Journal of Network and Computer Applications 35 (2012) 268–286

Contents lists available at SciVerse ScienceDirect

Journal of Network and Computer Applications

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

Review

Certification-based trust models in mobile ad hoc networks: A survey and taxonomy

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

[a] Université A/Mira, ReSyD, Bejaia, Algeria
[b] Université de Technologie de Compiègne, Heudiasyc-UMR CNRS 6599, Compiègne, France

ARTICLE INFO

Article history:
Received 14 March 2011
Received in revised form
11 July 2011
Accepted 23 August 2011
Available online 1 September 2011

Keywords:
Trust
Public-key
Certificate
Security
Mobile ad hoc networks

ABSTRACT

A mobile ad hoc network is a wireless communication network which does not rely on a pre-existing infrastructure or any centralized management. Securing the exchanges in such network 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. There is a host of research efforts in trust models framework to securing mobile ad hoc networks. The majority of well-known approaches is based on public-key certificates, and gave birth to miscellaneous trust models ranging from centralized models to web-of-trust and distributed certificate authorities. In this paper, we survey and classify the existing trust models that are based on public-key certificates proposed for mobile ad hoc networks, and then we discuss and compare them with respect to some relevant criteria. Also, we have developed analysis and comparison among trust models using stochastic Petri nets in order to measure the performance of each one with what relates to the certification service availability.

Contents

* Corresponding author. Tel.: +213 661 73 45 30.
E-mail address: mawloud.omar@gmail.com (M. Omar).

1084-8045/$ - see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jnca.2011.08.008

1. Introduction

Mobile ad hoc networking (Perkins, 2000; Wu and Tseng, 2007) is emerging as an important area for new developments in the field of wireless communication. The premise of forming a mobile ad hoc network is to provide wireless communication between heterogeneous devices, anytime and anywhere, with no infrastructure (Lauter, 2004; Mishra and Nadkarni, 2002; Papadimitratos and Haas, 2002). These devices, such as cell phones, laptops, palmtops, 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. to form a network with other nodes spread over an area. With the proliferation of mobile computing, 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 (Plesse et al., 2005) where their mobility is attractive, but have also a high potential for use in civilian applications such as coordinating rescue operations in infrastructure-less areas (Calafate et al., 2007), sharing content and network gaming in intelligent transportation systems, surveillance and control using wireless sensor networks (Yick et al., 2008), etc.

Inherent vulnerability of mobile ad hoc networks introduce new security problems, which 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 mobile 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 mobile ad hoc networks. New threats, such as attacks raised from internal malicious nodes, are hard to defend (Deng et al., 2002). The deployment of any security service requires the definition of a trust model that defines who trusts who and how. There are recent research efforts in trust models framework to securing mobile ad hoc networks. There exist two main approaches: (1) cooperation enforcement trust models (Buchegger and Le-Boudec, 2002; Michiardi and Molva, 2002; Janzadeh et al., 2009; He et al., 2004; Zouridaki et al., 2009; Ayday and Fekri, 2010; Marchanga and Dattab, 2008; Luoa et al., 2009; Boukerch et al., 2007; Liu and Lia, 2010), and (2) certification-based trust models (Zhou and Haas, 1999; Capkun et al., 2002, 2003; Raghani et al., 2006; Yi and Kravets, 2003; Luo et al., 2005; Ge et al., 2009; Kitada et al., 2005a; Kambourakis et al., 2010; Satizabal et al., 2007). In Table 1, we present the major differences between cooperation enforcement trust models and certification-based trust models.

The first trust models category is based basically on reputation among nodes. The reputation of a node increases when it carries out correctly the tasks of route construction and data forwarding. The models of this category support effective mechanisms to measure the reputation of other nodes of the network. They also incorporate techniques that isolate the misbehaving nodes that are those that show a low reputation value. Trust models based on cooperation enforcement are well surveyed in the literature. Marias et al. provided such a thorough survey of cooperation enforcement trust models in Marias et al. (2006). In this paper, we are interested in the category of certification-based trust models. Indeed, in this category, the trust relationship among users is performed in a transitive manner, such that if $\mathcal{A}$ trusts $\mathcal{B}$, and $\mathcal{B}$ trusts $\mathcal{C}$, then $\mathcal{A}$ can trust $\mathcal{C}$. In this relationship, the principal $\mathcal{B}$ is called Trusted Third Party (TTP). The latter could be a central authority (like CA – Certification Authority) or a simple intermediate user. Both points of view gave birth to two categories of models: (a) Authoritarian models, and (b) Anarchic models. In this paper, we review and classify the existing certification-based trust models belonging to each category. Moreover, to determine the efficiency of a given trust model, it is very important to estimate the certification service availability with respect to mobile ad hoc networks configuration. Therefore, we have modeled the certification process of each surveyed trust model using stochastic Petri nets (SPN) (Haas, 2002, 2007). As you will see in the following sections, this allows a better understanding of the

Table 1
Cooperation enforcement vs. certification-based trust models.

Trust metrics	Cooperation enforcement trust models	Certification-based trust models
Trust degree $\mathcal{T}$	Variable according to the node's behavior, such $\mathcal{T} \in]0,1[$	Decided in a strict manner: trusted or untrusted, such $\mathcal{T} \in \{0,1\}$
How to evaluate the trust degree of a new member node?	Supposed as a trusted node, then its trust degree will be updated according to its behavior	Offline authentication through the policy of certification
How to evaluate the trust degree of a given node at the first interaction?	Through the recommendation of its neighbor nodes	Through the certificates chain verification from a trusted party to the node
Node exclusion	The node will be isolated if the value of its trust degree decreases at a certain threshold	Through the revocation of its certificate