Mobile AD hoc Network
with
Embedded Secure System

Ève Atallah[1], Céline Burgod[1], Pierre-François Bonnefoi, Damien Sauveron

XLIM, UMR 6172
CNRS – Université de Limoges
123, avenue Albert Thomas
87060 Limoges CEDEX FRANCE

eve.atallah@labri.fr, burgod@msi.unilim.fr
bonnefoi@unilim.fr, damien.sauveron@unilim.fr

ABSTRACT: *Nowadays, the adoption of ad hoc networks is growing very quickly, but their approval in a working context requires improved security. Indeed wireless connectivity and mobility are the source of the main security issues. The aim of our work is to design a secure collaborative architecture for ad hoc networks using smart cards in order to support new applications enabled by these networks. The goals of this short paper are to introduce the important definitions which characterize the context of our work and some key concepts that we would like to develop in our framework.*

***KEYWORDS**: Smart Card, Wireless Ad Hoc Network, Secure Communication, Collaborative Systems.*

1 Introduction

By definition, a Mobile Ad hoc Network (MANet) is a network created in a spontaneous manner and composed of autonomous and mobile elements (laptop, PDA, smartphone, UMPC, tablet PC, etc.). It is not supported by a *preset infrastructure* and all its elements share a *common goal*. To enable this spontaneousness and this mobility, these elements generally use wireless communications (Bluetooth, WiFi, etc.) and operate on battery.

1.1 No preset infrastructure

An important characteristic of the mobile ad hoc networks is the total absence of infrastructure and the communication between the nodes are supported through their wireless connectivities. For example, as illustrated in Figure 1, when an application (1) on the node A sends a message to an application (3) on the node C, the message is routed by the node B to C, since C is outside of the A's radio coverage, and is, thus, not reacheable.

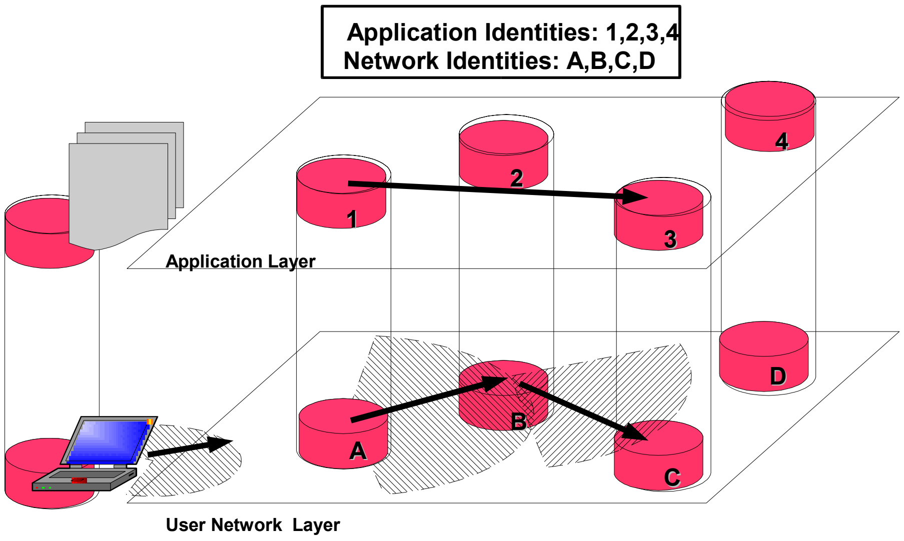

Figure 1: Communication in a Mobile Ad hoc Network

[1] Co-supervised by Prof. Serge Chaumette at the LaBRI (UMR 5800, CNRS – University Bordeaux 1, France) and by Dr. Pierre-François Bonnefoi at XLIM.

This work is supported by the French Agence Nationale de la Recherche under contract ANR-05-SSIA-0002-01.

By definition, the infrastructure is used as support for the activity in the network: it makes possible the exchanges (definition of interconnection paths) *and set up mechanisms ensuring the security*. In the traditional "wired" networks, the infrastructure is made up by a physical part (hardware – links and interconnection boxes) and it can be supplemented by a logical part (software – like VLAN, VPN, PKI, DHCP server, etc.). Some of these logical means represent a centralization compared to the network: all the elements of the network must be able to frequently join certain servers (for example, to the Certification Authority in the use of PKI).

However this approach is essentially contrary to the nature of the mobile ad hoc networks and nevertheless mechanisms must be set up to ensure their security as we will describe section 1.4.

1.2 A common goal

In general, the ad hoc networks have a goal shared by the elements which compose it: this common goal consists in enabling the data exchanges and the resources sharing between these elements of different nature and capacity. This sharing is carried out according to roles given to each element which makes it possible to organize the access and the use of a resource (for example it is possible to identify which node acts as a server and as a client as well as which node is granted to use it). This goal is organized by an administration which makes it possible to translate the human intention of the users (i.e. the security policy like the definition of the border of the network and the access rules to the resources).

1.3 Lifecycle of mobile ad hoc network

In a general manner, a network has a cycle of life. Before its existence, it is planned, i.e. administration and infrastructure are defined by taking into account the goal of the network and the functional needs. This planning can be the result of a negotiation between all the users or entrusted to a restricted number of privileged users (in this latter case, a centralization is implicitly needed). Then, during the lifespan of the network, the administration can be dynamic or not (evolution of the security policy, by addition or withdrawal of elements, or by the reconfiguration of the resources sharing). Note that it is also possible to start again a planning phase to create a new instance of the network provided with a new way of administration while integrating certain number of elements of the old network.

In the case of an ad hoc network, the infrastructure and the administration must be supported by the elements themselves. Consequently the definition and the application of the security policy depend on each element and the administration is distributed by nature. In the same way, the mobility of the elements makes extremely dynamic the infrastructure: the topology of the network changes quickly and in a random way (appearance/disappearance of nodes present or not at the starting of the network, modification of the communication links). Under these conditions, any approaches of centralization must be prohibited since the access to a group of selected elements may not be guaranteed during the lifespan of the network (for example the group hosting an authentification server). The administration uses the management of the identities in order to define the border of the network and to regulate the resources sharing. These operations must be in conformity with the security policy to which the users belonging to the network must adhere and conform. That also imposes that each element of the network is equipped with its own or a shared identity.

The infrastructure must enable the communication between all the elements belonging to the network, i.e. to enable the establishment of paths for the transfer of the messages between the elements. These paths cross the elements because they are the only ones being able to forward a message between two elements when they cannot communicate directly since they are outside of the radio coverage (requiring routing algorithm).

1.4 Security policy

The security policy must guarantee security fundamentals: authentication, integrity, confidentiality, non-repudiation and availability. The nature of the mobile ad hoc network implies new risks in particular related to elements of the network themselves since they provide the infrastructure, and new undesirable behaviors are highlighted: selfish behavior in addition to the malevolent behaviour. Some facts must be taken into account for the mobile ad hoc networks:

- the element itself provides its identity(ies). Consequently it is difficult to guarantee uniqueness and to prevent the impersonation of an element by another one;

- each element provides the support of the network, in particular it runs itself the needed algorithms. Thus the element is able to modify these algorithms;
- the element, mobile by nature, operates on battery what limits its autonomy and makes it less voluntary to ensure the support of the network: power consumption to the profit of the others and not for itself. This implies a new improper behavior: selfishness;
- the power saving functions as well as the mobility of the elements induce the appearance and the disappearance of the elements. Thus it is necessary to be able to distinguish its normal behavior from a selfish behavior.

To overcome the problem of a node that refuses to route the messages in order to save its battery or because it is malicious, we would like to contractualize node behaviours to support the network requirements, like routing, and to ensure some other fundamental properties to guarantee the security of mobile ad hoc network, i.e. the security of the identities and that of the routing algorithm.

1.5 Our context

Precisely the context of our work is:

- the planning phase which makes it possible to define the security policy before the starting of the network, specially the identities distribution is against the spontaneous nature of the network. Thus we will choose the case of a non-planned ad hoc network.
- the security policy can be dynamic or not, e.g. it can evolve during the lifespan of the network through the dynamicity of the border: additions of new unknown elements at starting and withdrawals of known elements (i.e. management of the identities), reorganization of the groups, regrouping of elements, etc. Thus we will support dynamic behaviour.
- the elements must be able to establish secure communication channels in the network according to their identity (such group can want to communicate with another in such a way that these two groups are the only ones being able to have access to the contents of the messages). Thus we will provide secure communication channels.
- the communication links being wireless, it is impossible to restrict the access or listening with a list of authorized elements (e.g. it is always possible to use amplified antennas to exceed the limits imposed by the nature of the obstacles in the environment of the element and to be able to collect the transmissions). Thus we will rely on a secure processing environment and ciphered exchanges.

2 Framework Overview and Key Concepts

In our platform, one requirement to secure the routing is to embed an environment for secure processing (*i.e.* a smart card) on each node to build a secure network between the different smart cards. Given this *control network*, we can distribute strong identities at several levels (for the nodes of the network and for the applications) and secure routing. In certain aspects this control network is similar to an application distributed on the Java Card Grid [1,2,3,4] developed at the LaBRI. We also proposed mechanisms to enforce the confidentiality and the privacy at the user network and application levels by ciphering the messages thanks to the smart cards capabilities. The messages that are exchanged between nodes are always ciphered and are only deciphered when the proper cipher key is provided by the control network smart cards, acknowledging that the user has been granted access to the message (full message content on the destination node or message header on intermediate node). To address the keys distribution problems between the smart cards, we have defined a solution based on an evolutive distributed mutual agreement that the person wishing to be part of the network must accept. This charter is a new sort of certificate, that can be viewed as an *active certificate* since it contains some sort of protected code that can be executed only on the smart cards to audit them, *i.e.* the participant identity (or other predefined criteria). The smart cards act as trusted third parties according that they run strictly the same applet for managing charter, grants, authentication process, etc., and provide the secure environment needed to protect the critical algorithms supporting the network.

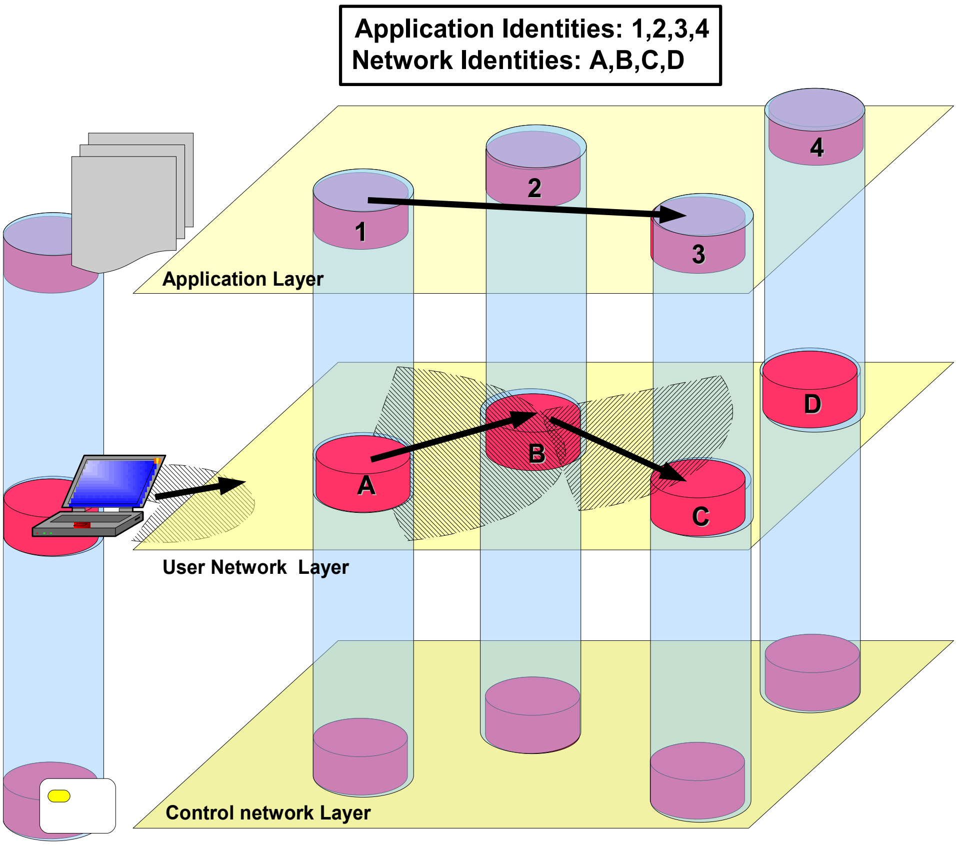

Figure 2: Overview of the MADNESS platform

In this framework[2], the key security elements are the smart cards that are trusted because of the security evaluation and certification process they are subjected to. In the real platform, the smart cards used are Java Cards for their multiapplication and dynamic loading features. However the proposed framework will take more advantage of the evolutions planned for the Java Card 3.0 specifications (TCP/IP, multithread, etc.).

3 Applications

With this platform, a straightfoward and fundamental service is the possibility to communicate securely. However this obvious feature is often not available in the main related work about the ad hoc network or is supported by a centralized PKI which is a negation of ad hoc nature of the network. A more advanced application that we wish to support takes advantage of the platform by addressing the complex problem of doing a collaborative task in an ad hoc network [5].

4 Conclusion

In this paper we have defined the context for which we develop our framework and we have presented the key concepts that we would like to implement in MADNESS.
We are convinced that in the context of the ad hoc network, the use of Java Cards in conjunction with the notion of *active certificate* will enable a high level of security to be provided but also the capability to have real applications in the new future.

References

[1] E. Atallah, S. Chaumette, F. Darrigade, A. Karray and D. Sauveron. *A Grid of Java Cards to Deal with Security Demanding Application Domains.* e-Smart 2005, 21-23 septembre, Nice, France. ***e-Smart 2005 Isabelle Attali Award for the best innovative technology***

[2] A part of this framework is currently developed in the « SARAH » project funded by the french ANR (National Agency for the Research).

[2] S. Chaumette and D. Sauveron. *A High Level Security Framework for the Grid: the Java Card Grid Testbed.* The 2006 High Performance Computing & Simulation (HPC&S) Conference. 28-31 May 2006, Bonn, Germany

[3] S. Chaumette, A. Karray and D. Sauveron. *The Software Infrastructure of a Java Card Based Security Platform for Distributed Applications.* 8th International Conference on Enterprise Information Systems (ICEIS 2006), 4th International Workshop on Security In Information Systems: WOSIS 2006. 23-24 May 2006, Paphos, Cyprus

[4] S. Chaumette, A. Karray and D. Sauveron. *Secure Collaborative and Distributed Services in the Java Card Grid Platform.* The 2006 International Symposium on Collaborative Technologies and Systems (CTS 2006), Workshop on Collaboration and Security (COLSEC'06). 14-17 mai 2006, Las Vegas, Nevada, USA

[5] P-F. Bonnefoi, P. Poulingeas and 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, TX, USA