Available online at www.sciencedirect.com

ScienceDirect

Computer Communications 30 (2007) 1498–1512

computer communications

www.elsevier.com/locate/comcom

Building a virtual hierarchy to simplify certification path discovery in mobile ad-hoc networks

Cristina Satizábal [a,b], Juan Hernández-Serrano [a], Jordi Forné [a], Josep Pegueroles [a,*]

[a] *Department of Telematics Engineering, Technical University of Catalonia, Jordi Girona 1-3 C3, 08034 Barcelona, Spain*
[b] *Department of Engineering and Architecture, Pamplona University, Km 1 via Bucaramanga, Pamplona, Colombia*

Received 25 July 2006; received in revised form 17 December 2006; accepted 29 December 2006
Available online 9 January 2007

Abstract

The ease with which nodes may join or leave a Mobile Ad-hoc Network (MANET) implies changing trust relationships among them and problems to build certification paths. Peer-to-peer Public Key Infrastructures (PKIs) are quite dynamic and certification paths can be built although part of the infrastructure is temporarily unreachable. However, path discovery is difficult because trust relationships are bidirectional. On the contrary, in hierarchical PKIs, there is only one path between two entities and certification paths are easy to find. We propose a protocol that establishes a virtual hierarchy in a peer-to-peer PKI. This protocol is suitable for dynamic environments such as MANETs since it is executed in a short time. In addition, our protocol does not require to issue new certificates among PKI entities, facilitates the certification path discovery process and the maximum path length can be adapted to the characteristics of users with limited processing and storage capacity.

Keywords: PKI; MANET; Hierarchical trust model; Peer-to-peer trust model

1. Introduction

Advances in wireless technology and portable computing along with demands for greater user mobility have provided a major impetus toward ubiquitous computing. Wireless networks provide mobile users with ubiquitous communicating capability and access to the information regardless of their location.

If we restrict ourselves to ground radio networks, we can define two basic types of wireless networks: cellular and multi-hop. In cellular radio networks mobile users communicate via a single hop wireless channel with a base station which is in turn connected to a wired backbone. In a multi-hop wireless network, in contrast, there are not fixed base stations connected to a wired network. Thus, all nodes communicate via the wireless channel with possible multi-hopping over several mobile stations. Examples of such networks are ad-hoc networks and packet radio networks.

Mobile ad-hoc networks (MANETs) are dynamic peer-to-peer networks that do not have a pre-existing infrastructure. This lack of fixed backbone means the absence of central administration, stable connection, control over the network principals and such. Consequently, mobile end-systems in an ad-hoc network are expected to act cooperatively to support all network functionalities. As a first approach, such functionalities are traffic routing and adaptation to the highly dynamic state of network links. These functionalities can also be extended to any service over the network, such as security. Since mobile devices are capable of forming an ad-hoc network on the fly, the existing security infrastructure of wired networks fails and demands dynamic security considerations, requiring as few assumptions as possible about the nature of the network.

Public Key Infrastructure (PKI) [1] can be used to provide the secure interchange of the information since it

[*] Corresponding author. Tel.: +34 934016012; fax: +34 934054264.
E-mail addresses: isabelcs@entel.upc.edu (C. Satizábal), jserrano@entel.upc.edu (J. Hernández-Serrano), jforne@entel.upc.edu (J. Forné), josep.pegueroles@entel.upc.edu (J. Pegueroles).

0140-3664/$ - see front matter © 2007 Elsevier B.V. All rights reserved.
doi:10.1016/j.comcom.2006.12.024

supports data integrity, confidentiality, strong authentication and non-repudiation. PKI uses Trusted Third Parties (TTPs), known as Certification Authorities (CAs) to digitally sign Public Key Certificates (PKCs), ensuring that a particular public key belongs to a certain user. In addition, the certificates allow establishing different trust relationships among the entities of the PKI. Thus, an entity can build certificate trust chains, known as certification paths, from its trusted CA to the other entities and verify the validity of the certificates.

However, PKI is mostly designed for centralized, wired and well-connected networks, so adopting PKI in MANETs is not an easy task since the network topology and resources can change frequently. Also, there is a high possibility that a node is compromised therefore some precautionary steps are needed to preserve the security of public key certificates. In addition, when CAs are not reachable, several PKI services, such as certification path processing and certificate status checking are not available.

Previous drawbacks are mainly overcome in MANETs by decentralizing CA functionalities and self-organized PKIs. In the latter, management of multiple trust relationships among PKI entities has to be taken into account, since nodes can dynamically create bidirectional trust relationships among them. In this scenario, certification path discovery becomes a difficult task because they can have multiple paths between two entities and all the options do not lead to the target entity.

Validation of long paths can also be hard for mobile devices with limited capacities from the computational point of view, since the public key algorithms require complex mathematics calculations, and considering the set of resources necessary to obtain, store and verify the certificates.

The purpose of our proposal is to take advantage of the efficiency in the path discovery process offered by hierarchical PKIs, where trust relationships are unidirectional and paths are easy to find. For that reason, our protocol establishes a virtual hierarchy among the entities of a peer-to-peer PKI and contributes to simplify the path discovery process. In a hierarchical model, there is only one path between two entities so the verifier must carry out less search operations to find a path than in a peer-to-peer architecture. Additionally, services based on hierarchical PKIs can be easily used. Also, since validation of long paths is difficult for verifiers with limited capacities, the hierarchy is built considering a maximum path length, whose value can be established taking into account the features of the users' terminals.

The different approaches that use PKI in MANETs are put forward in Section 2. Section 3 compares hierarchical and peer-to-peer trust models, and describes the certification path validation process. In Section 4, we present an example that shows the advantages of establishing a virtual hierarchy in a peer-to-peer PKI. Then, we describe the operation of our protocol in Section 5. Section 6 explains the reason for constructing the hierarchy from the leaves to the root instead of from the root to the leaves. In Section 7 we talk about the tools used to implement our protocol and the characteristics of the simulated environment. Section 8 contains the outcomes of the simulation. Finally, Section 9 concludes.

2. MANETS: Approaches to PKI

Node connectivity is not guaranteed in MANETs due to the limited-range and unreliability of wireless links. The absence of a routing infrastructure that assures connectivity of nodes precludes supporting a stable and long-term trust infrastructure, such as a hierarchy among subsets of network nodes. In addition, a single mobile node functioning as a CA will come to a halt the entire MANET if it moves out of the network and also can act as a single point of failure if it becomes compromised. Replicated CAs may be used to avoid this security bottleneck, but this solution is not scalable from administration perspectives and creates several points of failure if any CA node is compromised.

There are essentially two families of approaches for eliminating a centralized certification authority in a mobile ad-hoc network. The first consists in distributing the functionality of the certification authority among several nodes by threshold cryptography; and the second is based on a self-organized public-key infrastructure.

2.1. Distributed PKI with threshold cryptography

The ease with which nodes may join or leave a MANET shows that it is advisable to distribute the CA functionality among several nodes in the network rather than assign it to a single node. Using threshold cryptography, multiple trusted nodes are required to sign a certificate and an adversary would need to corrupt a large number of them before he/she can forge a certificate.

The fundamental problem of threshold cryptography is the secure sharing of a secret. A secret sharing scheme allows one to distribute a piece of secret information among several servers in a way that meets the following requirements: (1) no group of corrupt servers (smaller than a given threshold) can figure out what the secret is, even if they cooperate; (2) when it becomes necessary that the secret information be reconstructed, a large enough number of servers (a number larger than the above threshold) can always do it. Many existing threshold cryptosystems are based on Shamir's (k,n) secret sharing [2]. In these approaches, threshold cryptography is used for distributing the CA private key among n nodes, but the CA functionalities can be assumed by only k nodes ($k < n$). Thus, each time, k nodes collaborate to generate a signature. As these functionalities rely on the CA signature,[1] the goal is to distribute the signing power.

[1] Notice that the main functionality of a CA is to sign certificates.