) problem and propose a SAW (Simple Additive Weighting) based solution as in [8] and [9]. While taking into account the most essential elements, these solutions do not address the multilevel aspect of the platforms. Indeed, in our case, it comes to the special case of selecting the most appropriate intra-islet technology to enable peer-to-peer communication between two nodes, according to the constraints of the system. Our approach, by considering a multilevel architecture, is thus much more general.

Another noteworthy point is the concept of content-delivery in MANets. It is presented in various papers with a focus on a cooperative approach between nodes like in [10] or even with specific protocols for content-based communication as in [11]. These examples provide useful and relevant information for developing and deploying such networks. However, the multilevel aspect, that would consider the different technologies (from short/medium range to long range) available on a given node, is not handled. We claim that this is an important issue and we try to propose a solution for that.

Other approaches offer routing based solutions [12] [13] in the context of intermittently connected MANets based on collected mobility traces and estimations of the future behavior of the nodes of the network. Our approach with highly dynamic networks is to provide guarantees whatever the evolution of the network.

Simulation and traces thus do not help because they capture only one single execution path and cannot be used to prove results independently of the evolution of the network.

3 Reference Application: MuSMA

3.1 Architecture

The mobile application that we have implemented takes advantage of the availability of mobile devices (phones) equipped with at least four wireless technologies namely NFC, Bluetooth, Wi-Fi and GSM.

NFC [14], which stands for Near Field Communication, is a communication technology that has a range of about 10 centimeters. Indeed, because of its very short range, which requires entities wishing to communicate to be physically close to each other (which provides security guarantees), it offers an adapted way of starting the kernel information sharing process (see section 2.2).

Bluetooth, Wi-Fi and GSM are the elements of T among which a choice is performed to transmit a message. It is to be noted that when we mention the GSM technology it comes to sending messages via SMS (Short Message Service) and for Wi-Fi it is the direct mode [15], which enables direct peer-to-peer communications, that we consider.

Figure 4 shows the components of the application. The user interaction takes place through the GUI (Graphical User Interface) that lets the user enter the messages to send, view the received messages as well as the different profiles. The Personal Profile stores the private data of the user and its contacts. A key point lies in protecting the application with a password (selected by the user upon first use) which limits the access to sensitive information like the private key which is itself ciphered thanks to the above password. Then, there is the Technology Selection module which is responsible for selecting the most appropriate technology according to the cost evaluation strategy (section 2.2). It is also responsible for notifying the user of the technologies that are available to communicate with a given contact. It is accomplished by using the connection information (Bluetooth, Wi-Fi, GSM) contained in the profile of each contact; it helps to periodically perform ping requests, for each type of technology and for each contact, to collect the related connectivity status. The Exchange Protocol implements the protocol defined in subsection 2.2 so that the user can easily add a new contact. Finally, the Communication Management module interacts with the different available wireless technology layers to send and receive data.

3.2 Prototype Implementation

Our system requires the use of mobile phones that support NFC and more precisely its peer-to-peer mode (for direct communication between the phones) and the Wi-Fi direct standard. The phones must also be able to send messages via Bluetooth and GSM (SMS). The Android platform which is one of the most

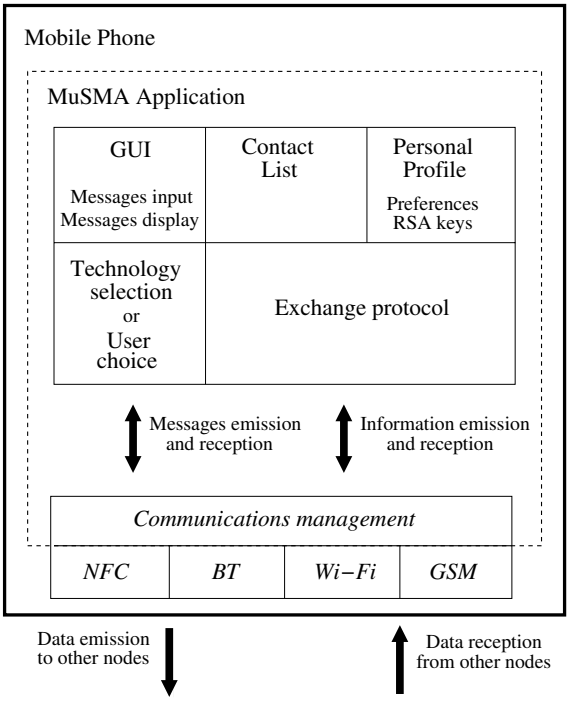

Fig. 4. MuSMA application architecture

dynamic at the moment, offers, in cooperation with the manufacturers, some phones that correspond to the required specifications. Therefore, we decided to target this platform which also has the APIs (in its 4.0.4 version) and provides a (limited and uni-directional) support for NFC peer-to-peer and Wi-Fi direct modes. Then, a first prototype has been developed to analyze and validate some aspects of the architecture proposed for MuSMA. The mobile used for this development is the Galaxy Nexus. A simple usage scenario of the application is described figure 5. In addition, figure 6 presents a screenshot of the current prototype where a user is willing to send a message to one of its contacts.

4 First Analysis of the Solution

The goal is to provide a first evaluation of the mobile application that we have developed. This first analysis must show the applicability of the multilevel framework (at least some aspects) to a real world mobile application in terms of efficiency and energy consumption while the application should ensure that the security requirements are guaranteed. It should be noted that usability is a key element in any mobile application. However, it is not considered in our analysis due to the fact that the user interface is based on the Android built-in SMS

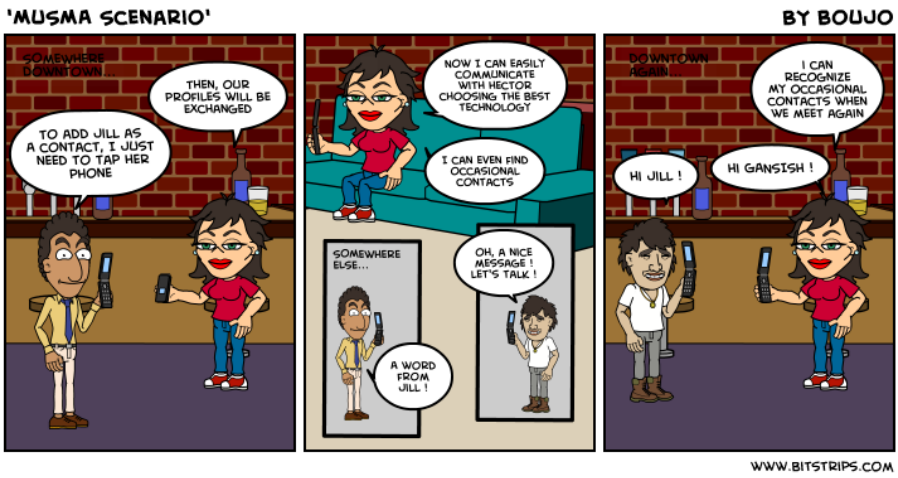

Fig. 5. Scenario for the tests

messaging application. Then, in our opinion it is not necessary to focus on this concept, at least for now.

4.1 Security

The security of the system, once the kernel information has been exchanged, relies on public/private keys based protocols where the confidentiality of the exchanges between the nodes are ensured (the authentication and integrity aspects are not considered for now). Of course, these procedures are dependent upon (i): the secrecy of the private key, but they also rely on (ii): the properties of the communication technologies that we use. Thus, we will focus on these two points.

As each instance of the application (with its user) acts as a node of the system, it is provided with a pair of RSA keys. The public key is provided to the external contacts while the private key is used to decipher incoming messages issued by known entities. The secrecy of the private key is entrusted by the fact that the access to the mobile application is protected by a password. Upon first use, the legitimate user chooses a password to proceed to a symmetric ciphering (with the AES protocol in our case) of the private key that is then stored in the mobile phone. Then, when launching the application, the user is prompted to enter a password which is used to decipher the private key. A random number is generated, ciphered with the public key (which is also stored in the phone) and deciphered with the private key resulting from the entered password. This results in another number. If the two numbers match, the access to all the functionalities of the application is granted. Hence, the secrecy of the private key is built on top of the strength of the underlying symmetric algorithm. However, when the application is running the private key is loaded to the memory of the phone to decipher incoming messages. It can cause security holes because the mobile phone is not considered a trusted device

Fig. 6. Screenshot of the prototype application

(malicious programs can corrupt it). We must consider a stronger solution where the private key would be stored in a secure element [16] ((U)SIM card, microSD smart card, etc.) that will perform the ciphering and deciphering operations. We have not tested the improved solution yet.

Concerning the kernel information exchange presented in 2.2, it is essentially the NFC technology which is concerned. Since our approach makes use of the NFC peer-to-peer mode, we must consider its threat model. There are attack scenarios such as eavesdropping, man-in-the-middle, and relay [14] [3]. All of them are not to really significant in our context. For example, the man-in-the-middle attack is difficult to set up in a real NFC-based environment [3] as well as the relay threat [17]. This is due to the nature (very low range) of the NFC technology that requires both transacting parties to be physically located next to each other. Thus, the main concern lies in the eavesdropping threat. An attacker could eavesdrop [18] and record the data of the transactions, namely the public key and the personal data of a node. The consequences of this attack are limited because either very few personal data or data intended to be public are transmitted through this channel. However, this issue could be solved by using the SNEP protocol [19] (which is unfortunately not yet implemented on the phones we have) to establish bi-directional NFC peer-to-peer connections in the initialization of the exchanges.

Even if the system can be enhanced, it nevertheless reaches a reasonable security threshold for our messaging application.

4.2 Energy

We wish to verify that the additional energy consumption induced by the use of the application is not too high. We have performed some tests to evaluate this consumption overhead. To do so, we have defined a specific usage profile of the application that is based on realistic statistics. Indeed, based on the average number of SMS sent [20] per month in Europe in 2011 (whereby in some countries users can issue up to 20 SMS per day), we assumed that a user could send 60 messages (20 via Bluetooth, 20 via Wi-Fi and 20 via GSM) per day using our application by taking into account the three available technologies. In a concrete way, we fully charged the battery of some phones that we used in a conventional manner recording the energy consumption. We repeated the same procedure under the same conditions and with the same phones but in addition running our mobile application (according to the previously defined usage profile). Figure 7 presents the results that we obtained with 3 phones. The overhead seems

	% Battery used	% Battery used with MuSMA	Overhead
Mobile 1	24	28	16.6%
Mobile 2	26	31	19.2%
Mobile 3	34	40	17.6%

Fig. 7. Energy consumption overhead for issuing the 60 messages

significant and it can be explained by the fact that the Bluetooth, the Wi-Fi direct and the GSM technologies must be permanently activated. Nevertheless, it must be put in perspective relatively to the consumption of other applications, for example the android OS built-in browser drains 0.35% of the battery for a 30s run [21].

5 Other Issues Regarding the Platform

Obviously, the next step in our work will be to go deeper in the modeling of the platform we are building. To do this, it will be necessary to detail in a systematic way the issues regarding the publication of profiles within the system as well as the discovery of the nodes and their recognition. It will also be fundamental to ensure a better selection of the technology to communicate with based on more criteria (the past activity for instance). This must be done bearing in mind that the proposed solutions must be tailored to fit the context of mobile phone oriented MANets. Indeed, in the context of MANets, the most critical issue is not to ensure that two nodes can always find a route to communicate with each other. The dynamic and mobile nature of the nodes makes it difficult

to implement such protocols in realistic applications. It is rather to ensure that, depending on the context, the possibilities of communication offered to each node of the system are optimal.

Concerning the publication of profiles, it is related to the process which manages *the search for communication partners*. As we already mentioned, each node of the system must publish as much as possible the information (about its profile) it wishes to provide the other with. The traditional approach which consists in flooding the system (each node that receives the information transmits them to all its neighbors) should be avoided because it is assumed that the nodes have limited resources in terms of energy and storage capacity (and broadcast storms should also be avoided). Each node must then send the profile to its neighborhood while paying attention not to send it several times to the same recipient (at least on the part of the network where the radio broadcast is not the underlying implementation). This must be done by keeping track of the nodes which received the considered profile. Each node must also make use of relay nodes available in its neighborhood and that are equipped with longer range technologies to reach inaccessible areas for the transmission of its profile.

The specification of the targets is also related to *the search for communication partners*. Indeed, this process allows to define a set of nodes that are targeted for a particular operation. This specification is based on a description of characteristics that must be common to all the targeted nodes. Concretely, the selection of a set of targets is carried out by means of an exploration request whose main argument is the characteristics sought among all the accessible nodes. The specification may involve one or more nodes. For example, if an entity wishes to try to get in touch with a node whose pseudonym it knows, it must initiate a exploration request with the pseudonym as an argument. This request causes the system to search, among the profiles that the requesting node can access, those containing the relevant characteristic. Depending on the process used for publishing profiles, we could for instance state that the accessible nodes to an entity that initiates an exploration request are the ones it received, the ones of its neighbors or those which are reachable through a relay node. This has to be explored further.

On the topic of improving the method for selecting the transmission technology, it mainly concerns *the technology to use for sending a message*. The selection method is based on the minimum of a cost function as presented in 2.2. It is therefore a question, for a given node n_i, of defining the appropriate strategy for computing the weights and the values for the parameters (such as $costE_{n_i}(t_j)$ and $costF_{n_i}(t_j)$) of the cost function while considering the factors that influence the constraints and their sets of definition. The factors to consider include the following: the technological preferences, the priorities in terms of cost and transmission rate, the profile of the sending node and the profile of the recipient.

We summarize figure 8 the operations within the system that are concerned with the presented perspectives. In the example, the node n_1 sends its profile and an exploration request to its neighbors. The neighbors are divided into three categories which are not disjoint: the group of neighbors accessible via the

communication technology t_1, the group of neighbors accessible via the communication technology t_2 and the group of neighbors accessible via the communication technology t_3. The relay nodes n_9 and n_{10} that are equipped with longer range communication technologies are used to transfer the messages to the entities to which n_1 has no direct access. This scenario puts forward the elements to consider in order to enhance the modeling of the platform. We will then incorporate all the improvements of our model in the mobile application that we develop. In order to get more valuable results in the analysis of our system, we plan to test our application on field and on a larger scale which may be considered through the deployment of the museum quest application (presented in the introduction) in some European cities (members of the SUS project). Another notable point is the fine grained energy profiling of our mobile application that must be performed to enhance its efficiency.

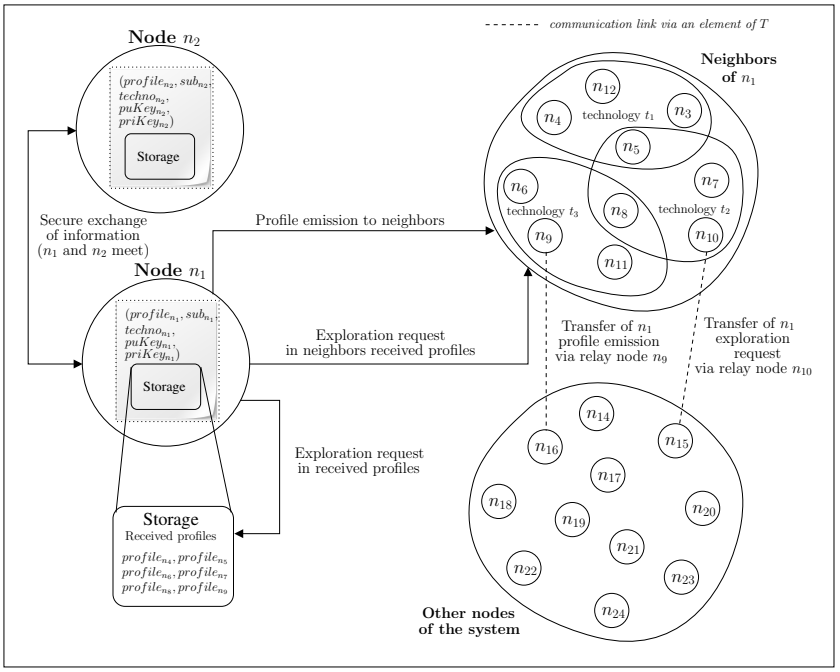

Fig. 8. Overview of operations within the platform

6 Conclusion

In this paper, we have presented our initial work on a model to support multilevel secure communications within mobile phones oriented MANets. The multilevel aspect, leveraging the technological capabilities of mobile phones, leads to the exchange of messages in peer-to-peer manner with the selection of proper communication means according to the profile and the availability of the considered

entities. This model, with its focus put on the search for communication partners via the profiles and the non-explicit localization of nodes, attempts to provide a more realistic approach of the highly dynamic nature of MANets. We have also presented and briefly analyzed (in terms of security and energy) the first mobile application that we have developed based on the model. The MuSMA application has made it possible to validate the feasibility of certain elements of the model including the secure exchange of minimal information and the choice of the transmission technology.

These initial results encourage us to pursue the definition, the improvement and the extension of our model while considering to use it with concrete cases such as the Multilevel Museum Quest application in the framework of the SUS European project. In addition, the description that we proposed concerning the remaining issues to solve (namely the publication of profiles, the specification of the targets and the improved method for selecting the transmission technology) draws clear directions for future work.

Acknowledgment. The work presented is this paper is carried out within the framework of Smart Urban Spaces, an ITEA2 [22] European project, the goal of which is to define new e-services for cities. The proposed services mainly take advantage of specific technologies, in particular NFC, in order to ease the everyday life of European citizens. Several use cases are concerned, for instance daycare organization, transportation or cultural events attendance. We would like to thank all the partners of the project with whom we have been working.

References

1. Chaumette, S.: Can highly dynamic mobile ad hoc networks and distributed MEMS share algorithmic foundations? In: Proceedings of the 2nd Workshop on Design, Control and Software Implementation for Distributed MEMS, Besancon, France (2012)
2. Smart urban spaces website (September 2010), `http://www.smarturbanspaces.org`
3. Haselsteiner, E., Breitfuss, K.: Security in Near Field Communications (NFC). In: Proceedings of the Workshop on RFID Security (2006)
4. Wang, H.J.: Policy-enabled handoffs across heterogeneous wireless networks. In: Mobile Computing Systems and Applications, WMCSA, pp. 51–60 (1999)
5. Serrador, A., Correia, L.M.: Policies for a cost function for heterogeneous networks performance evaluation. In: Proceedings of the 18th Annual IEEE International Symp. on Personal, Indoor and Mobile Radio Commun., Athens, Greece (2007)
6. Trestian, R., Ormond, O., Muntean, G.-M.: Power-friendly access network selection strategy for heterogeneous wireless multimedia networks. In: 2010 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting BMSB, pp. 1–5 (2010)
7. Shen, W., Zeng, Q.-A.: Cost-function-based network selection strategy in integrated wireless and mobile networks. In: Proceedings of the 21st International Conference on Advanced Information Networking and Applications Workshops, Washington, DC, vol. 02, pp. 314–319 (2007)

8. Zhang, W.: Handover decision using fuzzy MADM in heterogeneous networks. In: 2004 IEEE Wireless Communications and Networking Conference IEEE Cat No04TH8733, pp. 653–658 (2004)
9. Bari, F., Leung, V.C.M.: Automated network selection in a heterogeneous wireless network environment. IEEE Network, 34–40 (2007)
10. Ma, Y., Jamalipour, A.: A cooperative cache-based content delivery framework for intermittently connected mobile ad hoc networks. Trans. Wireless. Comm., 366–373 (2010)
11. Haillot, J., Guidec, F.: A protocol for content-based communication in disconnected mobile ad hoc networks. Mob. Inf. Syst., 123–154 (2010)
12. Lindgren, A., Doria, A., Schelén, O.: Probabilistic routing in intermittently connected networks. SIGMOBILE Mob. Comput. Commun. Rev., 19–20 (2003)
13. Spyropoulos, T., Psounis, K., Raghavendra, C.S.: Efficient routing in intermittently connected mobile networks: the multiple-copy case. IEEE/ACM Trans. Netw., 77–90 (2008)
14. Madlmayr, G., Langer, J., Kantner, C., Scharinger, J.: NFC devices: Security and privacy. In: Proceedings of ARES (2008)
15. Alliance, W.: Wi-Fi certified Wi-Fi direct: Personal, portable Wi-Fi technology. WIFI Alliance. Tech. Rep. (October 2010)
16. Reveilhac, M., Pasquet, M.: Promising secure element alternatives for NFC technology. In: 1st International Workshop on NFC, Hagenberg, Austria (2009)
17. Francis, L., Hancke, G., Mayes, K., Markantonakis, K.: Practical NFC Peer-to-Peer Relay Attack Using Mobile Phones. In: Ors Yalcin, S.B. (ed.) RFIDSec 2010. LNCS, vol. 6370, pp. 35–49. Springer, Heidelberg (2010)
18. Hancke, G.P.: Practical eavesdropping and skimming attacks on high-frequency RFID tokens. Journal of Computer Security 19(2), 259–288 (2011)
19. N. Forum, Simple NDEF exchange protocol - SNEP 1.0, NFC Forum, Tech. Rep. (2011)
20. GSMA, A. Kearney, and W. Intelligence, "European mobile industry observatory", GSM Association, Tech. Rep. (2011)
21. Pathak, A., Hu, Y.C., Zhang, M.: Where is the energy spent inside my app?: fine grained energy accounting on smartphones with eprof. In: Proceedings of the 7th ACM European Conference on Computer Systems, pp. 29–42. ACM, New York (2012)
22. Itea2 website (September 2010), `http://www.itea2.org/`