Journal of Network and Computer Applications 62 (2016) 112–127

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

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

Light-weight trust-enhanced on-demand multi-path routing in mobile ad hoc networks

Hui Xia [a,b,c,*], Jia Yu [a], Cheng-liang Tian [a], Zhen-kuan Pan [a,c], Edwin Sha [d]

[a] College of Computer Science and Technology, Qingdao University, Qingdao 266071, PR China
[b] Shandong Provincial Key Laboratory of Software Engineering, Shandong University, Ji'nan 250101, PR China
[c] Postdoctoral Research Station of System Science, College of Automation and Electrical Engineering, Qingdao University, Qingdao 266071, PR China
[d] Department of Computer Science, University of Texas, Dallas, TX 75083-0688, USA

ARTICLE INFO

Article history:
Received 21 February 2015
Received in revised form
12 December 2015
Accepted 23 December 2015
Available online 1 January 2016

Keywords:
Decentralized trust inference model
Trust attributes
Fuzzy AHP
Light-weight trust-enhanced routing protocol
Data-driven route maintenance mechanism
Attack resistance
Malicious node detection

ABSTRACT

Mobile ad hoc networks (MANETs) are originally designed for a cooperative environment, which are vulnerable to a wide variety of attacks due to their intrinsic characteristics. Trust can be introduced to address this security issue at some level. In this paper, we focus on the concept of trust and abstract a decentralized trust inference model, where the trust an entity has for a neighbor forms the basic building block of this model. Basing on the interest entity's historical behaviors, multi-dimensional trust attributes are incorporated to reflect trust relationship's complexity in various angles. The weight vector of attributes is calculated by fuzzy AHP scheme based on entropy weight measure. The trust inference framework provides the considerable security with an additional small overhead, which can be incorporated into any routing protocol. In this paper, the standard Ad hoc On-demand Multi-path Distance Vector protocol (AOMDV) is extended as the base routing protocol to evaluate this model. The proposed light-weight trust-enhanced routing protocol (TeAOMDV) can provide a feasible approach to choose an optimal two-way trusted route without containing the untrust worthy entities instead of the shortest route, thus mitigate the impairment effects from such entities. It is light-weight in the sense that the trust framework uses only passive and local monitoring information to evaluate the behaviors of an interest entity which is translated to an estimate of the trust, consumes limited computational resource. Moreover, the new proposed data-driven route maintenance mechanism reduces routing overhead and route discovery frequency. The simulations show that the proposed routing scheme behaves better in attack resistance (i.e., gray-hole attack and black-hole attack), and makes an improvement on the packets delivery ratio, routing packets overhead, route discovery frequency and malicious node detection. Finally, as an extension of the trust model, by utilizing the trust assessment data sequence, we propose an improved SCGM(1,1)-Markov chain prediction method based on the system cloud gray model and Markov stochastic chain theory to forecast entity's trust level for future decision making.

1. Introduction

In the last decade, researchers have explored many potential applications of mobile ad hoc networks (MANETs), which are usually deployed in harsh or uncontrolled environments. Due to the intrinsic characteristics (e.g., wireless medium, openness, the absence of a fixed infrastructure), such networks are vulnerable to a wide variety of attacks. Routing is a very important function in MANETs, which is productive unless all component nodes operate by a trustworthy manner. However, this is not always the case. The protocols used in this function are designed for minimizing the level of overhead and allowing every node to participate in the routing process, while usually not designed with security in mind and often are very vulnerable to node misbehaviors. Moreover, making routing protocols efficient often increases the security risk of the protocol and allows a single node to significantly impact the operation of the protocol because of the lack of protocol redundancy. An adversary or a malicious node can easily launch attacks on this important function, especially attacks on the packet routing (e.g., gray-hole, black-hole, cheating, or modification attack). The normal communications in network may be prohibited or hindered due to these attacks. The distribution of false routing information may cause the potential of denial of service attacks, unintended network routing loops, or other nonfunctional routes. Therefore, the security of routing protocol is an important area

* Corresponding author at: College of Computer Science and Technology, Qingdao University, Qingdao 266071, PR China.

http://dx.doi.org/10.1016/j.jnca.2015.12.005
1084-8045/

that needs to be addressed for such networks to widespread adoption.

To address the above issues, a variety of security-considered routing protocols have been proposed. The motivation of designing these protocols is that the networks need to determine the validity and safety of routing information prior to making routing decisions (Govindan and Mohapatra, 2012). Basing on the protection way of reducing or eliminating malicious attacks, these protocols can be classified into two types, secure routing protocol and trust-based routing protocol. Most of the secure routing protocols use cryptographic primitive techniques to secure the routing information. However, the disadvantage of using cryptographic tools is that the computational resource is very expensive, which is not suitable to be used in the resource-constrained mobile devices. These protocols create new avenues for denial of service (DoS) attacks in the attempt to prevent some other attacks (Li et al., 2012; Wang et al., 2011). Besides, several such secure routing protocols presume the existence of a centralized or distributed trusted third party, while this party actually violates the nature of self-organization (Wang et al., 2011). Moreover, such protocols usually cannot against or prevent the malicious attacks from malicious or compromised nodes which have been authorized as the participants in network from doing misbehaviors. Thus, it is becoming more acceptable to consider trust-based routing as a viable security solution. Such protocols attempt to establish trusted routes rather than shortest routes as is done in traditional routing protocols, which make tradeoff between the trustworthiness and the performance of networks. The establishment of such protocols contains two important segments, trust model and trust-enhanced routing strategy. Every node in the network independently executes a designed trust model. The task of trust model is to periodically quantify and establish the trustworthiness among entities based on some trust metrics or trust computational methods (Govindan and Mohapatra, 2012; Li et al., 2012; Wang et al., 2011; Liang and Shi, 2008; Xia et al., 2013a, 2013b; Velloso et al., 2010; Cho et al., 2011; Cho and Chen, 2013; Carullo et al., 2013; Elgohary et al., 2014; Onolaja et al., 2011). The estimated trust value can be directly applied to ensure proper operations, such as routing decision, authentication, access control, malicious node detection, and intrusion detection system (Deb and Chaki, 2012) (e.g., basing on the trust feedback information obtained from the trust inference model, the network participants could be reminded to participate in the network transaction with caution, the selection of next hops or forwarding paths). However, introducing the 'trust' will increase much excessive overhead. Therefore, the design principle for trust-based routing protocol in MANETs should be simple, effective, and with a low communication cost.

In this paper, we focus on the security of routing protocol in MANETs. Firstly, we abstract a decentralized trust inference model. Then by extending the standard Ad hoc On-demand Multi-path Distance Vector protocol (AOMDV), we propose a novel light-weight trust-enhanced routing protocol combined with the trust model, named as TeAOMDV. The persuasive experiments have been conducted to simulate and present the effectiveness of this new protocol.

The main technical contributions of our work are summarized as follows:

1. We firstly give the definition and derivation of trust, then abstract a decentralized trust inference model, where the trust an entity has for an interest neighbor forms the basic building block of this model. Basing on the interest entity's historical behaviors, multi-dimensional trust attributes are incorporated to reflect trust relationship's complexity in various angles. The weight vector of attributes is calculated by fuzzy AHP scheme based on entropy weight measure.
2. The standard Ad hoc On-demand Multi-path Distance Vector protocol (AOMDV) is extended as the base routing protocol to evaluate the proposed trust model. In the trust-enhanced routing strategy, *Hop Count*, *Forward Path Trust* and *Reverse Path Trust*, the three metrics compose a three-dimensional evaluation vector for routing decision which provides a flexible and feasible approach to establish multiple two-way trusted paths without containing the untrustworthy entities instead of the shortest route.
3. This new protocol (TeAOMDV) is light-weight, containing three layers of meaning: (1) the intrusion detection system (IDS) used for estimating the trust that one entity has for another, consumes limited computational resource; (2) the trust framework uses only passive and local monitoring information to evaluate the behaviors of an interest entity which is translated to an estimate of the trust; (3) the new proposed data-driven route maintenance mechanism, termed as path trust alert mechanism, reduces routing overhead and route discovery frequency.
4. The simulations show that the proposed routing scheme behaves better in attack resistance and makes an improvement on the packets delivery ratio, routing packets overhead, route discovery frequency and malicious node detection. There is a tradeoff between route optimality and route credibility. Moreover, at the same time, the simulation results prove that the recommendation mechanism does play an important role in trust assessment.
5. As an extension of our trust model, by utilizing the trust assessment data sequence, we propose an improved SCGM(1,1)-Markov chain prediction method based on the system cloud gray model and Markov stochastic chain theory to forecast entity's trust level for future decision making.

The remaining paper is organized as follows. Section 2 discusses the literature work. In Section 3, we describe our decentralized trust inference model in detail. Basing on the proposed trust framework, in Section 4, we propose a novel light-weight trust-enhanced routing protocol, named as TeAOMDV. Section 5 presents the experiments and analysis on the performance of the new protocol. We make a detailed analysis of our model in Section 6. As an extension of our trust model, we propose an improved SCGM(1,1)-Markov chain prediction method in Section 7. Finally, Section 8 gives the concluding remarks along with extensions and directions for future research.

2. Related work

Over the last few years, a number of trust-based schemes, trust-based systems and trust-based applications have been developed. As we are planning on adopting trust in MANETs, we firstly focus our attention on some trust models, and subsequently do a deep research on the modifications of routing strategy proposed in trust-based routing protocols.

2.1. Trust models in MANETs

By analyzing the existing trust models, we can see that although a lot of work has been done on the trust quantification, the research on trust is far from enough. A detailed survey on various trust computing approaches was presented (Govindan and Mohapatra, 2012). The summary and comparisons of these approaches were highlighted. The following contents are some efficient schemes used for estimating trust in MANETs found in the different references.

Observing a node's historical behaviors (e.g., packets delivery ratio, fully cooperation, bandwidth, residual energy and CPU