CHAPTER 35

SAACCESS: SECURED AD HOC ACCESS FRAMEWORK

H. CHAOUCI AND 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 protocols 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].

© 2007 Springer.
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 introduction 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