Ad Hoc Networks 30 (2015) 84–98

Contents lists available at ScienceDirect

Ad Hoc Networks

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

Trust based routing mechanism for securing OSLR-based MANET

Shuaishuai Tan [a], Xiaoping Li [a], Qingkuan Dong [b,*]

[a] School of Aerospace Science and Technology, Xidian University, Xi'an 710126, China
[b] State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China

ARTICLE INFO

Article history:
Received 2 August 2014
Received in revised form 8 December 2014
Accepted 7 March 2015
Available online 26 March 2015

Keywords:
Ad hoc networks
Trust model
Trust based routing algorithm

ABSTRACT

A mobile ad hoc network (MANET) is a kind of infrastructure-less wireless network that is self-organized by mobile nodes communicating with each other freely and dynamically. MANET can be applied to many fields, such as emergency communications after disaster, intelligent transportation, and Internet of things. With the rapid development of wireless network applications, MANET will become dense and large because more and more mobile devices are required to be interconnected. The optimized link state routing (OLSR) protocol is an efficient proactive routing protocol which is very suitable for such dense and large-scale MANET. However, in both data plane and routing plane, OLSR-based MANET suffers from many serious security threats which are difficult to resist via traditional security mechanisms. In this paper, we propose a trust based routing mechanism to alleviate this issue. In this mechanism, a trust reasoning model based on fuzzy Petri net is presented to evaluate trust values of mobile nodes. In addition, to avoid malicious or compromised nodes, a trust based routing algorithm is proposed to select a path with the maximum path trust value among all possible paths. Then we extend OLSR by using the proposed trust model and trust based routing algorithm, called FPNT-OLSR. For the implementation of FPNT-OLSR, we design a trust factor collecting method and an efficient trust information propagating method, which do not generate extra control messages. Simulation results show that FPNT-OLSR is very effective in establishing secure routes. It also performs better than existing trust based OLSR protocols in terms of packet delivery ratio, average latency and overhead.

1. Introduction

A mobile ad hoc network (MANET) is a kind of wireless network that is self-organized by mobile nodes communicating with each other freely and dynamically, without a fixed network infrastructure. With the rapid development of intelligent transportation, wearable technology, Internet of things (IoT) and ubiquitous computing, MANET becomes increasingly popular. According to Canalys's forecast, worldwide mobile device shipments (notebook PCs, tablet PCs, smart phones, etc.) will reach 2.6 billion units by 2016, which implies a large-scale and dense tendency of mobile networks. OLSR protocol is a standardized optimized link state routing protocol for MANET [1]. The protocol provides an efficient multipoint relays (MPR) selecting mechanism to achieve flooding reduction. Compared with reactive routing protocols, OLSR keeps more stable links and offers promising

* Corresponding author at: Mailbox 119, 2 South Taibai Road, Xidian University, Xi'an 710071, Shaanxi Province, China. Tel.: +86 153 3902 1227.
E-mail addresses: ss_tan@163.com (S. Tan), xpli@xidian.edu.cn (X. Li), qkdong@mail.xidian.edu.cn (Q. Dong).

http://dx.doi.org/10.1016/j.adhoc.2015.03.004
1570-8705/

performance in bandwidth and traffic overhead [2]. Furthermore, it is particularly suitable for large and dense mobile networks [1]. In 2014, IETF released a new version, OLSRv2 [3], which is the first updated ad hoc routing protocol compared with the other three standardized protocols, AODV, TBRPF, and DSR. All the situations indicate that OLSR has great potential in future mobile ad hoc networks.

Due to the openness of wireless links, frequent mobility of nodes and high dynamic of topology, nodes in MANET are more vulnerable to attacks in both *data plane* and *routing plane*.

- *Attacks in data plane*: certain attacks preventing data traffic from being delivered to destinations at a given timescale, such as blackhole attack, jellyfish attack [4], and DoS attack and other types of attacks [5].
- *Attacks in routing plane*: certain attacks disturbing a node to establish correct routing table, such as node isolation attack [6], routing message dropping attack, and control message flooding attack and other types of attacks [7,8].

Cryptography based security mechanisms [9–12] are introduced into MANET to authenticate identities of network entities, and assure the confidentiality and integrity of messages. It seems that the security problems are solved because a malicious entity without a legitimate identity is prevented from participating in the network and launching attacks any more. However, legitimate entities could change to be "malicious" for the following reasons: an entity such as a computer system can be penetrated and controlled; an entity like a device can be physically captured and manipulated; the secret keys of a cryptography system may be attacked; and the one who has secret keys may be exploited via social engineering skills. All these techniques will disable the authentication mechanism based on cryptography, and thus attackers are able to participate in the network again. In other words, networks still suffer from various threats even under the protection of identity based security frameworks.

As is well known, an attack method must have its specific behavior mode, which can be used to recognize it. On this basis, trust based security mechanisms are proposed to collect trust factors, evaluate target via a trust model, and employ countermeasures to eliminate or avoid threats. *Trust factor* is the information that can reflect behaviors and purposes of an entity. For its advantages in efficiency and dynamic, trust mechanism has been introduced into MANET. Although it has become a popular research area, the existing trust based solutions for securing OLSR based MANET mainly concentrate on dealing with one or several kind of attacks, such as DoS [2], collusion [8], and packet dropping [5]. Some other solutions merely seek to ensure security of either data plane [13] or routing plane [14–16]. Moreover, these solutions often generate excessive overhead in resource-constrained MANET in terms of extra detection messages and trust information propagation messages.

In order to defend against attacks in both data plane and routing plane in OLSR-based MANET, we propose a novel trust based routing mechanism. In this mechanism, a trust reasoning model based on fuzzy Petri net is presented to evaluate the trust value of a mobile node, and a trust based routing algorithm is proposed to avoid malicious or compromised nodes as much as possible. Note that the compromised nodes should also be avoided as they cannot provide normal services any more. Furthermore, we extend the OLSR protocol by integrating the proposed trust model and trust based routing algorithm, called the FPNT-OLSR protocol. Our main contributions are summarized as follows:

- A novel trust reasoning model based on fuzzy Petri net is proposed. This model evaluates trustworthiness of a node according to its behaviors in both data plane and routing plane. Compared with other trust reasoning models, our model makes the reasoning result as objective as possible by refining and layering fuzzy rules, and considers the incompleteness of the evidences.
- A trust recommendation aggregating method which is able to detect and filter slandering recommendations for calculating a correct trust value is presented.
- A trust based routing algorithm is proposed. The algorithm is capable of selecting a path with the maximum path trust value among all the possible paths between any pair of nodes. Furthermore, we prove the correctness of this algorithm.
- Using the proposed trust model and trust based routing algorithm, we extend the OLSR protocol, called FPNT-OLSR protocol. For the implementation of FPNT-OLSR, we design a feasible trust factor collecting method and an efficient trust information propagating method. The two methods do not introduce extra control messages. Simulations are also conducted to verify the effectiveness and efficiency of FPNT-OLSR.

The rest of this paper is organized as follows: Section 2 reviews the related work. Section 3 describes the fuzzy Petri net based trust reasoning model. Section 4 presents the trust based routing algorithm and its proof. Section 5 illustrates the FPNT-OLSR protocol. Simulation results are given in Section 6. Finally, Section 7 concludes the paper.

2. Related work

In this section, the OLSR protocol is briefly introduced first, followed by an outline of existing works on trust model and trust based routing algorithm for MANET, especially the OLSR based MANET.

2.1. Introduction of OLSR protocol

The OLSR protocol [1] was proposed by the Internet Engineering Task Force (IETF) MANET Working Group in 2003. The new version, OLSRv2 [3], was published in 2014. Main operations of OLSR include neighborhood discovery, Multipoint Relay (MPR) selection, topology discovery and route calculation, etc. In OLSR-based MANET, nodes periodically broadcast HELLO messages to discover 1-hop and 2-hop neighborhoods. According to the 1-hop and 2-hop neighborhoods, a node selects its MPRs which