SAACCESS : secured ad hoc access framework

Hakima Chaouchi, Maryline Laurent

SAACCESS: Secured Ad hoc ACCess framework[1]

H. Chaouchi, M. Laurent-Maknavicius

CNRS Samovar UMR 5157, GET/INT/LOR, 9 rue Charles Fourier, 91011 Evry, France

Abstract— Ad hoc technology being developed for over a decade now has not yet succeeded to get into the telecommunication service value chain. This is due mainly to, the lack of network control, quality of service and security support. From a service provider's point of view, to use the ad hoc technology in the value chain, an efficient AAA framework is mandatory. This is not easy because of the self organising aspect of the ad hoc network. This paper presents a brief overview of security issues in ad hoc networks and introduces a new AAA approach in an ad hoc network in order to allow secure exchange of services, thus being chargeable. It is mainly based on decomposing the AAA service which is classically centralized, into three sub-services and distributing them securely in the ad hoc network. This will allow the ad hoc technology to securely extend the access network coverage and introduce new services exchange within the ad hoc network.

1 Introduction

Ahoc network is a multi-hop network that is created by the mobile nodes when needed for their own communication purposes [1]. Typically this could mean that two hosts want to exchange some data. In an ad hoc network, mobile nodes come and go as they wish, so the topology of the network is changing quite rapidly. This creates new challenges for the proto-

[1] H. Chaouchi, M. Laurent-Maknavicius, " SAACCESS: Secured Ad hoc ACCess framework ", article invité, International Conference on New Technologies, Mobility and Security NTMS'07, Paris, April-May 2007.

cols to be used in ad hoc networks. Most of the traditional protocols don't fit very well into ad hoc networks. An ad hoc network is quite a new concept, so there isn't any approved protocol yet, for example, for routing purposes.

An ad hoc network can be created in a number of ways. One solution is to run routing protocols in the mobile nodes. This approach requires careful attention, because the rate of change in an ad hoc network is quite rapid compared to the Internet, to which most of the current routing protocols are designed. Another approach would be to treat the ad hoc network as an incompletely connected physical medium [1].

In the context of Always On era, ad hoc technologies integration with the infrastructure is without any doubt, the inevitable approach for extending at low cost the network access coverage. However a real and business oriented service deployment over ad hoc network requires firstly security of the communications and resource accounting. The lack of security and accounting mechanisms is the major issue that slows down the deployment of ubiquitous services. We believe that the integration of ad hoc and infrastructure-based technologies coupled with efficient security and accounting techniques is the answer for the urgent demand of network operators for appropriate architectures to host secure and large scale ubiquitous services.

There are several threats in ad hoc networks. First, those related to wireless data transmission such as eavesdropping, message replaying, message distortion and active impersonation. Second, those related to ad hoc construction of the network. This means that attacks can come also from inside the ad hoc network. Therefore we cannot trust one centralized node, because if this node would be compromised the whole network would be useless. Another problem is scalability. Ad hoc networks can have hundreds or even thousands of mobile nodes. This introduces important challenges to security mechanisms [2].

As most of the security issues in ad hoc networks are caused by trust less nodes, the authentication process is a strong solution to eliminate those misbehaving nodes. Nevertheless, ensuring authentication service in a self organized network is not easy to realize. We propose in this work to build a secured ad hoc infrastructure framework where the AAA service which is classically centralized in the infrastructure network is decomposed into three sub-services and partly executed by the infrastructure network. The Authentication service (Aaa), the Authorization and Accounting services (aAA). These services will be securely distributed in the servicing ad hoc nodes. For this purpose, a trust management framework is necessary.

One obvious and original consequence of the secured framework would be the integration of ad hoc technology in the service value chain by the in-

troduction of a new service provider entrant (ad hoc network service provider), and a new network access provider (ad hoc network). The classical operator then will make profit by offering in addition to his classical services (access to Internet), new services for ad hoc nodes. For instance, it will act as a third party between the servicing ad hoc nodes, and the customers (local ad hoc nodes). This will be to guarantee the AAA service and a secured transaction for exchanged services (peer-to-peer, packet forwarding, resource consumption…).

2 Security Issues and Challenges in Ad Hoc Networks

Ongoing research in ad hoc network security is mainly addressed in a pure ad hoc context and covers secure routing, key establishment, trust management, authentication and certification/revocation services. Assuring trustiness in ad hoc networks is a challenging issue due to the absence of communication infrastructures, and a fortiori third trust parties. Indeed, the infrastructure-less nature of ad hoc networks makes it difficult to adopt centralised or hierarchical trust models such as Public Key Infrastructures (PKI) [3]. Nevertheless, most of existing security paradigms for ad hoc networks assume the existence of public/private key pairs, and hence the existence of a key management infrastructure. For instance, secure routing protocols which are an essential security component for detecting and eliminating malicious nodes disrupting the network. That includes solutions such as ARAN [4], Ariadne [5], SAODV [6], and all of them are based on this very constrained prerequisite that nodes are configured with appropriate pre-shared key or public/private keys to support origin authentication.

As such, a number of works were conducted towards adapting certification and revocation services to ad hoc networks, and most of them identified the threshold cryptography [7, 8] as a possible solution where k-out-of-n nodes collaboratively provide a certification service for other nodes in the network. The revocation service is operated when a minimum number of k nodes are accusing a node of misbehaving, and sometimes the action is balanced with the reputation of each accusing node.

Therefore, the threshold cryptography is adapted to ad hoc networks to establish keys that may be used next to secure the routing, authenticate nodes and exchange encrypted data. Another solution is the ID-based cryptography [9] where the node's identifier is part of its public key, so a public key is naturally bound to the node. Another solution [10] considers both

cryptographies, the threshold one to initialize a private-key generation server for ID-based cryptography support.

3 AAA In Ad Hoc Networks

Typically Authentication, Authorization, and Accounting (AAA) are more or less dependent on each other. However, separate protocols are used to achieve the AAA functionality. IETF AAA working group is trying to design one AAA protocol that could be used in a variety of applications. AAAARCH is also trying to build a general architecture for AAA systems. Mobile Ad Hoc networking (MANET) brings new challenges to providing the AAA functionality. Ad Hoc networks are by their nature rapidly changing and dynamic. There isn't necessarily any network infrastructure present.
A number of research works were conducted on the classically centralized AAA functions [11, 12], but few of them studied the possible interactions between AAA and ad hoc network. For instance, [13] focuses mainly on the authentication architecture for enabling distant users to access to services (like internet) through an ad hoc network [13] proposes to perform authentication based on EAP-TLS and PANA [14], but in a multi-hop network context. The EAP-TLS authentication phases end with the ad hoc node and the access network sharing a security association for next data exchanges to remain confidential.

3.1 Authentication

Some kind of authentication is needed in ad hoc networks. Because an ad hoc network is open in the way that mobile hosts can come and go, there is no way to know, which mobile hosts are present in the network. If some data for example are being transmitted, it is important to make sure that the communication is established with the right host.
One way to deal with low physical security and availability constraints is the distribution of trust [1]. Trust can be distributed to a collection of nodes. If all t+1 nodes will be unlikely compromised, then a consensus of t+1 nodes is trustworthy [2].
In [2] a distributed key management service is described. In this (n, t+1) model there is not only one CA (*Certificate Authority*) but many. There are n special nodes which act as servers. As long as at most t servers are compromised the scheme works [1].

This key management approach is based on the *threshold cryptography*. A (n, t+1) threshold cryptography scheme allows n parties to share the ability to perform a cryptographic operation, so that any t+1 parties can perform this operation jointly whereas it is infeasible for t parties to do so, even by collusion [2].
In this key management service, n servers share the ability to sign certificates. A (n, t+1) threshold cryptography scheme is used to make the service tolerate t compromised nodes. Service private key is divided to n shares, which are distributed to all servers. To sign a certificate each server signs the certificate with its share and transmits the certificate to a combiner. A combiner is able to sign the certificate if it gets t+1 correct partial signatures. Compromised servers are not able to sign certificates, because there is at most t of them at any time [1].
After having built this kind of key management system a public key cryptography can be used to do the authentication [1].

3.2 Authorization

Authorization is also needed to avoid malicious host to be able to wreak havoc inside the network [1]. This can be prevented by keeping control of what hosts are allowed to do inside the ad hoc network. Authorization also needs some sort of distributed structure to avoid single point of failure. This is why the traditional way of using *access control lists* (ACL) in one central server isn't adequate in ad hoc networks [1].

3.3 Accounting

Accounting features are quite specialized in ad hoc networks. Because basically there is no network infrastructure that is providing the service, there isn't either the same kind of service provider concept as in traditional networks. In ad hoc networks individual mobile hosts are providing service to each others; hop by hop routing. There can be two kinds of situations in the charging point of view. The first one has no need to use charging. In this situation all the hosts have decided together that they want to form an ad hoc network for their own need to communicate with each other freely. This could mean they all belong to the same organization like in the case of military units or they are in the same place and want to communicate like in a meeting. So, this ad hoc network is most likely an infrastructureless intranet. In the second case, mobile nodes are just participating in the network to communicate with some of the other nodes only. In this situation, if some mobile node acts as a router in the network, providing con-

nectivity between two nodes that are not within each others range, then it would be reasonable to charge some money for this routing service [1].

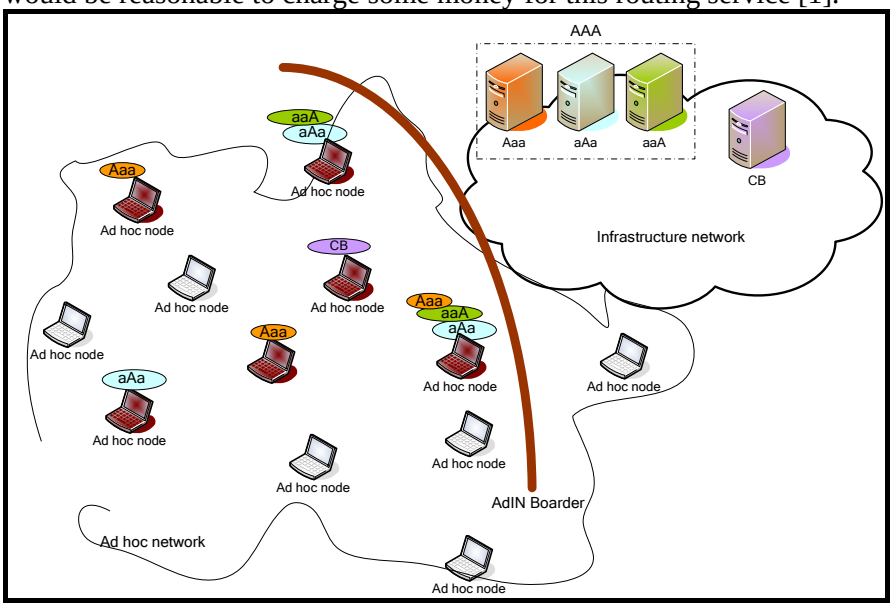

Fig. 1. AdIN Framework

Accounting in ad hoc networks hasn't been studied very much. So there is no protocol to do the actual charging yet. This area is however quite interesting, because it is faced with questions like how mobile nodes can charge each others? We cannot assume connectivity to some central server that takes care of the charging in the ad hoc network, so there is a clear need for distributed charging protocols as well with the strong constraint that banks are accepting this new individual to individual charging [1].

3.4 AAA systems

Ad hoc networks and general AAA systems can be seen as oxymoron. The biggest problem is related to the varying nature of the network. There are no home domains or foreign domains, because the networks are built in ad hoc way. Also the term service provider will have a different meaning than before. This does affect the AAA systems that the AAA working group is presenting, because some of the basic building blocks of their architecture are missing from the ad hoc networks [1].
The basic problem as we mentioned before is the model provided by the AAA working group which is a centralized trust model. This clearly does-

n't fit well into ad hoc networks since it’s decentralized. We need some other kinds of methods to achieve the AAA functionality.
One approach to provide authentication and authorization functionalities in ad hoc networks could be to use trust management based approaches like PolicyMaker or Keynote2 [1]. These are decentralized by nature and can provide the requested functionality in ad hoc networks quite easily. Also other protocols like SASL or ISAKMP/IKE could be used to provide the authentication functionality [1].

4 Secured Ad Hoc Access Framework

Introduction of AAA into ad hoc environment is not an easy task due to the self organising aspect of the ad hoc network. The objective of this approach is to design a functional bridge (architecture) between the ad hoc network and the infrastructure network when it is available to support secured exchange of services between the ad hoc nodes. The designed architecture named AdIN (Ad hoc/Infrastructure) is represented in Fig. 1 below. It targets deploying several mechanisms such as authentication, authorization, accounting, key management. Neighbour and Service discovery mechanisms are also necessary to provide information for the ad hoc node in order to allow him get the appropriate service.
The first strong point of AdIN framework, is to decompose the AAA service in the infrastructure into Aaa, aAa, and aaA services in order to offer them fully or separately to the ad hoc network and this would be seen as a service rendered to the ad hoc node and hence chargeable. Another strong point of this architecture is the delegation of one or all of these services (Aaa, aAa, aaA) into certain nodes of the ad hoc network. These nodes are supposed to be secure and trusted by the infrastructure. For instance, there might be nodes that belong to the infrastructure network administration (i.e. airport buses equipped with ad hoc material). These nodes are specially set up by the operator willing to extend his infrastructure network to the ad hoc network these special nodes might be freely moving in the ad hoc network carrying with them the AAA services configured at the first place by the operator. The carried AAA services would be offered to the ad hoc network, when this one could not join the infrastructure network to benefit from the AAA service located in the infrastructure. This delegation of AAA services to the ad hoc network assumes a trusted relationship between those ad hoc nodes capable of offering the AAA services.
The aAA services could be implemented by the ad hoc nodes that are willing to provide services to the other nodes (content delivery or exchange,

packets forwarding, Internet access …). So these services (aAa, aaA) might be easily distributed in the ad hoc network as long as an accounting and billing system is in place.
The Aaa service is more difficult to distribute totally since it authenticates users joining the ad hoc network. Those users are not known by the ad hoc network. That is why it is necessary to ensure an interdomain authentication between the ad hoc network and the infrastructure network. This interdomain signalling will be ensured by the AdIN boarder represented in the figure.
Finally the Charging and Billing (CB) service as represented in the figure could be offered by the infrastructure to the ad hoc nodes. It means that the infrastructure will be aware of the services exchanges between the ad hoc nodes and will charge the serviced ad hoc nodes for that. The servicing ad hoc node will get the payment for the service offered and will also pay the infrastructure network for supporting the CB on his behalf. As for the authentication (Aaa), authorisation (aAa) and accounting (aaA) services the infrastructure network will make profit on the usually not directly billed service which is here the CB.

4.1 Available services within ad hoc nodes

There might be users in the ad hoc network offering services like in Peer to Peer (video, music records…). They might behave as very small operators offering at low cost contents Ad hoc level services such as peer-to-peer content exchange, packet forwarding, resource consumption …etc. In airport for instance, there might be also shops offering a number of services, free services like advertisement, charged services like download of pieces of music and so on. Furthermore, the classical AAA services could be offered by the infrastructure network to the ad hoc network and made profit from it.
In that sense, we differentiate in this architecture the network and user services. The network service is the service that the infrastructure network would offer to the ad hoc networks such as the authentication service needed by the ad hoc nodes. The user service is the service that an ad hoc node would offer to neighbour ad hoc nodes or to another ad hoc network such as ad hoc routing.

4.2 Neighbour and service discovery

Neighbour and Service discovery mechanisms are necessary to provide information for the ad hoc node regarding the service availability at the in-

frastructure boarder or inside the ad hoc network in order to allow him get the appropriate service.
The IETF has defined few protocols for service discovery. Service Discovery Protocol (SDP), and Service Location Protocol (SLP) [15] are designed for service discovery. SLP provides a scalable framework for the discovery and selection of network services. The protocol allows, with little or no static configuration, to discover network services for accessing network based application.
Another approach would be to use Web services (WS) based architecture. This permits to include a rich suite of specifications that provides complementary functions in the areas of security, reliability, and transaction-based messaging.
In the context of our AdIN architecture, the service discovery framework has to consider both user services (those offered by ad hoc nodes) and infrastructure services (those offered by the infrastructure network to the ad hoc network such as Aaa).
Special gateways could be used at the boarder of the ad hoc network to present the services that the infrastructure could offer to the ad hoc network and vice versa. The service discovery framework would be combined with the accounting and charging service which is tightly related to the AAA service.

4.3 User identification and anonymity

It is important to ensure user anonymity over the ad hoc network. So the servicing node and even spying nodes are not able to know who is connected and accessing some services. That is, the infrastructure provider must identify the user, but the ad hoc servicing nodes should not know the users identity. The only constraint for the servicing node is to be paid for the accessed services such as content delivery or ad hoc routing. As such, pseudonyms might be used within ad hoc networks while ordinary identification and authentication of the users to access the infrastructure is mandatory.

4.4 Authentication to the infrastructure

The first ‘A’ in Aaa stands for authentication. It would be ideally distributed among ad hoc nodes. Due to the trust management problem, this would not be possible for now. However, the existing reliable and efficient Aaa system in the operator’s network could be extended towards the ad hoc structure. Consequently, the extended Aaa service would be consid-

ered as a standalone service for ad hoc groups that would be billed for this authentication service.
The Aaa service will be offered by the infrastructure to the ad hoc network to ensure the deployment of services in the ad hoc network. The AAA service will operate in a self organized network (muti-hop) which is a challenging task. The PANA approach is a promising candidate for supporting Aaa service in a multi-hop context as it works over the IP level [13], and as such is independent of the underlying access technologies including ad hoc networks.
Moreover, an Inter-domain AAA will be necessary for the network operator to open its Aaa service to ad hoc subscribers from another operator. As such, any user might be able to join any ad hoc network and to ask for local available services.

4.5 Authorization and Accounting

aAA would be distributed within ad hoc nodes, and this is very challenging from a research point of view as there is a need to define how servicing ad hoc nodes are collecting accounting information of ad hoc customers. This accounting information would be used for supporting secure electronic transactions and charging within ad hoc nodes.
The Accounting service (aaA) will be adapted to services available in ad hoc network. The servicing ad hoc nodes will adopt a certain accounting policy per service (forwarded packets, service duration, and content value, bid…). This will solve the selfish behaviour of certain ad hoc nodes which is a very well known issue by encouraging them to participate in the ad hoc network communication.

4.6 AAA as a basis for securing communications between ad hoc nodes

The idea is to benefit from the Aaa exchanges with the network operator to establish some security material (keys, algorithms…) within ad hoc networks and thus to ensure the protection of ad hoc communications. Some of the EAP authentication methods like EAP-TLS, EAP-TTLS… permit both authenticating parties to share a common key (called MSK for Master Session Key) at the end of EAP exchanges. In the context of ad hoc nodes, this EAP method might be very helpful for nodes to establish a common secret and use it to secure their connections. For instance, a group key might be pushed by the infrastructure to the ad hoc nodes. It is also

possible for the infrastructure to generate and distribute attribute certificates to the ad hoc nodes.

4.7 Trust management within ad hoc nodes

Trust management is necessary during the creation and the evolution of the ad hoc network. It is the fundamental premise to build a secured exchange of services where services such as authentication, authorisation, accounting, charging and billing are supported.
Trust management is mainly used to control that nodes are actively participating to the connectivity maintenance of the network, performing for instance packet forwarding. As secure routing protocols designed for ad hoc network are based on heavy cryptographic tools, deploying trust management might be advantageously used to ensure some control within ad hoc networks. Actually, trust management might be enough to ensure a certain security level without heavy crypto based protocols.
In an infrastructure network, network nodes (e.g. routers) are under the control of a certain administration (network operator, corporate network…), that is a strong trust basis. On the other hand, in an ad hoc network, there is no administration a priori to control the network. That is the reason why there is no intrinsic trust in an ad hoc network. It explains some security problems such as selfish behaviour of certain ad hoc nodes. When the ad hoc network can get access to the infrastructure network, it can benefit from a strong authentication offered by the infrastructure network and will then authenticate all the ad hoc nodes that will join the ad hoc network, thus ensuring the trust relation between all the ad hoc nodes.
The problem of trust creation and maintenance in ad hoc networks is worsen when this one cannot have access to a strong authentication like the one offered by the infrastructure network. There are few mechanisms that are dealing with this problem. For instance a reputation based mechanism which is very likely similar to trust building in a human community.

4.8 New business model

The resulted business model will be more complex with the interaction of four parties: operators, content and application/software providers, ad hoc nodes distributing contents to any nodes purchasing contents. The content provider's role will consist in providing the active ad hoc nodes with contents so a new market based on the peer-to-peer principle (with no de-

ployment needs for the provider) is made possible. To bring new ad hoc node content distributors, remuneration of distributors may be envisioned.
Another point will be to introduce the application service provider role in the ad hoc network. However, the risk is high that the application providers are infected by a virus due to customers executing malicious programs. For such services to remain securely deployed, the ad hoc machine architecture should be carefully designed with disk partitioning for example.
Limited resource (UPC, bandwidth,…) networks like domestic networks might also benefit from the security AAA mechanisms defined in the AdIN approach. Domestic networks meet difficulties performing auto configuration, security initialization, and the AdIN approach may be of some help using the operator's access network as a third party. It might also be envisioned that videos digitally registered by individuals are billed to the neighbours including taxes for the authors' rights. However, there is a need to adapt AdIN mechanisms to such low resources devices.

5 future works

As this paper introduces a new framework to allow the integration of ad hoc network with the infrastructure network, next step of our work is the implementation of the concepts introduced (AdIN boarder, decomposed AAA service, …) and the validation of the AdIN framework. In this architecture, the Aaa, and the aAA services will be distributed but will need somehow a certain control from the infrastructure network which is until now the sole trusted party that can guarantee the trueness of the information necessary for user authentication. The need for AAA distribution may happen when the ad hoc group is temporarily disconnected from the infrastructure and continuous service delivery is highly expected; especially in that case, the use of prepaid tools might be helpful for the serving service node to manage on its own the billing.

6 Conclusion

With the need for Always On, the coverage of current access networks infrastructures must be extended and the ad hoc network technology is an enabling technology for the always on technology at low cost, with auto configuration capabilities, network dynamicity management… In this new designed ad hoc/infrastructure architecture, new business oriented services will emerge within the ad hoc network with local ad hoc customers. How-

ever, until today, the ad hoc network technology is not finding its way to integrate the value chain of telecommunication. We propose in this paper to integrate the ad hoc technology in the service deployment value chain by decomposing the AAA service and executing it in the ad hoc network to ensure secured exchange of services. The infrastructure network would benefit from integrating the ad hoc technology in the access network since it will bring more users in the network. It will also benefit from converting the classically indirectly chargeable services such as authentication, authorisation, accounting, charging, billing,…etc directly chargeable to the ad hoc nodes using those services to build an ad hoc structure to exchange services.

7 References

1. Levijoki S. (2000) Authentication, Authorization and Accounting in Ad Hoc networks**,** http://www.tml.tkk.fi/Opinnot/Tik110.551/2000/papers/authentication/aaa.htm#chap5
2. Zhou L., Haas Z. (1998), Securing Ad Hoc Networks, 1998. http://www.ee.cornell.edu/~haas/Publications/network99.ps
3. Housley R., Ford W., Polk W., Solo D.(1999), Internet X509 Public Key Infrastructure Certificate and CRL Profile, RFC 2459, January 1999.
4. Hu Y. C., Perrig A., Johnson D. B. (2002): Ariadne: A secure on-demand routing protocol for Ad Hoc networks, Proceedings of the 8th ACM International Conference on Mobile Computing and Networking, 2002.
5. Guerrero Zapatav M.(2002), Secure Ad hoc On-Demand Distance Vector Routing, ACM Mobile Computing and Communications Review (MC2R), vol. 6, no. 3, pp. 106–107, July 2002.
6. Luo H, Zerfos P., Kong J., Lu S., Zhang L. (2002) Self-securing Ad Hoc Wireless Networks, Seventh IEEE Symposium on Computers and Communications (ISCC'02), 2002.
7. Yi S., Kravets R. (2003), MOCA: Mobile Certificate Authority for Wireless Ad hoc Networks, in Proceedings of 2nd Annual PKI Research Workshop, NIST, Gaithersburg, MD, April 2003.
8. Boneh D., Franklin M. (2001) Identity-Based Encryption from the Weil Pairing. In J. Killian, editor, Advances in Cryptology, CRYPTO 2001, volume 2139 of Lecture Notes in Computer Science, pages 213-229. Springer Verlag, August 2001.

9. Khalili A., Katz J., Arbaugh W.A. (2003), Towards secure key distribution in truly ad hoc networks, IEEE Workshop on Security and Assurance in Ad hoc Networks, 2003.
10. IEEE Standard 802.1X-2004, Standard for Local and Metropolitan Area Networks: Port-Based Network Access Control, December 2004.
11. Lopez R. Marin, Bournelle J., Combes J.-M., Laurent-Maknavicius M., Gomez Skarmeta A. F. (2006), "Improved EAP keying framework for a secure mobility access service", International Wireless Communications and Mobile Computing Conference IWCMC 2006, Published in ACM Digital Library, Conference, Vancouver, Canada, July 2006.
12. Bournelle J., Laurent-Maknavicius M., Giaretta G., Guardini I., Demaria E., Marchetti L (2005)., Bootstrapping Mobile IPv6 using EAP, Joint IEEE Malaysia International Conference on Communications and IEEE International Conference on Networks, MICC-ICON 2005, Lumpur, Malaysia, November 2005.
13. Cheikhrouhou O., Laurent-Maknavicius M., Chaouchi H. (2006), Security architecture in a multi-hop mesh network, 5ème conférence sur la Sécurité et Architectures Réseaux SAR 2006, Seignosse, Landes, France, juin 2006.
14. Parthasarathy M. (2005), Protocol for Carrying Authentication and Network Access (PANA) Threat Analysis and Security Requirements, RFC 4016, March 2005.
15. Service Location Protocol: http://www.openslp.org, IETF - Service Location Protocol : http://www.ietf.org/html.charters/OLD/svrloc-charter.html