Contents lists available at ScienceDirect

Ad Hoc Networks

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

E-Hermes: A robust cooperative trust establishment scheme for mobile ad hoc networks

Charikleia Zouridaki [a], Brian L. Mark [a,*], Marek Hejmo [a], Roshan K. Thomas [b]

[a] Department of Electrical and Computer Engineering, George Mason University, Fairfax, VA 22030, USA
[b] SPARTA, Inc., 5875 Trinity Parkway, Suite 300, Centreville, VA 20120, USA

ARTICLE INFO

Article history:
Received 29 December 2006
Received in revised form 6 October 2008
Accepted 8 October 2008
Available online 22 October 2008

Keywords:
Security
Trust establishment
Reliability
Performance
Routing

ABSTRACT

In a mobile ad hoc network (MANET), a source node must rely on intermediate nodes to forward its packets along multi-hop routes to the destination node. Due to the lack of infrastructure in such networks, secure and reliable packet delivery is challenging. We propose a robust cooperative trust establishment scheme to improve the reliability of packet delivery in MANETs, particularly in the presence of malicious nodes. In the proposed scheme, each node determines the trustworthiness of the other nodes with respect to reliable packet forwarding by combining first-hand trust information obtained independently of other nodes and second-hand trust information obtained via recommendations from other nodes. First-hand trust information for neighbor nodes is obtained via direct observations at the MAC layer whereas first-hand information for non-neighbor nodes is obtained via feedback from acknowledgements sent in response to data packets. The proposed scheme exploits information sharing among nodes to accelerate the convergence of trust establishment procedures, yet is robust against the propagation of false trust information by malicious nodes. We present simulation results which demonstrate the effectiveness of the proposed scheme in a variety of scenarios involving nodes that are malicious with respect to both packet forwarding and trust propagation.

© 2008 Elsevier B.V. All rights reserved.

1. Introduction

In recent years, there has been considerable interest in the topic of trust establishment for ad hoc networks. Trust establishment is an important and challenging issue in the security of ad hoc networks [1]. The lack of infrastructure in a mobile ad hoc network (MANET) makes it difficult to ensure the reliability of packet delivery over multi-hop routes in the presence of malicious nodes acting as intermediate hops. In this paper, we present a robust, cooperative trust establishment scheme, called *E-Hermes* (Extended-Hermes), which enables a given node to identify other nodes in terms of how "trustworthy" they are with respect to reliable packet delivery. The proposed scheme is cooperative in that nodes exchange information in the process of computing trust metrics with respect to other nodes. At the same time, the scheme is robust in the presence of malicious nodes that propagate false trust information.

The proposed scheme extends our earlier work on *Hermes* [2], a trust establishment framework that incorporates a Bayesian approach for trust computation as well as the notion of confidence, based on first-hand observations of packet forwarding behavior obtained by neighbor nodes. In Hermes, trust establishment of non-neighbor nodes relies on the second-hand trust information obtained from the propagation of recommendations. This approach is vulnerable to attacks by nodes that propagate erroneous trust information in the network. The trust establishment scheme proposed in the present paper avoids such attacks by extending the notion of first-hand evidence among

[*] Corresponding author. Tel.: +1 703 993 4069; fax: +1 703 993 1601.
E-mail addresses: charikleia@gmail.com (C. Zouridaki), bmark@gmu.edu (B.L. Mark), mhejmo@gmail.com (M. Hejmo), roshan.thomas@sparta.com (R.K. Thomas).

1570-8705/$ - see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.adhoc.2008.10.003

neighbor nodes to non-neighbor nodes by employing a secure acknowledgement protocol.

The main contribution of the present paper[1] is a trust establishment scheme for MANETs, which addresses the propagation of false trust information with respect to packet forwarding behavior. The proposed E-Hermes scheme obtains first-hand trust information with respect to non-neighbor nodes and combines this information with second-hand trust information to accelerate the establishment of trust in an ad hoc network. The key novel components of the proposed trust establishment scheme are an acknowledgement scheme for first-hand trust information with respect to non-neighbor nodes and a recommendation scheme that is robust against the propagation of false trust information by malicious nodes. The proposed scheme, in conjunction with a routing protocol based on the computed trust metrics should lead to improved packet delivery in the presence of misbehaving nodes.

The remainder of the paper is organized as follows: Section 2 reviews related work on trust establishment in ad hoc networks and sets the context for the present paper. Sections 3 and 4 discuss the core concepts and advances of the paper. Section 5 addresses the security properties of the proposed trust establishment scheme. Section 6 presents results from simulation experiments that demonstrate the robustness and key properties of the proposed scheme. Finally, the paper is concluded in Section 7.

2. Background and scope of work

2.1. Related work

In recent years, there has been considerable interest in the topic of trust establishment for ad hoc networks. The authors of [1] present a high-level framework for generation, revocation and distribution of trust evidence and demonstrate the significance of estimation metrics in trust establishment. A mechanism for trust evidence dissemination based on a model of ant behavior is proposed in [4] along the lines suggested in [1]. Others have approached trust establishment based on the use of a Bayesian framework [5,2]. In this framework, a random variable that follows the beta distribution is associated with the trust value of a node. Also, the posterior distribution that represents a notion of trust is derived from a prior distribution. The Bayesian approach was initially explored in [5]. The Hermes scheme presented in [2] builds on the Bayesian approach by incorporating the notion of statistical confidence associated with a trust value.

In [6], a trust model is presented that allows the evaluation of the reliability of the routes, using only first-hand information. The notion of confidence as it relates to trust management was explored in [7] and a semi-ring approach was suggested to evaluate trust and confidence along network paths. In [8], a framework for stimulating cooperation in MANETs is proposed. The approach is based on a credit system for packet forwarding while trusted hardware is assumed. The goal of collaboration is also pursued in [9], which proposes a trust management model, whereby each node carries a portfolio of credentials, which it uses to prove its trustworthiness. An autonomous trust establishment framework is proposed in [10,11], which relies on the introduction of pre-trusted agents and a public key infrastructure.

2.2. Hermes framework

The Hermes framework for trust management introduced in [2] maps trust and confidence into a new composite metric, called “trustworthiness”, which can be more easily used for making network decisions such as route selections. Furthermore, Hermes deals directly with the issue of how evidence can be collected from the network to establish and update trust. The work in [6] uses only first-hand information, while Hermes incorporates third-party information to derive the notion of an opinion that a given node has for any other node. While many of the works deal with qualitative or abstract notions of trust, the Hermes framework provides metrics and mechanisms for establishing trust quantitatively with respect to the objective of reliable packet delivery.

The majority of papers related to MANET security focus on securing the route discovery phase of an ad hoc routing protocol. By contrast, the Hermes framework is intended to provide the means to thwart a class of attacks on packet delivery in MANETs during the data transmission phase rather than the route discovery phase. Most of the well-known MANET routing attacks discussed in the literature, such as the wormhole and Sybil attacks, are attacks on the route discovery phase of a routing protocol. Various authors have proposed schemes for avoiding such attacks [12,13] in the route discovery phase.

The Hermes scheme is needed because even if routes are discovered correctly by means of a secure routing protocol, nodes can misbehave during the data transmission phase even if the route is a valid one. Most of the secure routing protocols in the recent literature do not deal with such attacks that occur during the data transmission phase, i.e., packet dropping and packet misforwarding. Moreover, an insider node may behave correctly during the route discovery phase, but then begin misbehaving during the data transmission phase. Secure routing protocols generally do not provide any defense against such attacks.

2.3. Overview of Hermes trust establishment

The notion of trust and trust relationships have been studied extensively in the literature [14]. Associated with the notion of trust is confidence, which is a measure of the level of assurance in the trust relationship. It is helpful to combine trust and confidence into a composite notion called *trustworthiness* [2] as it makes trust-related computations more straightforward. We apply all these notions to the problem of reliable packet delivery in MANETs. First-hand information on packet delivery is what can be directly observed by the sender in a path, whereas second-hand information is obtained via third parties. The literature discusses the conveyance of second-hand information through a variety of schemes such as recommendations [6,15–18]. In

[1] A preliminary version of this work was presented in [3].

Download English Version:

https://daneshyari.com/en/article/446318

Download Persian Version:

https://daneshyari.com/article/446318

Daneshyari.com