Toward a new ad hoc node design for secure service deployment over ad hoc network

Hakima Chaouchi, Maryline Laurent

TOWARD A NEW AD HOC NODE DESIGN FOR SECURE SERVICE DEPLOYEMENT OVER AD HOC NETWORK*

HAKIMA CHAOUCHI, MARYLINE LAURENT- MAKNAVICIUS
{Hakima.Chaouchi, Maryline.Maknavicius}@it-sudparis.eu
Institut TELECOM, TELECOM & Management SudParis
LOR/SAMOVAR/CNRS UMR-5157
9 rue Charles Fourier, 91011 Evry
France

Abstract- Security in ad hoc networks is a major issue when it comes to real deployment of services over this sort of networks. A large amount of research effort was directed toward routing in ad hoc networks, however securing the connectivity and the packet transmission is a brake in relying on an ad hoc network as any other infrastructure based network. In this paper, we propose a secured architecture over ad hoc network based on the AAA concept (Authentication, Authorisation, Accounting), and a new ad hoc nodes design for any kind of ad hoc nodes to securely support part or full AAA services.

Keywords: ad hoc networks, AAA, virtualization.

1. Introduction

Ad hoc network is dynamically changing its network topology. It is an infrastructureless network created by mobile nodes in an ad hoc way. 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 routing protocols to be used in ad hoc networks. Most of the traditional protocols don't fit very well into ad hoc networks. New routing protocols [1, 2] were developed but none of them is really deployed.

In the context of Always On era, ad hoc technologies integration with the infrastructure is without any doubt an interesting 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

* This work has been done in the context of the French research project SARAH, ANR 2006

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 [3].

As most of the security issues in ad hoc networks are caused by trust less nodes, the authentication process is a strong solution to identify 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 by the servicing ad hoc nodes. For this purpose, a trust management framework is necessary. Furthermore, we propose a new design of ad hoc nodes that enables any kinds of ad hoc nodes to securely support part or full AAA services, and to act as individual or delegated ad hoc service providers to other ad hoc nodes.

One obvious and original consequence of the secured framework and node design would be the integration of ad hoc technology in the service value chain by the introduction of a new service provider (ad hoc network service provider), and a new network access provider (ad hoc network). Users provided with one or more suitably designed ad hoc node(s) are also able to join the service value chain by offering their nodes capacity to some well known ad hoc (service or network access) providers. 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. AAA in ad hoc networks

Typically authentication, authorization, and accounting 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. These and other features of ad hoc networks present many new requirements for the protocols that are to be used in ad hoc networks [4].

A number of research works were conducted on the classically centralized AAA functions [5, 6], but a very few of them studied the possible interactions between AAA and ad hoc network. For instance, [7] focuses mainly on the authentication architecture for enabling distant users to access to services (like internet) through an ad hoc network. [7] proposes to perform authentication based on EAP-TLS and PANA [8], but in a multi-hop network context. The EAP-TLS authentication phase ends with the ad hoc node and the access network sharing a security association for next data exchanges to remain confidential.

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 is 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 [4]. 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 [3].

Authorization is also needed to avoid malicious host to be able to wreak havoc inside the network [4]. 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 [4].

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. There can be two kinds of situations in the charging point of view. One is the kind of a situation in which there is 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. This could mean that they all belong to the same organization like in the case of military units or that they are in the same place and want to communicate like in the case of meetings. So, this kind of ad hoc network is a kind of intranet. In the other kind of situation individual mobile nodes are just participating in the network to communicate with some of the other nodes, not all. In this situation, if some mobile node acts as a router in the network, providing connectivity between two nodes that are not within each others range, then it would be reasonable to charge some money for this service [4].

Accounting in ad hoc networks hasn't been studied very much yet. So there exists no protocols to do the actual charging if that is needed. This area is however quite interesting, because it is faced with questions like how individual mobile nodes can charge each others? Because we cannot assume connectivity to some central server that takes care of the charging, there is a clear need for distributed charging protocols as well [4] with the strong constraint that banks are accepting this new individual to individual charging.

d) 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 an 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 [4].

The basic problem as we mentioned it before is that the model provided by the AAA working group is a centralized trust model. This clearly doesn't fit well into ad hoc networks, because the network structure is 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 [4]. 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 [4]

3. Related work: AAA architecture over infrastructure based ad hoc networks

As described in [9], the 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, and 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.

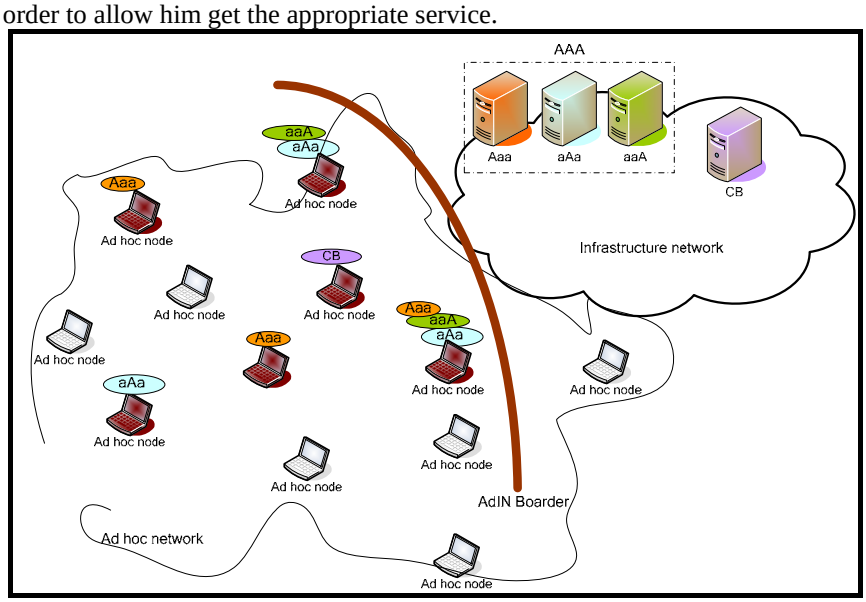

Figure.1: AdIN Framework

The main features of AdIN architecture are [9]:

- available service within ad hoc nodes;
- neighbour and service discovery;
- user identification and anonymity;
- AAA as a basis for securing communications between ad hoc nodes;
- trust management within ad hoc nodes

AdIN framework suggests decomposing the AAA service in the infrastructure into Aaa, aAa, and aaA services in order to offer them completely

or separately to the ad hoc network. 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. There might be nodes that belong to the infrastructure network administration (i.e. airport buses equipped with ad hoc material). These nodes might be freely moving in the ad hoc network carrying with them the AAA services. The carried AAA services would be offered to the ad hoc network, when this one could not join the infrastructure network and 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 figure 1.

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.

In [9], we considered those AAA services to be hosted by some ad hoc nodes belonging to some administrative providers. In the next section, thanks to the proposed design of ad hoc nodes, those AAA ad hoc nodes can also be owned by users.

4. A proposed AAA architecture over infrastrureless/standalone ad hoc network

We consider a scenario depicted on figure 2 where we can build in a secured and ad hoc way a connected network based on special ad hoc nodes belonging

either to providers or individuals. We introduce new ad hoc nodes pre-configured by a network or service provider to allow the establishment of an ad hoc network that will be used either to offer application services (video, network games, …), ad hoc connectivity or internet connectivity. Those nodes might be certified as supporting ad hoc services, and sold to users as generating possible profits. In the case of internet connectivity, it will be an infrastructure based ad hoc network [9]. We consider the usage of the ad hoc network for service deployment within the ad hoc nodes. It means that some ad hoc nodes will host servers. The other ad hoc nodes will connect to these ad hoc servers to get services.

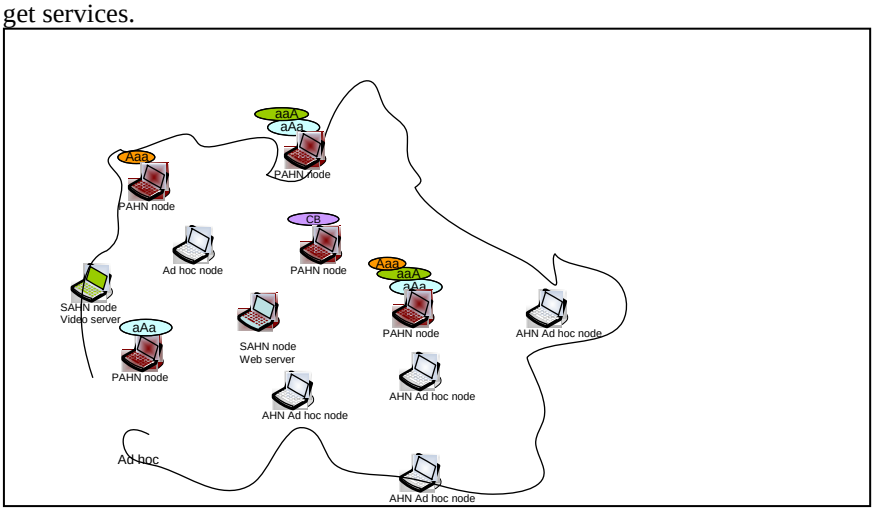

Figure.2:: **Ad hoc network based on Preconfigured ad hoc nodes**

We name:

- PAHN (Preconfigured Ad Hoc Node); the ad hoc nodes pre-configured by a network provider to launch a secure ad hoc network offering ad hoc connectivity. It is offering mainly AAA services.
- SAHN (Servicing Ad Hoc Node); the ad hoc node hosting an application based server (web content, video…). It can be preconfigured by a service provider extending their service to an ad hoc area.
- GAHN (Gateway Ad Hoc node); the ad hoc node offering access to internet. It is similar to a PAHN in the architecture; it is different in the offered service which is here the connectivity to internet.
- AHN an Ad Hoc Node.

These nodes will be designed with separated parts, thanks to the virtualisation concept where each of them is running separately from the others a specific environment at a same time. In these new designed ad hoc nodes, one part will run the user environment, another part will run the secured connectivity related

part (PAHN) and another one can run a service (SAHN) related part. This is illustrated on the figures below. It is also possible to consider a separation on network side or on a physical side. In the first case, one single network interface will be used for both user traffic and ad hoc network related traffic (using ad hoc routing). In the second case, two separate network interfaces will be used where one is dedicated for the user's traffic and the other one is used for the ad hoc network traffic. In this case we'll make sure that the user has no access at all to the traffic forwarded by his ad hoc node. In both cases the users agreed with the service or network provider to use their node as an ad hoc node which means that it will forwards other node's traffic. This agreement is defined in specific terms of the business model including the ad hoc nodes in the value chain [9].

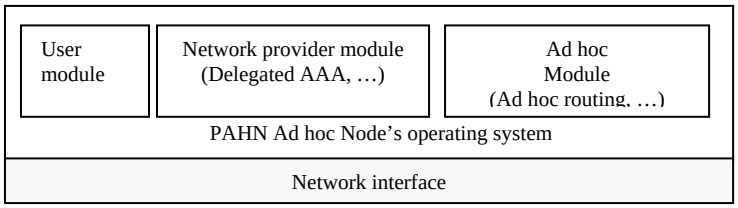

Figure3. Pre-configured ad hoc node (PAHN) with a unique network card.(Virtualisation at network layer)

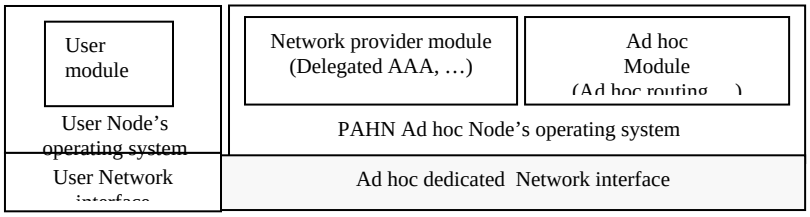

Figure 4. Pre-configured ad hoc node (PAHN) with two network cards; one for user traffic and the other is dedicated for the traffic of the other ad hoc nodes (Virtualisation at all layers, physical separation between user environment and the ad hoc treatment environment).

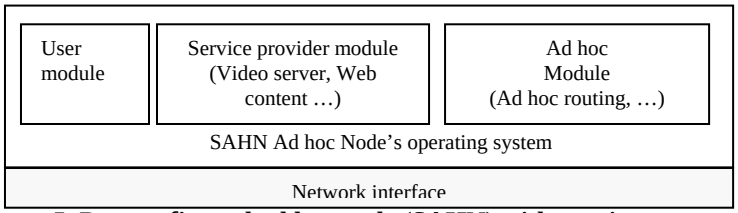

Figure 5. Pre-configured ad hoc node (SAHN) with a unique network card.(Virtualisation at network layer)

It is also possible for the ad hoc node to be PAHN and SAHN at a same time. In that case, both service provider and network provider modules will be located in the ad hoc node.
Note that a smartcard technology can be used to securely implement the network provider or server provider related environment. We can also use the virtualization technology to maintain the separation between the different modules.

The main application of these new designed ad hoc nodes is a fast deployment of a connected network without a real time support of the AAA service of the infrastructure, and with no mandatory presence of administrative ad hoc nodes. In fact the AAA service is preconfigured on the PAHN, thus allowing the authentication of the ad hoc nodes forming the network. This ad hoc network is created to provide networked applications and not internet access. In the case where internet access is needed, the GAHN are needed as well in the ad hoc node to provide a gateway service from the ad hoc node to the internet infrastructure.

5. Conclusion

The infrastructure network (network and service providers) will benefit from integrating the ad hoc technology in the access network since it will bring more users in the network. In this paper, we introduce a pre-configured ad hoc nodes design in order to build a secure ad hoc network that will support service deployment. In these pre-configured ad hoc nodes, the usually centralized AAA service will be offered by those ad hoc nodes in the ad hoc network (hybrid or standalone). Other services such as application based will be offered by other preconfigured ad hoc nodes. This will expand the service deployment of service providers to a standalone ad hoc network. The major issue will remain in battery consumption of those ad hoc nodes. They will probably use longer life battery than a simple consuming ad hoc node.

6. References

1. M. Guerrero Zapata: “Secure Ad hoc On-Demand Distance Vector Routing,”ACM Mobile Computing and Communications Review (MC2R), vol. 6, no. 3, pp. 106–107, July 2002.
2. Y. C. Hu, A. Perrig, D. B. Johnson: “Ariadne: A secure on-demand routing protocol for Ad Hoc networks”, Proceedings of the 8th ACM International Conference on Mobile Computing and Networking, 2002.
3. L. Zhou and Z. J. Haas. *Securing Ad Hoc Networks*. IEEE Network Magazine, vol. 13, no.6, November/December 1999.

4. S. Levijoki. *Authentication, Authorization and Accounting in Ad Hoc networks***,** 2000, http://www.tml.tkk.fi/Opinnot/Tik-110.551/2000/papers/authentication/aaa.htm
5. R. Marin Lopez, J. Bournelle, J.-M. Combes, M. Laurent-Maknavicius, A. F. Gomez Skarmeta. *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.
6. J. Bournelle, M. Laurent-Maknavicius, G. Giaretta, I. Guardini, E. Demaria, L. Marchetti. *Bootstrapping Mobile IPv6 using EAP*. Joint IEEE Malaysia International Conference on Communications and IEEE International Conference on Networks, MICC-ICON 2005, Lumpur, Malaysia, November 2004.
7. O. Cheikhrouhou, M. Laurent-Maknavicius, H. Chaouchi. *Security architecture in a multi-hop mesh network.*, 5ème conférence sur la Sécurité et Architectures Réseaux SAR 2006, Seignosse, Landes, France, juin 2006.
8. M. Parthasarathy. *Protocol for Carrying Authentication and Network Access (PANA) Threat Analysis and Security Requirements*. RFC 5016, March 2004.
9. H. Chaouchi, M. Maknavicius. *SAACCESS: Secured Ad hoc ACCess framework*. NTMS 2007, Paris May 2007.