Journal of Network and Computer Applications 62 (2016) 153–162

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

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

Secure and reliable certificate chains recovery protocol for mobile ad hoc networks

Mawloud Omar*, Hamida Boufaghes, Lydia Mammeri, Amel Taalba, Abdelkamel Tari

Laboratoire d'Informatique Médicale, Faculté des Sciences Exactes, Université de Bejaia, 06000 Bejaia, Algeria

ARTICLE INFO

Article history:
Received 12 April 2014
Received in revised form
28 July 2015
Accepted 6 January 2016
Available online 21 January 2016

Keywords:
Mobile ad hoc network
Certificate
Public-key
Web-of-trust

ABSTRACT

The deployment of any security policy requires the definition of a trust model that defines who trusts who and how. There is a host of research efforts in the trustworthy area to securing mobile ad hoc networks. Among the most used approaches are based on public-key certificates and gave birth to miscellaneous trust models ranging from centralized models to web-of-trust and distributed certification authorities. Certificates management in mobile ad hoc networks is a veritable challenge because of constrictions imposed by the nature of the network. The freedom of nodes mobility involves some constraints when designing reliable certification systems. In this paper, we address this issue and we propose a secure and reliable certificate chains recovery protocol for mobile ad hoc networks. Our proposal is based on web-of-trust in which the users ensure themselves the role of the certification service by issuing and managing the public-key certificates. The shortest and the safest certificate chains are selected in order to reduce the communication overhead and resist against compromised nodes which can generate false certificates. An analytical model is developed and simulations are performed in order evaluate the performances of our protocol, in which it demonstrates interesting results.

1. Introduction

Mobile ad hoc networking (Basagni et al., 2013) is one of the most important areas in the field of wireless communication. The premise of forming a mobile ad hoc network is to provide wireless communication among mobile devices anytime and anywhere with no infrastructure. These devices, such as cell phones, laptops, etc., carry out communication with other nodes that come in their radio range of connectivity. Each participating node provides services such as message forwarding, providing routing information, authentication, etc. with other nodes spread over an area. They are mostly employed in the military applications where their mobility is attractive, but have also a high potential for use in civilian applications such as coordinating rescue operations in the infrastructure-less areas, sharing content and network gaming in the intelligent transportation systems, surveillance and control in wireless sensor networks, etc.

The inherent vulnerability of mobile ad hoc networks introduces new security problems, which are generally more prone to physical security threats. The possibility of eavesdropping, spoofing, denial-of-service and impersonation attacks increase. Similar to the fixed networks, security of mobile ad hoc networks is considered from different points such as availability, confidentiality, integrity, authentication, non-repudiation and access control. However, the security approaches used to protect the fixed networks are not feasible due to the salient characteristics of mobile ad hoc networks. New threats, such as attacks raised from internal malicious nodes are hard to defend. The deployment of any security service requires the definition of a trust model that defines who trusts who and how. There are research efforts in the trust model framework for securing mobile ad hoc networks. In this paper, we focus on the category of certification-based trust models. The trust relationship among users is performed in a transitive manner, such that if A trusts B and B trusts C, then A can trust C. In this relationship, the principal B is called “trusted third party”. The latter could be a central authority (like CA – certification authority) or a simple intermediate user in the case of web-of-trust based models (Omar et al., 2012).

The certificate chain recovery based on the web-of-trust in highly dynamic networks, such as mobile ad hoc networks, involves two major challenges representing the main topic covered in this paper. The first problem is related to the credibility degree, which we should assign when evaluating the trust chains. This problem is specific to the web-of-trust based models, in which the users themselves, without being controlled by a central authority, establish the trust relationship propagation autonomously and in a transitive way. The transitive trust spread can cover compromised intermediate nodes, which could compromise the network security. The second problem is related to the

* Corresponding author: Tel.: +213(0)555150466.
E-mail address: mawloud.omar@gmail.com (M. Omar).

http://dx.doi.org/10.1016/j.jnca.2016.01.007
1084-8045/© 2016 Elsevier Ltd. All rights reserved.

certificate collection service availability, which is a specific problem to the imposed constraints by mobile ad hoc networks. Centralize certificate repositories on the servers could compromise the access availability, where the network is a subject of partitioning because of the mobility of nodes. Designing a distributed certificate collection protocol is crucial in order to overcome the availability problem, however, it opens for other issues relating to the capacity of nodes, which are constrained in terms of resources. Thus, three main criteria must be optimized, namely the computation load, the storage and the transmission.

In response to the challenges described above, we contribute through this work with a secure and reliable certificate recovery approach. The security aspect is addressed to answer the first challenge and we propose a trust chain selection mechanism based on the nodes credibility. The credibility of a node increases proportionally to the certificate number issued for that node. The proposed mechanism maximizes this criterion when selecting a trust chain in order to avoid compromised nodes to be considered. Therefore, we maximize the probability of successful signature verification of the certificate chain, and thus, decreasing the probability of reiterating the collection and verification process for another alternative chain. The reliability is addressed to answer the second challenge and we propose a negotiation protocol in order to collect information about “who trusts who”. A prior analysis relating to the trust chain length is performed before executing the certificate collection process. A high chain length involves a considerable communication overhead when collecting and an expensive computation load when verifying the signatures. The storage is reduced by keeping at each node only the certificates signed by or for the node in question. The set of required certificates is collected in a distributed manner when the authentication is required between two nodes.

Our proposal allows nodes to generate, store and distribute their public-key certificates without any central server or trusted party. All the nodes have a similar role and we do not assign special functions to specific nodes. The main motivation for employing this approach comes from the self-organized nature of mobile ad hoc networks and from the need to allow users to fully control the security settings in the network. Users public and private keys are created by the users themselves and key authentication is performed via chains of public-key certificates following the web-of-trust. Instead of storing certificates in centralized certificate repositories, certificates are stored and distributed by nodes themselves. The performance evaluation is done through both analytical modeling and simulations with comparison to concurrent approaches. The evaluated metrics are the certification success probability, the response time and the communication overhead. The certification success probability evaluates the safety metric of our protocol and it is performed through an analytical modeling using Markov chains. The response time and communication overhead evaluate the metric of the certificate chain length and are performed through simulations.

The remaining of this paper is structured as follows. In Section 2, we introduce the related work and we give a general presentation of our contributions. In Section 3, we give detailed description of our protocol. In Section 4, we present and discuss the results of performances evaluation in which we have developed both analytical model and simulations. We finally conclude this work in Section 5.

2. Related work

In the web-of-trust based models, there is no central authority. Each user acts as a certification authority independently of the other users in the network. This model is decentralized in nature and so is very adequate for mobile ad hoc networks. In this section we survey the most relevant web-of-trust based public-key certification protocols for mobile ad hoc networks, which are classified into two categories: proactive and reactive protocols. In the remaining of this section, we give descriptions of the protocols belonging to each category, an overall analysis and we summarize our contributions.

2.1. Proactive protocols

In this category of protocols, the process of certificate collection is executed systematically among neighboring nodes. Thus, when the node needs to verify a certificate, it is done instantly since the required chain of certificates could have been already retrieved from the network. Capkun et al. (2003) have proposed a fully and self-organized protocol, which requires no central authority. Each node in the network holds a certificate repository and the certificate collection process is executed in a proactive manner, in which the certificates are exchanged among neighbor nodes at each direct contact. When a node needs to authenticate the public-key of another node, both nodes merge their local repositories and try to find a certificate chain from the one to the other. Ren et al. (2004) have proposed a modified version of the protocol of Capkun et al. by introducing a boot server to initialize the system. The boot server computes and distributes to each node a short list with a set of bindings (nodes identifiers and public-keys). Then, each node stores it locally and generates the corresponding certificates. Thus, a web-of-trust is formed and the system becomes fully distributed, where the nodes authenticate themselves through certificate chains. Omar et al. (2009) have introduced a threshold scheme within the web-of-trust. During the network initialization, nodes share the system private-key and each node holds one private-share. Instead of using the private-key for certificate signing, a node uses its private-share. Each node in the network maintains a partial view of the web-of-trust, which is updated systematically through partial certificate exchanging protocol among neighboring nodes. The public-key authentication among nodes is performed via the combination of the partial certificate chains.

2.2. Reactive protocols

In this category of protocols, the certificate collection process is executed on-demand. When the node needs to verify a public-key, it collects the appropriate chain of certificates in a distributed manner from the network. Funabiki et al. (2006) have proposed a centralized protocol based on clustering. The certificate issuance is ensured by the nodes themselves, however they are stored at a particular node named CMN (certificate management node) in each cluster. All the cluster nodes should request the CMN to collect the required certificates in order to verify the trust chain. Kitada et al. (2005a,b) have proposed a distributed protocol, where each node holds a local repository that contains the node's certificates signed by some other nodes and certificates delivered by the node itself for the other nodes. When a node needs to verify the public-key of another node, it broadcasts a search request to the nodes that it directly trusts. Each intermediate node includes its own certificate in the request. Finally, the destination node adds its own certificate and sends to the source node the certificate chain. Hisham and James (2009) have proposed a modified version of the protocol of Kitada et al., in which upon receiving the different certificate chains, the source node proceeds to verify the shortest chain in order to minimize the computation overhead. Kambourakis et al. (2010) have considered that the web-of-trust has the form of a binary tree. Hence, in order to respect the tree structure, each node in the network is certified by only one of its neighboring nodes and it certifies at the maximum to two of its neighboring nodes. Xia et al. (2004) have proposed a certification protocol executed by the nodes themselves. Each node that first joins the network performs a