available at www.sciencedirect.com

ScienceDirect

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

Computers & Security

WARP: A wormhole-avoidance routing protocol by anomaly detection in mobile ad hoc networks

*Ming-Yang Su**

Department of Computer Science and Information Engineering, Ming Chuan University, 5 Teh Ming Road, Gwei Shan District, Taoyuan 333, Taiwan

ARTICLE INFO

Article history:
Received 11 August 2009
Received in revised form
9 September 2009
Accepted 30 September 2009

Keywords:
MANETs (Mobile Ad hoc Networks)
Wormhole attacks
AODV (Ad hoc On-demand Distance Vector) routing protocol
Multi-path routing

ABSTRACT

The infrastructure of a Mobile Ad hoc Network (MANET) has no routers for routing, and all nodes must share the same routing protocol to assist each other when transmitting messages. However, almost all common routing protocols at present consider performance as first priority, and have little defense capability against the malicious nodes. Many researches have proposed various protocols of higher safety to defend against attacks; however, each has specific defense objects, and is unable to defend against particular attacks. Of all the types of attacks, the wormhole attack poses the greatest threat and is very difficult to prevent; therefore, this paper focuses on the wormhole attack, and proposes a secure routing protocol based on the AODV (Ad hoc On-demand Distance Vector) routing protocol, which is named WARP (Wormhole-Avoidance Routing Protocol). WARP considers link-disjoint multipaths during path discovery, and provides greater path selections to avoid malicious nodes, but eventually uses only one path to transmit data. Based on the characteristic that wormhole nodes can easily grab the route from the source node to the destination node, WARP enables the neighbors of the wormhole nodes to discover that the wormhole nodes have abnormal path attractions. Then, the wormhole nodes would be gradually isolated by their normal neighboring nodes, and finally be quarantined by the whole network.

1. Introduction

In all possible methods of attacks in Mobile Ad hoc Networks (MANETs), the wormhole attack is one of the most threatening and hazardous attacks. A wormhole attack is usually performed by two or more malicious nodes in conspiracy. Two malicious nodes at different locations send received routing messages to each other via a secrete channel. In this way, although the two malicious nodes are located far from each other, they appear to be within one-hop communication range. Therefore, the route passing through the malicious nodes is very likely to be shorter than any other regular one. Wormhole nodes can easily grab the route from the source node to the destination node, and then sniff, drop, or selective-drop data packets passed by. Wormhole nodes can successfully execute such attacks without compromising any computer, and are unavoidable, even though some MANETs provide authenticity and confidentiality protection.

In a wormhole attack, malicious node $m1$ first captures a routing message from a neighboring node, and then sends the message to another malicious node, $m2$, by means of a secret tunnel, $m2$ then broadcasts or propagates the message received. In this way, a tunnel-like channel is formed between the two malicious nodes. Even though the tunnel has a very

* Tel.: +886 3 3507001; fax: +886 3 3593874.
E-mail address: minysu@mail.mcu.edu.tw
0167-4048/$ – see front matter © 2009 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2009.09.005

long distance, other normal nodes may mistakenly think that there is only a distance of a one-hop count. The tunnel-like channel can be realized by two methods (Khalil et al., 2005): packets encapsulated channel and out-of-band channel, as shown in Fig. 1(a) and (b), respectively.

Packets encapsulated channel is also called in-band channel, where a malicious node puts a captured routing message in a data packet payload, and uses normal nodes to transmit the data packet to another malicious node. The malicious node receiving the data packet draws the routing message out of the packet payload and further broadcasts or propagates it. In this way, the hop count is reduced to increase the chance of grabbing a route, and as no field information is changed, neither Secure AODV (SAODV) (Zapata and Asokan, 2002), which can protect routing messages, nor Authenticated Routing for Ad hoc Networks (ARAN) (Sanzgiri et al., 2002), which can authenticate each neighbor, have any way of defending against attacks from a encapsulated channel. As shown in Fig. 1(a), a path is built in advance between the two malicious nodes, $m1$ and $m2$, and s is the source node and d is the destination node. When s broadcasts a Route Request (RREQ), it would be received by malicious node $m1$, and then $m1$ encapsulates the RREQ into the payload of a data packet, and transmits it using the pre-built path between $m1$ and $m2$. After receiving the data packet, $m2$ would extract the original RREQ and broadcast it till it reaches the destination node. As the path passing through the malicious nodes saves 4 hop counts on the surface and thus is shorter than the other two paths, node d would finally choose the path to respond a Route Reply (RREP). In this way, the malicious nodes would deprive the route of passing data packets. The method of an out-of-band channel differs from encapsulating packet mainly in the type of tunnel-like channel. A special channel may be a connection by a wired network between the two malicious nodes, or a private channel between the two ends using a high-powered transmission to send signals over a long distance, as shown in Fig. 1(b).

This paper proposes a secure routing protocol to defend against wormhole attacks based on the Ad hoc On-demand Distance Vector (AODV) routing protocol (Perkins et al., 2004), which is named WARP (Wormhole-Avoidance Routing Protocol). WARP considers link-disjoint multipaths during path discovery in order to choose a safer path to avoid wormhole nodes. Since wormhole nodes have great abilities to grab the routes from the source nodes to the destination nodes, after a certain time of executing wormhole attacks, the wormhole nodes would be rejected by their neighboring nodes, thereby preventing them from transmitting routing messages, and hence, they are quarantined by the whole MANET. Some normal nodes may be located at key positions of connectivity within the network, and thus, may be quarantined due to considerable acquisition of routing paths; however, they would not be in key positions for long as the MANET topology is constantly changing. In addition, in the design of WARP, when a node is quarantined by its neighbors, and then has no abnormal behaviors for a certain period, it would be recovered from the quarantine.

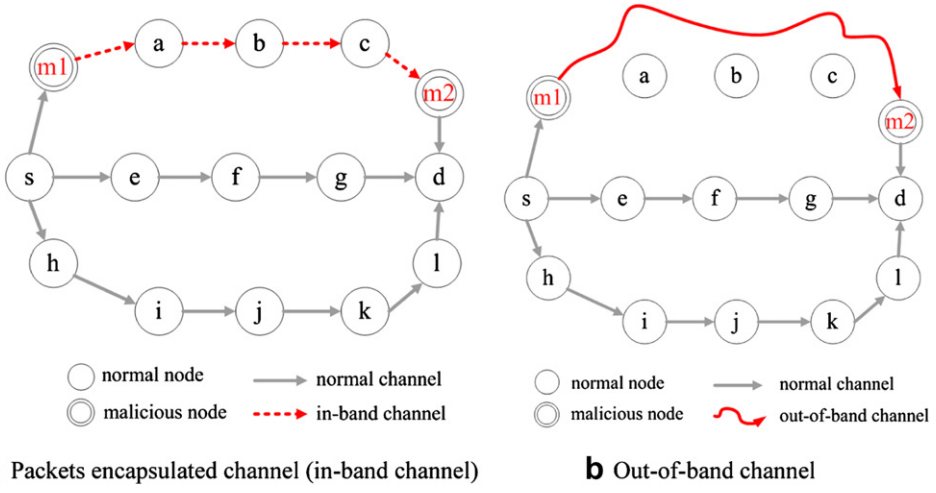
The remainder of this paper is organized as follows. Section 2 provides a brief review on previous works against wormhole attacks and the AODV routing protocol. Section 3 describes the details of the proposed routing algorithm – WARP, in detection and defense against wormhole nodes. Section 4 offers discussion on the properties of WARP. Section 5 is the outcome and analysis of ns2 simulation. Section 6 offers conclusions.

2. Related works

Since the proposed WARP is based on AODV, in addition to reviewing previous research on defending wormhole attacks, the AODV is also briefly described.

2.1. Previous researches

The methods proposed in literature to defend against wormhole attacks can be divided into three categories. The first is to modify a well-known routing protocol, such as Ad hoc On-demand Distance Vector (AODV) (Perkins et al., 2004) or Dynamic Source Routing (DSR) (Johnson et al., 2004), to avoid wormhole nodes during path discovery, such as (Song et al., 2005; Chiu and Lui, 2006; Lee et al., 2008; Su and Boppana, 2007;



a Packets encapsulated channel (in-band channel) **b** Out-of-band channel

Fig. 1 – Two possible implementation methods of wormhole attacks.