available at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Reliable and fully distributed trust model for mobile ad hoc networks

Mawloud Omar[a,*], *Yacine Challal*[b], *Abdelmadjid Bouabdallah*[b]

[a]*ReSyD, Bejaia University, Algeria*
[b]*Heudiasyc Lab., Compiegne University of Technology, France*

ARTICLE INFO

Article history:
Received 26 February 2008
Accepted 26 November 2008

Keywords:
MANETs
Security
Trust model
Trust graph
Threshold cryptography

ABSTRACT

A mobile ad hoc network (MANET) is a wireless communication network which does not rely on a pre-existing infrastructure or any centralized management. Securing the exchanges in MANETs is compulsory to guarantee a widespread development of services for this kind of networks. The deployment of any security policy requires the definition of a trust model that defines who trusts who and how. Our work aims to provide a fully distributed trust model for mobile ad hoc networks. In this paper, we propose a fully distributed public key certificate management system based on trust graphs and threshold cryptography. It permits users to issue public key certificates, and to perform authentication via certificates' chains without any centralized management or trusted authorities. Moreover, thanks to the use of threshold cryptography; our system resists against false public keys certification. We perform an overall evaluation of our proposed approach through simulations. The results indicate out performance of our approach while providing effective security.

1. Introduction

A mobile ad hoc network (MANET) (Perkins, 2000) comprises a group of wireless independent nodes which temporarily forms a network without pre-existing infrastructure; all networking operations (routing, mobility management, and so on) are performed by the nodes themselves. This emerging technology seeks to provide "anytime, anywhere" networking services for mobile users. With the proliferation of mobile computing and communication devices, mobile ad hoc networking is predicted to be a key technology for the next generation of wireless communications (Giordano, 2001). They are mostly desired in military applications where their mobility is attractive but where their insecurity continues to slow down more widespread take-ups.

Operation in an ad hoc network introduces new security problems: ad hoc networks are generally more prone to physical security threats. The possibility of eavesdropping, spoofing, denial-of-service, and impersonation attacks increases (Corson and Macker, 1999). Similar to fixed networks, security of the ad hoc networks is considered from different points such as availability, confidentiality, integrity, authentication, non-repudiation, access control and usage control (Zhou and Haas, 1999; Zhang and Lee, 2000). However, security approaches used to protect the fixed networks are not feasible due to the salient characteristics of the ad hoc networks. New threats, such as attacks raised from internal malicious nodes, are hard to defend (Deng et al., 2002). In the literature, there are several manners to introduce security in mobile ad hoc networks that can be classified into two main approaches:

(1) Models based on TTP (Trusted Third Party) where certificates and/or keys are issued by a single authority

* *Corresponding author.*
E-mail addresses: mawloud.omar@gmail.com (M. Omar), ychallal@hds.utc.fr (Y. Challal), bouabdal@hds.utc.fr (A. Bouabdallah).
0167-4048/$ – see front matter © 2008 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2008.11.009

(or a group of special servers), like PKI (public key Infrastructure) (Perlman, 1999; Zhou and Haas, 1999) and Kerberos (Kohl and Neuman, 1991; Pirzada and McDonald, 2004).
(2) Through full self-organization, where security does not rely on any trusted authority or fixed server, like models based on trust propagation through a trust graph, such as PGP (Abdulrahman, 1997).

Our proposal is based on the second approach, and we propose *a fully distributed trust model based on trust graph for mobile ad hoc networks*, that allows nodes to generate, store, and distribute their public key certificates without any central server or trusted party. In our system, all the nodes have a similar role, and we do not assign any special functions to a subset of nodes. The main motivation for employing this approach comes from the self-organized nature of MANETs and from the need to allow users to fully control the security settings in the network. In our system, like in PGP (Abdulrahman, 1997), users' public/private keys are created by the users themselves, and key authentication is performed via chains of public key certificates in the graph of trust. Also, like in Capkun et al. (2003), instead of storing certificates in centralized certificate repositories, certificates in our system are stored and distributed by nodes themselves. Our main contribution is the inclusion of a threshold scheme within the graph of trust, in order to resist against false public key certificates issued by malicious nodes in the network. During network initialization, nodes share a private key, and each node holds one private share. Instead of using private keys for certificates signing, nodes will use their private shares. Our solution is developed for open networks, in which nodes can join/leave the network without any centralized administration. The joining operation is performed by a coalition of member nodes to allow access to a new node.

The remaining of this paper is structured as follows: in Section 2, we give an overview of threshold cryptography. In Section 3, we introduce the related works. In Sections 4 and 5, we give detailed description and analysis of our trust model. In Section 6, we describe and discuss simulation results. We finally conclude this work in Section 7.

2. Threshold cryptography: a background

A (t, n) threshold scheme ($t \leq n$) is a cryptographic technique that allows to hide a secret S in n different shares S_i ($1 \leq i \leq n$), so that the knowledge of at least t shares is required to recover the initial secret S. Let us illustrate this technique with the following famous scheme: Shamir's threshold scheme (Shamir, 1979) is based on polynomial interpolation, and the fact that a univariate polynomial $y = f(x)$ of degree $t-1$ is uniquely defined by distinct t points (x_i, y_i).

Setup: The trusted party T begins with a secret integer $S \geq 0$ it wishes to distribute among n users:

(1) T chooses a prime $p > \max(S, n)$, and defines $f(0) = a_0 = S$.
(2) T selects $t-1$ random, independent coefficients $a_1, \ldots, a_{t-1}$, $0 \leq a_j \leq p-1$, defining the random polynomial over Z_p, $f(x) = \sum_{j=0}^{t-1} a_j x^j$.
(3) T computes $S_i = f(i) \bmod p$, $1 \leq i \leq n$ (or for any n distinct points i, $1 \leq i \leq p-1$), and securely transfers the share S_i to user P_i, along with public index i.

Recovering the secret: To recover the initial secret S, a subgroup of at least t users should exchange their shares. After the exchange, each user of the subgroup will get t distinct points (i, S_i) of the polynomial f. These t points allow to calculate the coefficients of the polynomial f using the Lagrange interpolation as follows:

$$f(x) = \sum_{i=1}^{t} S_i \prod_{1 \leq j \leq t, j \neq i} \frac{x-j}{i-j}$$

Since $f(0) = a_0 = S$, the shared secret may be expressed as:

$$S = \sum_{i=1}^{t} c_i S_i, \quad \text{where } c_i = \prod_{1 \leq j \leq t, j \neq i} \frac{j}{j-1}$$

3. Related works

In this section we survey the most interesting public key-based trust models in MANETs, which we classify into two categories: partially and completely distributed models, as illustrated in Fig. 1.

3.1. *Partially distributed models*

Zhou and Haas (1999) proposed a partially distributed certification authority (CA) relying on threshold cryptography. The CA is distributed among particular nodes: servers, combiners, and a dealer. Servers and combiners sign public key certificates for users. The dealer is a special server which knows the CA's private key. For any joining node, if all partial signatures are collected, it can then compute the complete signature locally to obtain the complete public key certificate. Recently, Raghani et al. (2006) proposed a similar solution, in which they allow to dynamically adjust the value of the threshold when required, and thereby reduces the certification delays.

Yi and Kravets (2003) follows the same direction by building a distributed CA based on threshold cryptography. They improve security by secure and power selected nodes as MOCA servers (MObile Certification Authority) and reduce communication overhead by caching routes to MOCA servers. The system uses unicast instead of flooding when sufficient cached routes exist.

Luo et al. (2005) proposed DICTATE (Distributed CerTification Authority with probabilisTic frEshness for ad hoc networks). DICTATE uses a hierarchical CA between one mCA (mother CA) in wired network, and a group of dCA (distributed CA) in ad hoc network. Nodes in ad hoc network can collectively be isolated from the mCA, but always have the need for CA's services. The mCA delegates a group of dCA during the isolation period in order to ensure the availability of security services.

Zhang et al. (2006) proposed an ID-based key management system using threshold cryptography. The system is a "certificateless"-based model in which nodes' public keys are directly derivable from their known identifiers (IDs) plus some