Ad Hoc Networks 11 (2013) 2096–2114

Contents lists available at SciVerse ScienceDirect

Ad Hoc Networks

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

Trust prediction and trust-based source routing in mobile ad hoc networks

Hui Xia [a], Zhiping Jia [a,*], Xin Li [a], Lei Ju [a], Edwin H.-M. Sha [b]

[a] School of Computer Science and Technology, Shandong University, Ji'nan 250101, China
[b] Department of Computer Science, University of Texas, Dallas, TX 75083-0688, USA

ARTICLE INFO

Article history:
Received 15 October 2011
Received in revised form 14 February 2012
Accepted 16 February 2012
Available online 25 February 2012

Keywords:
Ad hoc
Trust prediction
Source routing
Security requirement
Malicious node

ABSTRACT

Mobile ad hoc networks (MANETs) are spontaneously deployed over a geographically limited area without well-established infrastructure. The networks work well only if the mobile nodes are trusty and behave cooperatively. Due to the openness in network topology and absence of a centralized administration in management, MANETs are very vulnerable to various attacks from malicious nodes. In order to reduce the hazards from such nodes and enhance the security of network, this paper presents a dynamic trust prediction model to evaluate the trustworthiness of nodes, which is based on the nodes' historical behaviors, as well as the future behaviors via extended fuzzy logic rules prediction. We have also integrated the proposed trust predication model into the Source Routing Mechanism. Our novel on-demand trust-based unicast routing protocol for MANETs, termed as Trust-based Source Routing protocol (TSR), provides a flexible and feasible approach to choose the shortest route that meets the security requirement of data packets transmission. Extensive experiments have been conducted to evaluate the efficiency and effectiveness of the proposed mechanism in malicious node identification and attack resistance. The results show that TSR improves packet delivery ratio and reduces average end-to-end latency.

1. Introduction

Wireless networks allow a more flexible model of communication than traditional networks since the nodes is not limited to a fixed physical location. Unlike cellular wireless networks, mobile ad hoc networks (MANETs) are spontaneously deployed over a geographically limited area without well-established infrastructure. They are widely deployed in applications such as the disaster recovery and distributed collaborative computing, where routes are multi-hop and inter-agent communication are achieved by message transmission. Each node acts as a wireless router which delivers packets for neighbors to reach the intended destination, which allows MANETs to accommodate high mobility and frequent topology changes. Meanwhile, a MANAT works well only if the mobile nodes are trusty and behave cooperatively.

Due to the distributed nature, openness in network topology and absence of a centralized administration in the management, MANETs often suffer from attacks by malicious nodes [1]. These attacks range from naive passive eavesdropping to vicious battery draining attacks. Routing protocols, data, battery power and bandwidth are the common targets of these attacks. Specifically speaking, attacks on MANETs can be characterized by the types of attackers. External attackers attempt to disrupt the network by injecting erroneous routing information. They create routing loops or other non-functional routes, or attempt to partition the network by creating a wormhole. External attackers may also replay old routing information or modify route information being transmitted between nodes. Internal attackers are nodes that have been compromised by malicious parties. They advertise

* Corresponding author. Tel.: +86 13964096689.
E-mail addresses: sprit_xiahui@mail.sdu.edu.cn (H. Xia), jzp@sdu.edu.cn (Z. Jia), lx@sdu.edu.cn (X. Li), julei@sdu.edu.cn (L. Ju), edsha@utdallas.edu (E.H.-M. Sha).

1570-8705/$ - see front matter © 2012 Elsevier B.V. All rights reserved.
doi:10.1016/j.adhoc.2012.02.009

false routing information in order to disrupt the flow of information in the network, generating gray-hole, black-hole, modification or Sybil attacks. The highly mobile nature of nodes also creates security challenges. As nodes regularly drop in and out of the radio frequency range, the network topology is highly dynamic. Mobility also makes physical security more challenging as the compromise of a legitimate node or the insertion of a malicious node may go unnoticed in such a dynamic environment. As MANETs typically lack a central authority for authentication and key distribution, security mechanisms must be scalable and capable of frequent topology changes. They must also safeguard against the broadcasting of false routing information by malicious nodes. In order to reduce the hazards from such nodes and enhance the security of network, it is important to rate the trustworthiness of other nodes without relying a central authority to build up a 'trust' environment. Trust prediction mechanisms allow a node to evaluate trustworthiness of other nodes, which not only help in malicious node detection, but also improve network security performance and robustness. In other words, mobile nodes can know whether and how much they can trust other mobile nodes with the help of such mechanisms. The trust information guide nodes to avoid highly risky actions, such as receiving (forwarding) packets from (to) the node with low trustworthy levels [2]. Recently, various researches work on building up 'trust' among distributed network nodes to simulate cooperation and improving the performance and security of the network. Our proposed framework evaluates trust on a continuous scale and takes into account both node trust and route trust.

The primary security threat to MANETs routing is the possibility of an adversary disrupting traffic by compromising the routing mechanisms. The distribution of false routing information allows the potential of unintended network routing loops, denial of service attacks, or other nonfunctional routes. These attacks may hinder or prohibit the communication vital to fulfilling the mission of networked nodes. It is therefore critical for nodes to dynamically determine the validity of routing information prior to making routing decisions. With authentication and encryption mechanisms, secure routing protocols have been developed to ensure properties such as confidentiality and integrity. These protocols require a centralized trusted third party, which is impractical for MANETs [3]. Moreover, the traditional cryptosystem based security mechanism is typically used to resist the external attacks. They show inefficiency in handling the attacks from the internal malicious nodes which may lead to serious influence on the security, the confidentiality, and the life cycle of the whole network. Recently a new class of routing protocols in MANETs has been proposed, called trusted routing protocols. The trust-based routing protocols are not absolutely secure, but certainly have an accurate measure of reliability in them. Careful selection of a dependable trusted route may mitigate the impairment from malicious nodes, however, it is also critical to route packets to destinations without generating excessive overhead. Therefore, how to design an efficient and effective trusted routing protocol is a major challenging issue for this network.

Since MANET routing is a cooperative process where route information is relayed between nodes, any secure routing mechanism must evaluate the trustworthiness of other nodes. In this paper, we build a simple trust prediction model based on evaluated node's historical behaviors (forwarding packets) and its capability to deliver a mutually agreed service to predict this node's future behaviors. Our trust evaluation framework provides considerable security with minimal overhead, and it is scalable and flexible to be easily combined with other existing schemes for security enhancement. Moreover, we propose a novel on-demand unicast routing protocol for MANETs as an application of the proposed trust model, by extending the Source Routing Mechanism [12]. In our Trust-based Source Routing protocol (TSR), each node in a MANET predicts their neighbors' future behaviors and selects the shortest trusted route to transmit required packets. Experiments have been conducted to evaluate the efficiency and effectiveness of the protocol in malicious node identification and attack resistance.

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

1. In our trust prediction model, each node derives neighbors' historical trusts based on their own packet correct forwarding ratios. In other words, our model only uses packets correct forwarding ratios to recognize an evaluated (or monitored) node's historical behaviors. Taking an evaluated node's historical trust and its capability to deliver a mutually agreed service as the inputs, we use the fuzzy logic rules prediction method to calculate this evaluated node's current trust on the point view of the monitor. The obtained value not only offers a prediction of one's future behaviors, but also provides a relative identification of node's properties (i.e., normal or malicious nodes). The obtained nodes' trust values can be easily used in trust management strategy includes the applications anti-attack, decision making etc. These concepts yield a trust model suitable for applications in content-based routing schemes while not impacting the route-discovery.
2. In this paper, we consider trusted routing as a case study to detailed illustrate the trust application, in which a node's trust value is introduced as a constraint of route-finding. Basing on the proposed trust prediction model, we propose a novel on-demand trust-based unicast routing protocol for MANETs, namely Trust-based Source Routing protocol (TSR), which extends from Source Routing Mechanism with the extension of 'trust'. In this new protocol, a source can establish multiple loop-free routes to a destination in one route discovery process, and each route has an evaluation vector composed of hop count and route trust value. A destination will respond with qualified routes as candidates that satisfy the trust requirements of transmitting data packets. The shortest one will be selected as the transmitting (forwarding) route.
3. We evaluate our proposed TSR, by comparing to with DSR [12] and Trusted-DSR [20] using the NS-2 simulator. The experimental results show that our protocol is more effective. In particular, as a trust-based routing