

Distributed AAA Scheme for Mobile Ad-hoc Networks

Sondes LARAFI
Maryline LAURENT-MAKNAVICIUS
GET/INT, 9 rue Charles Fourier
91011 EVRY, FRANCE
sondes.larafa@it-sudparis.eu
Maryline.Maknavicius@it-sudparis.eu

Richard NOCK
UAG, qua Ravine Touza,
97233 SCHOELCHER, FRANCE
Richard.Nock@martinique.univ-ag.fr

I. INTRODUCTION

Ad-hoc networks are wireless networks that autonomously auto-configure and need no network administrators' intervention. They are infrastructure-less i.e. they need no central entity for packet routing. Ad-hoc networks are very dynamic. A mobile node joins an ad-hoc network simply by connecting to the nearest already connected nodes. Once a mobile node is connected, it has 3 functions: transmitting and receiving data in addition to routing.

Ad-hoc networks are very useful during military and rescue operations because they are simple to set up and remain operational as long as there are enough nodes to relay traffic. They are also likely to be snuffed by providers of content, multi-media, games, etc, since they are less expensive than infrastructure networks and allow better users' mobility.

The wireless nature of ad-hoc connections and the dynamicity of these networks make them vulnerable to attacks. Hence security is of large concern. There are 2 approaches for security: secure individual communications and secure the whole network. Securing individual communications of a node A with a node B means that A shares some security material with B or trust a third party to get security material and communicate with B. Securing the whole ad-hoc network means that every joining node must authenticate itself to a trust entity in the network in order to be able to send traffic via the network. The second approach allows better network security since we control the access to the network. Control network access can be achieved with AAA infrastructures [1] [2] [3], that is why we analyze in this article a AAA solution for ad-hoc networks.

The simplest approach to provide AAA functionality in ad-hoc network is to assign a single node to be the AAA server. The success of this scheme depends on that single AAA server node. This approach is not fault tolerant and is highly vulnerable, since failure of one node or compromising it by an adversary breaks the system. In addition availability of the AAA server is not always possible given the expected mobility and unpredictability of ad-hoc networks. Therefore, a single AAA server cannot effectively service a whole ad-hoc network.

Replicating a fully functional AAA server on several different nodes, say n nodes (n AAA servers) can ensure the missing robustness in the single AAA server scheme. With n replicas, the system can withstand $n - 1$ failures because the AAA service is available as long as there is at least one operational AAA server. Availability has also been improved since a joining node has a better chance of reaching one of the n AAA servers to be authenticated. Unfortunately, the system has become more vulnerable. An adversary need only compromise one of the n AAA servers to compromise the whole system. Therefore using replicated AAA servers is not a viable solution in ad-hoc networks. The problem of using replicated AAA servers stems from the fact that each replica has full knowledge of the system secret.

To insure invulnerability it would be better to distribute the AAA server on the n most powerful and trustful mobile nodes (future AAA servers) that can be selected by a third party (organization, operator, etc). There are different ways to distribute the server. This depends specially on the authentication method used. Our solution is based on authentication with public certificates [4]: the AAA servers share one public certificate and each new arriving node must have already a public certificate delivered by the same certification authority. The location of the certification authority is out of the scope of this article.

A public certificate can be shared between several nodes by sharing the same private key. Shamir proposed a way to share a key between n different parties so that only $t \leq n$ parties associated among them can compute the original key [5]. Shoup proposed a way to compute signature shares, using these key shares, so that once combined give only one signature of an entity that stands for all the parties [6].

This document introduces a new AAA architecture in mobile ad-hoc network. It's a distributed and dynamic architecture composed of AAA servers, AAA clients and Enforcement Points (EP). AAA servers are selected by the operator or the organization and AAA clients/EP are the nodes that have been already authenticated by the AAA servers to join the ad-hoc network.

II. FRAMEWORK

To ensure AAA service, ad-hoc nodes are either AAA servers or AAA clients/Enforcement Points.

The service initiation depends on a high institution (a trusted third party) such as a Service Provider, a Military institution, a Rescue Organization, etc, which indicates the mobile nodes to be AAA servers. These servers offer AAA service.

When a sufficient number n of AAA server devices (n fixed by the trusted third party) present in the ad-hoc network is reached, the service can start. n can be equal to 1. In this case there is one server in the network. This can be sufficient if the total number of nodes to be authenticated is small (not more than 10). However if this server breaks down or disconnects, the service will be unavailable. For this reason it is better to choose n bigger than 1.

Every user of the network must be authenticated once the service is available. Authentication is carried out with public certificates [4] and the trusted third party is responsible for distributing them to all members of the ad-hoc network. AAA servers get only one certificate and can use it as a group. No server can use it on its own. However a subgroup of them could use it if the trusted third party decided it. This can be possible by applying threshold cryptography [5]: out of $n (=t + k)$ servers any t servers, as a group, can use the public certificate during authentication.

Threshold cryptography is very important in our framework. It is based on the idea of sharing the private key [7] (that is associated to the public key that lies in the public certificate of the AAA service) into key shares to be held by the servers. An adversary have to corrupt at least t servers out of n to lay a hand on service's certificate and so controle the whole AAA service. That is why it is necessary to refresh servers' key shares periodically.

During the existence of the ad-hoc network, some mobile nodes join it and some other leave it. Some server nodes may also leave. In that case it is necessary to elect new ones. when the number of AAA servers is no longer enough to handle future authentications (this is a boundary to evaluate) it is necessary to do election, too. In our framework, election is based on "Election Parameters" and followed by key shares' redistribution. Thereafter elected nodes receive these newly generated key shares.

Authentication is mutual i.e. the joining node authenticates to the group of AAA servers and the group authenticates to the the joining node. Each node that is not a AAA server is a AAA client. So the joining node is a AAA client. It has already a public certificate and uses it to authenticate to the servers. When authentication succeeds, the servers send an ACCESS TOKEN to the joining node which becomes,so , an authenticated node. The ACCESS TOKEN is to some extent like the passport for the joining node.

Authenticated nodes are not only AAA clients but also Enforcement Points. They watch out the traffic received from their neighbors and examine especially ACCESS TOKEN. When this latter does not exist or is false they do not relay the traffic.

III. FUTURE WORK

Our solution treats essentially the authentication and authorization issues in ad-hoc network. The AAA infrastructure proposed is in fact a light infrastructure. We believe that new services will be created to be used over ad-hoc network and that services providers will need to charge these services. So accounting is a real issue in ad-hoc networks. [8] proposes a model for accounting when there is a close relationship between the ad-hoc network and the trusted third party. It is still necessary to define a distributed model for a quasi-independent ad-hoc network. It is also necessary to define the accounting messages exchanges and their format.

Besides an implementation or/and simulation is to be accomplished to evaluate several parameters such as the density of AAA traffic. Thereafter we can improve our solution.

REFERENCES

- [1] B. Abobaa, P. Calhoun, S. Glass, T. Hiller, P. McCann, H. Shiino, G.Zorn, G. Dommety, C. Perkins, B. Patil, D. Mitton, S. Manning, M. Beadles, P. Walsh, X. Chen, S. Sivalingham, A. Hameed, M. Munson, S. Jacobs, B. Lim, B. Hirschman, R. Hsu, Y. Xu, E. Campbell, S. Baba, and E. Jaques. (2000, November) Criteria for Evaluating AAA Protocols for Network Access.
- [2] C. Rigney, S. Willens, A. Rubens, and W. Simpson. (2000, June) Remote Authentication Dial In User Service (RADIUS).
- [3] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, and J. Arkko. (2003, September) Diameter Base Protocol.
- [4] R. Housley, W. Ford, W. Polk, and D. Solo. (1999, January) Internet X.509 Public Key Infrastructure Certificate and CRL Profile.
- [5] A. Shamir. (1979) How to Share a Secret.
- [6] V. Shoup. (2000) Practical Threshold Signatures.
- [7] R. Rivest, A. Shamir, and L. Adleman. (1978) A Method for Obtaining Digital Signatures and Public-Key Cryptosystems.
- [8] H. Chaouchi and M. Laurent-Maknavicius. SAACCESS: Secured Ad hoc ACCess framework.