Journal of Network and Computer Applications 34 (2011) 1138–1149

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

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

Building a trusted route in a mobile ad hoc network considering communication reliability and path length

Jian Wang [a,b], Yanheng Liu [a,b,*], Yu Jiao [a,b]

[a] College of Computer Science and Technology, Jilin University, Changchun 130012, China
[b] Key Laboratory of Symbolic Computation and Knowledge Engineering of Ministry of Education, Jilin University, Changchun 130012, China

ARTICLE INFO

Article history:
Received 13 March 2010
Received in revised form
21 October 2010
Accepted 18 November 2010
Available online 26 November 2010

Keywords:
Mobile ad hoc network
Trusted routing
Trust degree
Attribute similarity

ABSTRACT

In a mobile ad hoc network (MANET), a source node must rely on other nodes to forward its packets on multi-hop routes to the destination. Unlike most previous studies that sought only the shortest path, our study proposes a novel trusted route that considers communication reliability and path length for a reliable and feasible packet delivery in a MANET. In most MANET routing schemes, security is an added layer above the routing layer. We introduce the concept of attribute similarity in finding potentially friendly nodes among strangers; so security is inherently integrated into the routing protocol where nodes evaluate trust levels of others based on a set of attributes. Unlike the fixed probability of dropping packets adopted in other routing mechanisms, our new forwarding rule is designed based on the attribute similarity and provides a recommended method in calculating the degree of similarity between attributes. The simulations show that the proposed routing scheme behaves better than the Dynamic Source Routing (DSR) protocol in warding off blackhole and changing behavior attacks and that it is unaffected by slander attacks. We also investigate the effects of transmission range, velocity, and number of nodes on routing performances.

1. Introduction

The past decade has witnessed the emergence of a mobile ad hoc network (MANET). Routing security problems in MANETs have hindered the development and deployment of these networks (Marti et al., 2000; Sonja and Boudec, 2002; Lee et al., 2009; Martignon et al., 2009; Gobel et al., 2009; Catanuto et al., 2009; Yu and Leung, 2009; Agrawal and Patwari 2009; Kang et al., 2010). A MANET has several special properties: network topologies and memberships are constantly changing, and no predefined trust exists between communication partners; limited bandwidth, battery lifetime, and computation power prohibit the deployment of complex encryption algorithms and the establishment of public key infrastructure (PKI). Although these characteristics are essential for the flexibility of a MANET, they introduce specific security concerns that are unknown or less severe in wired networks. Therefore, transplanting the common routing protocols and security infrastructure to a MANET is impossible due to the lack of centralized services. Trust has been recently introduced in solving this problem and is used in existing protocols for ad hoc networks to improve security.

There is a common assumption among routing protocols and applications for ad hoc networks that all nodes are trustworthy and cooperative (Ramana et al., 2010), i.e., all nodes behave in accordance with the defined specifications of such protocols and applications. Nevertheless, this hypothesis is erroneous due to restricted resources and malicious behaviors among nodes, e.g., selfish nodes deny relaying the packets of other nodes, and malicious nodes disturb the network. Several attacks, such as man-in-the-middle, blackhole, and DoS, may target a MANET. Thus, the aforementioned assumption may lead to unforeseen pitfalls, namely, low network efficiency and high vulnerability to attacks. Furthermore, other factors such as reliability and bandwidth are occasionally included in discovering routes aside from determining the shortest distance. Assigning a local trust level to a node pair can not only alleviate the negative effects caused by misbehaviors but also make communication occur only among trustworthy neighbors with respect to the fact that the exchange of information with compromised nodes can deteriorate the performance of ad hoc networks. Therefore, incorporating a relationship of trust into MANET nodes is important. Moreover, designing a mechanism that allows nodes to infer the trustworthiness of other nodes, especially of strangers, is necessary.

In most of the previous relaying rules (Zouridaki et al., 2005; Raya and Hubaux, 2007; Adibi and Agnew, 2008), the forwarding behaviors of nodes do not change with the running system. However, in reality, nodes may be intelligent and can display alterable delivery behaviors according to their own conditions as

[*] Corresponding author at: College of Computer Science and Technology, Jilin University, 2699 Qianjin Avenue, Changchun 130012, China.
Tel.: +86 431 85168355; fax: +86 431 85168337.
E-mail address: lyh_lb_lk@yahoo.com.cn (Y. Liu).

1084-8045/$ - see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jnca.2010.11.007

well as the conditions surrounding them. Hence, we propose the probability of whether node *i* agrees to forward the packets of node *j* depending on the extent of attribute similarity between them. Most of the past routing protocols only pursue the shortest path to the destination (Johnson and Maltz, 1996; Perkins and Royer, 1999; Karp and Kung, 2000; Pirzada and McDonald, 2007), which is more adaptive to a high quality network where the link and connectivity are safe and stable. A routing path with the shortest length may not be the best one for a MANET due to its unstable topology and signal attenuation. Moreover, most of the existing models do not study further the cases where nodes have separate attributes. Experience with MANETs suggests that participants should have distinct characteristics from each other, namely, surrounding communication environment, velocity, and moving direction. Due to the absence of attributes in prior works, all individuals were treated equally in routing packets and propagating trust. For example, if user *A* (mama) is already known to trust user *B* (*A*'s son), and user *B* trusts user *C* (his wife), we would like to know whether user *A* trusts user *C*. The current trust models can conclude that user *A* trusts user *C*, but it is uncertain in the aforementioned case. This misjudgment is attributed to the negligence of individual attributes and roles. Thus, we propose a concept of attribute similarity, where the trust degree between nodes is initialized and updated constantly. Finally, we incorporate the attribute similarity and the trust degree into an on-demand routing protocol considering the communication reliability and the path length.

The main contributions of this study are summarized as follows: (1) a novel scheme for evaluating trust based on attribute similarity is proposed, (2) a recommended method for computing the attribute similarity between two given nodes is provided, (3) an intelligent delivery rule is designed, and (4) an approach to incorporate attribute similarity and trust degree into a routing protocol is provided. Moreover, we present simulations demonstrating the effectiveness of the proposed routing scheme in selecting more trustful nodes and defending against malicious attacks. The extensive results reveal the effects of transmission range, velocity, and number of nodes on network performances.

The rest of this work is organized as follows. Section 2 summarizes the related work on trust evaluation and trust-based routing protocols. Section 3 covers the problem statement. The definitions of trust and similarity are given in this section. Section 4 describes the new routing scheme in detail. Section 5 presents the extensive experimental results. The theoretical and practical implications, as well as the study's limitations and future research directions, are given in Section 6. Finally, the conclusions are drawn in Section 7.

2. Related works

Integrating trust into a MANET routing is an intensive research field, and numerous solutions to this have been proposed. As we are planning on adopting trust in this work, we first focus our attention to trust evaluation models in MANETs. We already have a notion of trust between nodes, and thus we also discuss trust routing in MANETs. Most of the existing routing protocols are the extensions of popular on-demand routing protocols such as Dynamic Source Routing (DSR) (Peng et al. 2010).

2.1. Trust evaluation

Candolin and Kari (2002) chose to compute the incomplete trust for a third node using a second node hierarchically. However, this method is prone to random attacks if the second node (recommending node) itself is malicious. Pirzada and McDonald (2004) sought to establish trust in pure ad hoc networks using the concept of weights. Nonetheless, they neglected the "knowledge" learned from past incidents. Anantvalee and Wu (2007) proposed a reputation-based system as an extension to source routing protocols for detecting and punishing selfish nodes in MANETs. However, they did not consider how to compute the reputation values of nodes. Peng et al. (2008) assessed the subjective trust of nodes through the Bayesian method, but they were not able to detect dishonest recommendations. Luo et al. (2008) proposed a fuzzy trust recommendation framework based on collaborative filtering, but they neglected the evolution of trust relationships. Li et al. (2008) proposed an objective trust management framework, where trust was based not only on direct observations but also on second-hand information. However, they did not consider the recommendation trust model.

At present, most of the trust evaluation frameworks belong to a recommendation-based methodology such that the evaluation results are heavily dependent on the accurate measurement of the forwarding behaviors of neighboring nodes and on the degree of honesty of the recommenders. In contrast to previous works, our research is motivated by a collaborative manner among strangers in human life. We combine search, evaluation, propagation, and evolution of trust between each node to provide an independent trust evaluation model for a MANET, which is determined only by self-relevant knowledge and is the basis for routing protocols.

2.2. Trust-based routing protocols

Marti et al. (2000) proposed the use of Watchdog and Pathrater. Watchdog promiscuously listens to the transmission of the next node in the path to detect misbehaviors. Pathrater keeps the ratings for other nodes and performs route selection by choosing routes that do not contain selfish nodes. However, the Watchdog mechanism needs to maintain the state information on the monitored nodes and the transmitted packets, which undoubtedly increases memory overhead. Buchegger and Boudec (2002) proposed an extension (CONFIDANT) to the DSR protocol. When misbehaving nodes are detected, an alarm is sent to other nodes (friends) in the network to isolate the misbehaving nodes from the network. However the misbehavior could be mistaken during detection. Winjum et al. (2005) described a method using a trust metric for routing. The concept works by identifying the routing information sent by trusted nodes from the others. However, in this method, each node has to maintain two routing tables: one for classical (untrusted) routing and another table with the trusted routes. Pirzada et al. (2006) incorporated trust and reputation into the DSR protocol to realize a dependable routing where trust values are used to construct trusted routes passing through benevolent nodes and circumvented malicious nodes. However, this method does not consider preventing dishonest recommendations. Chang et al. (2006) employed distributed authentication authorities and distributed trusted groups to assist in the authentication process. However, this proposal does not fit well in the dynamic MANET environment because a multi-party authentication introduces high delay. Chen et al. (2009) designed a distributed trusted routing framework that achieves the authentication of messages, nodes, and routes. However, this framework also needs the assistance of a certificate authority. Yu et al. (2009) proposed an attack detection and defense mechanism using the route redundancy in networks and message repetition in topological discovery, but they neglected the prevention of dishonest recommendations in their trust model.

As trusted and untrusted routes are not equally treated, a node may have two routes to a given destination. One short route is untrusted, whereas the long one is trusted. Designing a rational strategy in making consistent decisions is one of our main aims. The detailed implementation of our scheme is an extension of the DSR