Ad Hoc Networks 21 (2014) 109–122

Contents lists available at ScienceDirect

Ad Hoc Networks

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

TOHIP: A topology-hiding multipath routing protocol in mobile ad hoc networks

Yujun Zhang [a], Tan Yan [b,*], Jie Tian [b], Qi Hu [a], Guiling Wang [b], Zhongcheng Li [a]

[a] Institute of Computing Technology, Chinese Academy of Sciences, Beijing, PR China
[b] Department of Computer Science, New Jersey Institute of Technology, Newark, USA

ARTICLE INFO

Article history:
Received 8 April 2013
Received in revised form 3 December 2013
Accepted 7 May 2014
Available online 27 May 2014

Keywords:
Multipath routing
Topology hiding
MANET

ABSTRACT

Existing multipath routing protocols in MANETs ignore the topology-exposure problem. This paper analyzes the threats of topology-exposure and propose a TOpology-HIding multipath Protocol (TOHIP). TOHIP does not allow packets to carry routing information, so the malicious nodes cannot deduce network topology and launch various attacks based on that. The protocol can also establish multiple node-disjoint routes in a route discovery attempt and exclude unreliable routes before transmitting packets. We formally prove that TOHIP is loop-free and does not expose network topology. Security analysis shows that TOHIP can resist various kinds of attacks efficiently and effectively. Simulation results demonstrate that TOHIP has better capability of finding routes and can greatly increase the capability of delivering packets in the scenarios where there are malicious nodes at the cost of low routing overhead.

1. Introduction

Multipath routing protocols have attracted a lot of attentions recently in MANET for their unique capability in supporting load balancing and improving routing reliability in high dynamic scenarios [1,2]. However, this kind of protocol may become a vulnerable target for the malicious nodes to explore and launch various attacks for the same reason. Therefore, many researchers have designed secure multipath routing protocols [3].

However, as far as we know, none of the existing secure multipath routing protocols deals with the topology-exposure problem. Topology-exposure is a serious problem for MANET, which makes it possible for the malicious nodes to launch many kinds of attacks, such as black hole attack [4], wormhole attack [5], rushing attack [6,7] and sybil attack [8]. Topology-exposure is much more serious in multipath routing protocols than in other routing protocols considering that multipath routing protocols usually carry a lot of routing information in route messages in order to find sufficient routes. In some cases, data packets are also required to carry routing information. For example, Dynamic Routing Protocol (DSR) carries the whole route from source to destination in packet headers [9]. Malicious nodes can deduce part or the whole network topology based on the captured routing information and it is hard to ensure the confidentiality of routing information because of the open media network environment in which any node can capture packets within its transmission range.

To deal with the topology-exposure problem, this paper thoroughly analyzes the threats brought by topology-exposure, defines topology-hiding and designs a TOpology-HIding multipath routing Protocol (TOHIP). TOHIP does not contain link connectivity information in route

* Corresponding author. Tel.: +1 2018880680.
E-mail addresses: zhmj@ict.ac.cn (Y. Zhang), ty7@njit.edu (T. Yan), jt66@njit.edu (J. Tian), huqi@ict.ac.cn (Q. Hu), gwang@njit.edu (G. Wang), zcli@ict.ac.cn (Z. Li).

http://dx.doi.org/10.1016/j.adhoc.2014.05.012
1570-8705/© 2014 Elsevier B.V. All rights reserved.

messages. Thus no node can deduce network topology by capturing route messages and the network topology is hidden. TOHIP can also find as many node-disjoint routes as possible, defend against attacks and exclude the unreliable routes. We formally prove that TOHIP is loop-free and topology-hiding. We also conduct intensive performance evaluation, which shows that TOHIP has better capability of finding routes and does not downgrade performance when there is no malicious node. When there are malicious nodes, TOHIP can greatly improve the packet delivery ratio at a low routing overhead and short routing convergent time.

The rest of this paper is organized as follows. Section 2 presents the threats of topology-exposure and defines topology-hiding. Section 3 discusses related works. Section 4 describes the design of TOHIP. Formal proof of the protocol's characteristics and security analysis are given in Section 5. An enhanced protocol is proposed in Section 6, and performance evaluation is conducted in Section 7. Section 8 concludes this paper.

2. Topology-exposure problem and definition of topology-hiding

Consider an example MANET, whose topology is shown in Fig. 1. *S* is the source node and *D* is the destination node. There are two routes from node *S* to node *D*, which are $S \rightarrow C \rightarrow F \rightarrow D$ and $S \rightarrow A \rightarrow D$, in some multipath routing protocols. Based on the two routes, node *D* can conclude that *S* is connected to *A* and *C*, *C* is connected to *F*, *A* and *F* are connected to *D*. Obviously, the two routes enable node *D* to obtain the whole network topology. We call this problem topology-exposure.

The knowledge of the network topology enables many kinds of attacks to be more harmful in MANET. Some examples are shown in Table 1. Taking the black hole attack as an example, if the malicious node intends to intercept the data packets to a specific destination, it should advertise that it has the route to this destination. It is difficult for this malicious node to redirect routing if no routing information is carried in packets. Also in order to choose the victim node and to intrude into a network, the malicious node needs to know network topology; otherwise, the malicious node cannot perform the black hole attack effectively. In addition to the attacks listed in Table 1, the launch of some other attacks, such as middle-person attack [10] and routing loops, also require the knowledge of network topology.

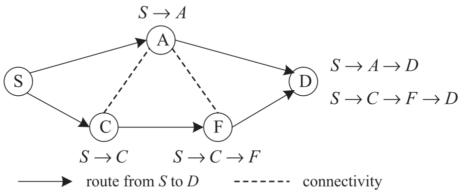

Fig. 1. Topology-exposure by routing information.

We use simulations to show the damage enabled by topology exposure. We take Secure Routing Protocol (SRP), a typical secure multipath routing protocol [11–13], as an example and study the effect when there are malicious nodes. Malicious Dropping Ratio ($\overline{MDR}$) is defined to evaluate the bad effect brought by the malicious nodes.

$$\overline{MDR} = \frac{\sum \text{data packet discarded by the malicious nodes}}{\sum \text{data packet sent by the source node}}$$

Two kinds of attacks, the *black hole attack* and the *rushing attack*, are launched in the simulation. The malicious nodes that launch black hole attack simply drop all packets passing by. When launching rushing attack, the malicious nodes not only get time advantage in route discovery by closing radio shock [6], but also drop all packets passing by. Fig. 2 shows the threat of topology-exposure by comparing the $\overline{MDR}$ of the two attacks in MANET under different intrusion positions. From Fig. 2(a) we can see that when the attackers randomly choose positions to intrude into the network, the two kinds of attackers almost have the same $\overline{MDR}$, which means they cause the same damage to the network. From Fig. 2(b) and (c), we can see the attackers in central positions can drop more packets than those in random positions. This is because the malicious nodes in the central position are likely to be included into the routes, so they can drop more packets. The simulation results show that the attackers that know network topology can give more damage to MANETs.

Both analysis and simulation show that some common attacks in MANET greatly leverage the knowledge of network topology. Hiding network topology can prevent many common attacks from the beginning and thus improve MANET security effectively. We define topology-hiding as follows. We define topology-hiding as follows.

Definition 1. Let N be the set of all nodes in a MANET. Let $dist(n_i, n_j)$ be the hop count between a node n_i and a node n_j. A routing protocol is topology-hiding only if:

For any $n_i \in N$ and $n_j \in N$, if $dist(n_i, n_j) > 2$, then node n_i cannot know which nodes are connected to node n_j.

Table 1
Attacks vs. network topology.

Name of attack	Principle of attack	Dependence on network topology
Black hole [4]	Disrupt route discovery by redirecting routes	Choose the central positions to intrude into MANET
Wormhole [5]	Disrupt route discovery by using tunnel to reduce the hop count	
Rushing [6,7]	Disrupt routing discovery by illegally getting the time advantage to forward route messages	
Sybil [8]	Disrupt route discovery by disguising other nodes	Acquire other nodes' identities