Ad Hoc Networks 44 (2016) 58–75

Contents lists available at ScienceDirect

Ad Hoc Networks

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

Trust threshold based public key management in mobile ad hoc networks

Jin-Hee Cho[a,*], Ing-Ray Chen[b], Kevin S. Chan[a]

[a] U.S. Army Research Laboratory, Adelphi, MD 20783, USA
[b] Department of Computer Science, Virginia Tech, Falls Church, VA 22043, USA

ARTICLE INFO

Article history:
Received 5 October 2015
Revised 14 January 2016
Accepted 21 February 2016
Available online 2 March 2016

Keywords:
Public key management
Mobile ad hoc networks
Trust
Private key
Public key
Certificate authority

ABSTRACT

Public key management in mobile ad hoc networks (MANETs) has been studied for several decades. However, the unique characteristics of MANETs have imposed great challenges in designing a fully distributed public key management protocol under resource-constrained MANET environments. These challenges include no centralized trusted entities, resource constraints, and high security vulnerabilities. This work proposes a fully distributed trust-based public key management approach for MANETs using a soft security mechanism based on the concept of trust. Instead of using hard security approaches, as in traditional security techniques, to eliminate security vulnerabilities, our work aims to maximize performance by relaxing security requirements based on the perceived trust. We propose a composite trust-based public key management (CTPKM) with the goal of maximizing performance while mitigating security vulnerability. Each node employs a trust threshold to determine whether or not to trust another node. Our simulation results show that an optimal trust threshold exists to best balance and meet the conflicting goals between performance and security, by exploiting the inherent tradeoff between trust and risk. The results also show that CTPKM minimizes risk (i.e., information leakout) using an optimal trust threshold while maximizing service availability with acceptable communication overhead incurred by trust and key management operations. We demonstrate that CTPKM outperforms both existing non-trust-based and trust-based counterparts.

Published by Elsevier B.V.

1. Introduction

In resource-constrained mobile ad-hoc networks (MANETs), it is inefficient to employ cryptographic techniques for key management due to high computation and communication overhead as well as network dynamics that could require frequent key reassignments. In addition, the unique nature of MANETs does not allow any centralized trusted certificate authority (CA) to deal with all key management operations, including key generation, distribution, update, and revocation. Essentially, it is infeasible to build a system using hard security approaches (e.g., encryption or authentication techniques) to meet the dual goals of performance (i.e., efficiency) and security due to the inherent tradeoff. In this work, we take a soft security approach by applying the concept of trust to meet both performance and security requirements.

The concept of "trust" originally is derived from social science and defined as the degree of a subjective belief about the behaviors of a particular entity [1]. Blaze et al. [2] first introduced the term "trust management" and identified it as a separate component of security services in networks. They explained that "Trust management provides a unified approach for specifying and interpreting security policies, credentials, and relationships." Trust management in MANETs is needed when participating

* Corresponding author. Tel.: +1 301 394 0492.
E-mail addresses: jinhee.cho@us.army.mil (J.-H. Cho), irchen@vt.edu (I.-R. Chen), kevin.s.chan@us.army.mil (K.S. Chan).

http://dx.doi.org/10.1016/j.adhoc.2016.02.014
1570-8705/Published by Elsevier B.V.

nodes, without any previous interactions, desire to establish a network with an acceptable level of trust relationships among themselves.

Trust management, including trust establishment, trust update, and trust revocation, in MANETs is more challenging than in traditional centralized environments [3]. First of all, collecting trust evidence to evaluate trustworthiness is difficult due to topology changes caused by node mobility/failure. Further, resource constraints often confine trust assessment process only to local information. The dynamic nature and characteristics of MANETs result in uncertain, incomplete trust evidence, which is continuously changing over time [3,4]. Cho et al. [5] comprehensively surveyed trust management in MANETs recognizing that trust originates from various domains including psychology, sociology, economics, philosophy, organizational theory, and so on. Cho et al. [5] suggested that the following properties be considered when designing trust-based MANET protocols: (1) potential risk; (2) context-dependency; (3) each party's own interest (e.g., utility/payoff based on rational selfishness); (4) learning based on cognition/experience; and (5) system reliability.

Trust management has diverse applicability in many decision making situations including intrusion detection [6,7], authentication, access control, key management, isolating misbehaving nodes for effective routing [6,8,9], and many other purposes [9]. In addition, the concept of multidimensional trust recently has been explored in networking and computing research areas and applied in various security services [6,7,10–13]. Bao et al. [6,7] proposed trust-based secure routing and intrusion detection mechanisms for wireless sensor networks by considering multiple dimensions of trust. Cho et al. [10,11] and Chen et al. [12] proposed trust management protocols for MANETs or delay tolerant networks considering multiple trust components. However, the above works [6,7,10–12] did not consider trust-based public key management while assuming a pre-loaded private/public key pair in each node. Very recently Mahmoud et al. [13] proposed trust-based secure and reliable routing for heterogeneous multihop wireless networks where competence and reliability of a node are estimated and used to derive the node trust level that can be used in routing decisions. However, Mahmoud et al. [13] assumed the existence of a centralized offline trusted party to deal with public key management including issuance, distribution, and update of a public/private key pair to nodes in the network. Our work uses distributed peer-to-peer trust evaluation for public key management using three trust dimensions capturing the unique aspects of trust in a MANET.

In this paper, we propose a composite trust-based distributed key management algorithm (CTPKM) for MANETs without using a centralized trusted CA. Our approach falls under the category of certificate-based public key management. The proposed protocol is designed to meet a required level of security (e.g., the fraction of valid, correct and uncompromised public keys, and information risk) as well as to meet performance requirements (e.g., service availability and communication overhead), without relying on trusted third parties such as CAs. The proposed protocol aims to achieve: (a) resiliency against misbehaving nodes in the network to maintain minimum security vulnerability; (b) availability in service provision in the presence of compromised nodes; and (c) efficiency in minimizing communication overhead incurred by trust and key management operations. CTPKM satisfies the requirements of self-organized and distributed key management for MANETs as discussed in [14]: (a) no single point of failure, i.e., no trusted third party is required; (b) resilience with low security vulnerability in the presence of hostile entities, i.e., little exposure of a compromised key; (c) high service availability, i.e., a sufficient number of valid, correct public keys are kept in each node; and (d) scalability, i.e., low communication overhead for obtaining a valid/correct public key whose corresponding private key is not compromised.

The contributions of our work are as follows:

1. Relative to existing non-trust-based distributed key management algorithms for MANETs without using a centralized trusted [15–19], our contribution is to develop a composite trust-based distributed key management algorithm (CTPKM) that allows each node to make local peer-to-peer trust assessment for distributed decision making based on a composite trust metric. We consider multiple dimensions of trust (i.e., competence, integrity, and social contact) that are estimated based on evidence derived from the characteristics of communication, information, and social networking in a MANET. This allows fast and safe propagation of the keys to trustworthy nodes for preserving quality-of-service (QoS).
2. Relative to existing trust-based distributed key management algorithms for MANETs without using a centralized trusted CA [20–24], our contribution is to develop a threshold-based filtering mechanism that can effectively exploit the inherent tradeoff between trust and risk. The end result is that CTPKM is able to identify the optimal trust threshold to be applied at runtime for differentiating trustworthy vs. untrustworthy nodes to maximize key management service availability.
3. We conduct a comprehensive performance analysis comparing CTPKM with both non-trust-based and trust-based counterparts. We demonstrate that CTPKM outperforms a non-trust-based baseline model and two existing trust-based key management schemes [20,21], and can identify an optimal operational setting meeting dual conflicting goals of performance and security.

The rest of the paper is organized as follows. Section 2 discusses related work. Section 3 describes the system model including the attack model, trust model, protocol description, and performance metrics. Section 4 conducts a comparative performance analysis and reports numerical results. Section 5 concludes our paper and suggests future work.

2. Related work

In this section, we discuss existing work in certificate-based public key management for MANETs, and compare