Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 56 (2015) 384 – 390

Procedia Computer Science

International Workshop on Cyber Security and Digital Investigation (CSDI 2015)

Analysis of Detection Features for Wormhole Attacks in MANETs

Muhammad Imran[a], Farrukh Aslam Khan[b,]*, Tauseef Jamal[a], Muhammad Hanif Durad[a]

[a]*Department of Computer and Information Sciences, Pakistan Institute of Engineering and Applied Sciences, Islamabad, Pakistan.*
[b]*Center of Excellence in Information Assurance (CoEIA), King Saud University, Riyadh, Saudi Arabia.*

Abstract

Mobile Ad hoc Networks (MANETs) work without any fixed infrastructure and each node in the network behaves as a router in order to transmit data towards the destination. Due to the lack of central point of control, MANETs are more vulnerable to routing attacks as compared to other networks. Wormhole attack is one of the most severe routing attacks, which is easy to implement but hard to detect. Normally, it works in two steps; in the first step, the wormhole nodes attract more and more traffic towards them through the wormhole channel, and in the second step, they start harming the network by modifying or dropping the network traffic. Several authors have proposed different solutions to counter wormhole attacks in MANETs. In this paper, we thoroughly analyze these existing techniques on the basis of their limitations as well as features that are vital in detecting wormhole attacks in MANETs.

*Keywords:*Wormhole Attacks; Intrusion Detection System; Mobile Ad hoc Networks (MANETs).

1. Introduction

Over the past few years, Mobile Ad hoc Networks (MANETs) have emerged in several forms due to the unprecedented development in the wireless communication technology. The primary features of MANETs include lack of infrastructure, shared broadcast channel, insecure wireless environment, absence of central point of control, dynamic topology, and limited resources. MANETs can be used for several applications e.g., in disaster areas to collect useful information, in battlefield for communication among soldiers, and in oceans for extracting and communicating critical information etc. In MANETs, each node communicates directly with its neighboring nodes that are in its transmission range and works both as a host as well as a router. In order to communicate with non-

* Corresponding author. Tel.: +966-11-4697341; fax: +966-11-4696452.
E-mail address: fakhan@ksu.edu.sa

doi:10.1016/j.procs.2015.07.224

neighbors, a node establishes indirect connection with the help of other nodes in its neighborhood in a hop-by-hop manner. Routing protocols play an important role in finding, maintaining, and repairing routes in the network. Researchers have proposed a number of routing protocols for MANETs over the past several years[1,2].

Wormhole attack is a well known and one of the most serious security threats in MANETs[3,4,5]. It can harm several MANET routing protocols such as Dynamic Source Routing (DSR), Ad hoc On-demand Distance Vector (AODV), Optimized Link State Routing (OLSR), Destination Sequenced Distance Vector (DSDV), and Topology Dissemination Based on Reverse-Path Forwarding (TBRPF) etc. Generally, two or more malicious nodes launch a wormhole attack using a private channel called tunnel, between them. The working of wormhole attack is shown in Figure 1. At one end of the tunnel, a malicious node captures a control packet and sends it to another colluding node at the other end through a private channel, which rebroadcasts the packet locally. Route for communication between source and destination is selected through the private channel because of having better metrics e.g., less number of hops or less time, as compared to packets transmitted over other normal routes. The attack normally works in two phases. In the first phase, the wormhole nodes get themselves involved in several routes. In the second phase, these malicious nodes start exploiting the packets they receive. These nodes can disrupt the network functionality in a number of ways. For example, these nodes can confuse the protocols that depend on node location or geographic proximity, or the colluding nodes may forward data packets back and forth to each other in case of virtual tunnel so as to exhaust the battery of other intermediate nodes. Wormhole nodes can drop, modify, or send data to a third party for malicious purposes.

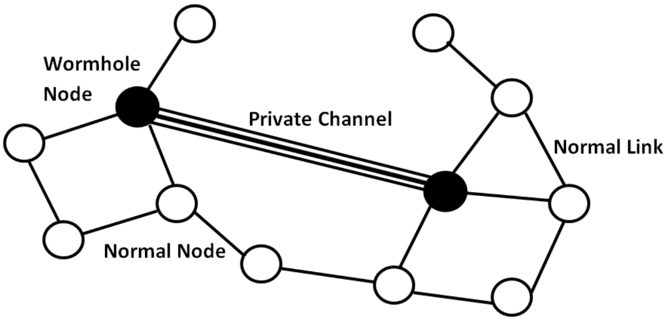

Fig. 1. Working of Wormhole Attack in MANETs.

This paper analyzes different wormhole detection techniques and tries to identify some common limitations of these techniques, which can negatively affect the performance of MANETs in different ways. In addition to this, it also identifies the features of MANETs on the basis of which wormhole attacks can be detected. A critical analysis is also carried out at the end of the paper.

The remainder of this paper is organized as follows: Section 2 provides a brief overview of the techniques proposed by different authors to counter wormhole attacks. Section 3 presents different features, which can be used to detect wormhole attacks in MANETs. Section 4 discusses the limitations of techniques used to detect wormhole attacks. Section 5 shows a comparison of different techniques on the basis of limitations and features used in them. Finally, section 6 conclude the paper and presents some future directions.

2. Related Work

During the past several years, a number of researchers have proposed various solutions especially to tackle the wormhole attacks in MANETs. In this section, we discuss different wormhole detection techniques based on their features and categories. Hu *et al.*[5] introduced a technique to detect wormhole attack with temporal or geographical leash. Hu and Evans[6] presented a technique to avoid wormhole attacks with the help of directional antennas, which sense the direction from which they receive the data. Khalil and Shroff[7] proposed a method called LITEWORP to detect wormhole attacks by keeping and sharing neighboring nodes lists in encrypted form. Chiu and Lui[8] proposed a technique called DelPHI (Delay Per Hop Indication) to prevent wormhole attacks using AODV routing protocol. The technique tries to avoid wormholes with the help of RREQ, RREP, and time duration. Yun *et al.*[9] proposed a technique called WODEM (WOrmhole DEfense Mechanism) with a detector node having GPS technology and ability to transmit data at different powers. Choi *et al.*[10] proposed an algorithm called WAP (Wormhole Attack Prevention) to prevent wormhole attacks in MANETs. Nodes in the network maintain a neighbor table that records sending and receiving times of RREQ as well as the suspected value of that node. Hayajneh *et al.*[11] proposed DeWorm protocol that finds alternate routes to the destination that do not pass through the wormhole nodes. Azer *et al.*[12] developed a prevention and detection technique on the principles of a theory from social sciences known as diffusion of innovations. Alam and Chan[13] developed a technique for wormhole detection called RTT-TC based on round-trip time and topological comparisons. Su[14] presented a technique to avoid wormhole attacks called WARP (Wormhole Avoidance Routing Protocol). Shi *et al.*[15] proposed a novel technique to detect wormhole attacks in MANETs. The technique has three phases i.e., location phase, detection phase, and bidirectional location phase. Each of these phases is initiated if the previous stage produces a suspicious node. Gupta *et al.*[16] proposed a protocol called WHOP, which is the modification of AODV protocol for wormhole detection. Shin and Halim[17] proposed a method based on route redundancy and time-based hop calculation, which detects and isolates wormhole nodes. Khan and Islam[18] proposed an approach based on DSDV protocol for self-sufficient wormhole attacks, which detects suspicious links by modifying the routing table. Chourasia and Singh[19] proposed an efficient approach called modified wormhole detection AODV protocol, which detects wormhole attack by using number of hops and delay of each node in different routes between source and destination. Agrawal and Mishra[20] presented a method to detect wormhole attacks in MANETs on the basis of RTT estimator for AODV protocol in Network Simulator-3 (NS-3).

3. Detection Features

In this section, we discuss different features of MANETs, which can be helpful in the detection of wormhole attack. The techniques discussed in section 2 also use one or more of these features for wormhole detection. Here we discuss each feature in detail.

3.1. Location

In case of wormhole attack, location is a very important feature. If we know the exact location of mobile nodes, then it would be very easy to build a graph of the network. One way of implementing this system is to equip each node in the network with a Global Positioning System (GPS) device. To reduce cost, some special nodes having GPS receiver can be deployed at specific locations in the network to get locations of the neighboring nodes. The relative location information can also be collected by using special antennas, which are able to detect the direction from which the data is received. The use of GPS device or special antenna will increase the cost of nodes and make the network more expensive. This will also decrease the battery timing of mobile nodes. By using exact or relative location as a detection feature can also increase the False Positive Rate (FPR), as in MANETs nodes change their positions frequently.

3.2. Time

The time feature can also be helpful in wormhole attack detection. The route having wormhole attack will have more average time per hop as compared to the normal route. To calculate accurate time difference between source and destination, all nodes in the network should be equipped with tightly synchronized clock. The time difference can also be calculated without tightly synchronized clock where source node sends a special lightweight Hello message to the destination and records the sending time of the packet. When the destination node receives that Hello message, it replies with a Hello-Reply message. The difference between sending and receiving time is calculated and is divided by two after excluding the processing time at source, destination, and intermediate nodes. Then the average time of each hop is calculated. To implement a synchronized clock is a difficult and expensive task in MANETs. The techniques that use time difference as a detection feature can face the problem of increasing FPR due to congestion in the network. It is also difficult to identify the location and identity of malicious nodes with simple time difference methods.

3.3. Hop Count

The wormhole nodes generally attract the network traffic by showing shorter path (i.e. less number of hops), therefore, the hop count feature can also be used as a detection parameter. A path through wormhole nodes contains less number of hops as compared to the normal path because hop count does not increase when the message moves through the private channel between malicious nodes. Some techniques find the presence of wormhole by using hop count information in association with time or location. Average time for a single hop is calculated by dividing the total hops by total time or distance. If the average hop time or distance is greater than the normal preset hop time, then the path contains malicious nodes. Techniques based on average time or distance may require synchronized clock or GPS device respectively. The Intrusion Detection System (IDS) that works on avoiding the shortest route may neglect the legitimate path having shortest route to the destination.

3.4. Neighborhood

The basic property of wormhole attack is to represent two non-neighbor nodes as neighbors. So the wormhole can also be detected by getting data about neighboring nodes. Such techniques collect and maintain the data related to immediate (one hop) neighbors of a node while some other techniques try to identify the wormhole attack by keeping and analyzing the data of two-hop neighbors collected by Hello message. These techniques face problems in dense networks where each node contains many neighbors. Therefore, to keep and analyze data up to two-hop neighbors require more memory, storage, and processing power. In addition, Hello messages will also increase the overall network traffic. These techniques will not perform efficiently in networks with high mobility rate because neighbor lists will also change frequently, as a result of which FPR will increase.

3.5. Data Packets

Some intrusion detection techniques try to detect wormhole nodes on the basis of ratio of data packets received and sent. In these techniques, all nodes are set in promiscuous mode so that they can listen data packets in their neighborhood. The nodes record the number of packets received and forwarded by their neighboring nodes in a table so that they can estimate the state of their neighbors whether they drop, modify, or forward data packets to some node other than the destination node. On the basis of this information, they calculate trust value of each neighboring node. Although this is a simple technique, it can work effectively in large networks with high mobility. However, setting nodes in promiscuous mode is not an efficient way because by doing so, each node will have to process each data packet broadcasted in its neighborhood in addition to the processing of control messages.

3.6. Route Reply

Route Reply (RREP) is also used as a detection feature to detect wormhole attacks. On receiving a request for a fresh route, a node sends RREP message to the source node if it is the destination node or have a fresh route to the destination node. The wormhole nodes usually violate this condition to launch the attack. Since RREPs are unicasted only, nodes that want to keep record of the RREPs have to be set in the promiscuous mode, which can affect the network efficiency.

3.7. Route Request

Route Request (RREQ) is the most important feature for on-demand routing in MANETs. Like RREP, it is also used with some other features to detect wormhole attacks. As each RREQ generated by a source node normally reaches every node in the network, IDSs based on RREQ mostly have simple computations and require fewer resources as compared to other methods.

4. Limitations of Intrusion Detection Techniques

By applying intrusion detection techniques in MANETs, we can face some problems due to their specific nature. In this section, we discuss some problems that can negatively affect the network performance in different ways.

4.1. Congestion

Some IDSs try to identify or locate malicious nodes by sending some additional or special packets (other than control packets) to all or some of the nodes involved in a route. In MANETs, topology changes frequently as nodes are free to move, so there will be plenty of special and control messages in the network that will cause congestion. This will put negative effect on the network performance by decreasing throughput due to increase in queuing delay and packet drop rate. Congestion will also increase FPR of the IDS, which detects wormhole attack by calculating the time duration.

4.2. Routing Delay

Routing delay is the time duration that is consumed during route discovery and route verification process before sending the actual data. If an IDS takes extra measures to establish and validate path between source and destination, then it will take considerable amount of time. Therefore, there will be an increase in the routing delay, which will affect the network performance directly.

4.3. Resource Overuse

Resource overuse means additional use of a resource by a node for any activity other than route finding and maintaining or transmitting data. Mobile nodes may have limited resources in terms of memory, storage, processing power, and battery life. If an IDS involves too much data and computations, then there will be more usage of memory and the processing power.

4.4. Special Hardware

Special hardware is any additional hardware that is used other than the hardware normally required for routing and data transfer. This special hardware may be in the form of a GPS device, special nodes containing extra features, or other special devices such as directional antennas etc. It may overuse resources and overall cost of the network will also be increased.

4.5. Mobility

Mobility is the key property of MANETs as nodes are free to move within the network. The IDS may block malicious nodes locally (from neighborhood) or network wide (from the whole network) by sending some block or trust messages. If an IDS avoids or blocks the malicious nodes locally, it will not work properly when the malicious node changes its position. Due to mobility, FPR of an intrusion detection technique based on location can be increased.

5. Comparative Analysis of Detection Features

In this section, we perform a logical comparison of wormhole detection techniques based on different features discussed in section 3. Table 1 shows the comparison of different detection features according to the limitations of IDSs. To detect wormhole attack, each node must have to perform some extra processing whatever the technique is used. So there will be resource overuse for every feature. Special hardware is required for location and time features, and promiscuous mode is required for features like data packets and route reply. Neighborhood and route reply are the features that will not work properly for nodes moving from one position to another. Data packets and neighborhood features will create congestion in the network and the techniques based on hop count will cause the routing delay in the network. If we have an overview of the detection features, we can say that the techniques based on features like location, time, and neighborhood are more expensive as compared to the techniques based on hop count, route reply, and route request in terms of cost, memory, and processing. In the similar way, the intrusion detection techniques, which have the limitation of congestion and routing delay are more acceptable as compared to the techniques having limitations such as resource overuse, special hardware, disability to handle mobile malicious nodes, and to declare normal nodes as wormhole. On the basis of this analysis, the best wormhole detection technique could be based on route request and with a little overuse of resources. Moreover, it should not deviate from the basic protocol and avoid any assumptions.

Table 1. Comparison of wormhole detection features.

Detection Feature	Congestion	Routing Delay	Resources Overuse	Special Hardware	Mobility
Location[5,6,9,12]	---	---	Yes	Yes	---
Time[5,8,10,13,15,17,19,20]	---	---	Yes	Yes	---
Hop Count[11,13,14,16,17,20]	---	Yes	Yes	---	---
Neighborhood[7,10,18]	Yes	---	Yes	---	Yes
Data Packets[12]	Yes	---	Yes	Yes	---
Route Reply[8,16]	---	---	Yes	Yes	Yes
Route Request[8,10,18]	---	---	Yes	---	---

6. Conclusion

Mobile Ad hoc Networks (MANETs) are infrastructure-less, self-configured, and self-maintained wireless networks. These networks have more security threats due to lack of central point of control as compared to fixed networks. Wormhole attack is one of the most severe routing attacks, which is launched by two colluding nodes by establishing a private channel between them. This paper presented the features that could be used to detect the wormhole attack. These features are discussed in detail with their pros and cons. The possible limitations of Intrusion Detection Systems (IDSs) are also discussed. This work provides a basis to build an efficient IDS to detect wormhole attacks in MANETs. According to our analysis, the techniques based on route request (RREQ) or hop count would be better than other techniques to detect wormhole attacks. As our future work, we plan to build an IDS for MANETs based on RREQ.

References

1. Perkins, C., Belding-Royer, E. Ad-hoc On Demand Distance Vector (AODV) Routing. *In IETF RFC 3561*, Mountain View, USA, July 2003.

2. Abolhasan, M., Wysocki, T., Dutkiewicz, E. A review of routing protocols for mobile ad hoc networks. *Ad Hoc Networks*, Volume 2, Issue 1, Pages 1-22, January 2004.

3. Imran, M., Khan, F.A., Abbas, H., Iftikhar, M. Detection and Prevention of Black Hole Attacks in Mobile Ad hoc Networks. *Security in Ad Hoc Networks (SecAN) Workshop, 13th International Conference on Ad-Hoc and Wireless Networks* (ADHOC-NOW), Benidorm, Spain, June 22-27, 2014.

4. Nagrath, P., Gupta, B. Wormhole attacks in wireless adhoc networks and their counter measurements: A survey. *3rd International Conference on Electronics Computer Technology (ICECT)*, April 8-10, 2011.
5. Hu, Y.C., Perrig, A., Johnson, D.B. Wormhole Attacks in Wireless Networks. *IEEE J. Sel. Area Comm.* Volume 24, Pages 370–380, 2006.

6. Hu, L., Evans, D. Using Directional Antennas to Prevent Wormhole Attacks. *In Network and Distributed System Security Symposium (NDSS 2004)*, San Diego, California, USA. February 2004.

7. Khalil, S., Shroff, N. B. LITEWORP: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks. *International Conference on Dependable Systems and Networks (DSN'05)*, pp. 612-621, 2005.

8. Chiu, H.S., Lui, K.S. DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks. *In Proc. International Symposium on Wireless Pervasive Computing*, Phuket, Thailand, January 2006.

9. Yun, J., Kim, I., Lim, J., Seo, S. WODEM: Wormhole Attack Defence Mechanism in Wireless Sensor Networks. *ICUCT 2006*, LNCS 4412, pp. 200–209, 2007.

10. Choi, S., Kim, D., Lee, D., Jung, J. WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks*. in Proceedings of IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC 2008)*, pp. 343-348, June 2008.

11. Hayajneh, T., Krishnamurthy, P., Tipper, D. DeWorm: A Simple Protocol to Detect Wormhole Attacks in Wireless Ad hoc Networks. *3rd International Conference on Network and System Security*, 2009.

12. Azer, M.A., El-Kassas, S.M., El-Soudani, M.S. An innovative approach for the wormhole attack detection and prevention in wireless ad hoc networks. *International Conference on Networking, Sensing and Control (ICNSC)*, pp.366-371, 10-12 April 2010.

13. Alam, M.R., Chan, K.S. RTT-TC: A topological comparison based method to detect wormhole attacks in MANET. *12th IEEE International Conference on Communication Technology (ICCT)*, pp.991-994, 11-14 November 2010.

14. Su, M.Y. WARP: A wormhole-avoidance routing protocol by anomaly detection in mobile ad hoc networks. *Computers & Security*, Volume 29, Issue 2, Pages 208-224, March 2010.

15. Shi, F., Jin, D., Liu, W., Song, J. Time-Based Detection and Location of Wormhole Attacks in Wireless Ad Hoc Networks. *IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pp.1721-1726, Nov. 2011.

16. Gupta, S., Kar, S., Dharmaraja, S. WHOP: Wormhole attack detection protocol using hound packet. *International Conference on Innovations in Information Technology (IIT)*, pp.226-231, 25-27 April 2011.

17. Shin, S., Halim, E.H. Wormhole attacks detection in MANETs using routes redundancy and time-based hop calculation. *International Conference on ICT Convergence (ICTC),* pp.781-786, 15-17 Oct. 2012.

18. Khan, Z.A., Islam, M.H. Wormhole attack: A new detection technique. *International Conference on Emerging Technologies (ICET)*, pp.1-6, 8-9 Oct. 2012.

19. Chaurasia, U.K., Singh, V. MAODV: Modified wormhole detection AODV protocol. *Sixth International Conference on Contemporary Computing (IC3)*, pp.239-243, 8-10 Aug. 2013.

20. Agrawal, N., Mishra, N. RTT Based Wormhole Detection Using NS-3. *International Conference on Computational Intelligence and Communication Networks (CICN)*, pp.861-866, 14-16 Nov. 2014.