International Journal of Security and Its Applications
Vol.9, No.7 (2015), pp.293-298
http://dx.doi.org/10.14257/ijsia.2015.9.7.26

Wormhole Attack in Mobile Ad-hoc Network: A Survey

Akansha Shrivastava and Rajni Dubey

Department of Computer Science Engineering
SRCEM, Banmore M.P
akanshasrivastav9oct@gmail.com, rajni.dubey04@gmail.com

Abstract

Security is the one of the major issue that exists in Mobile Ad hoc network. Mobile Ad hoc network is infrastructure less network so it is vulnerable to several security attacks that are on different layers. Wormhole attack is one of the serious routing attack on network layer. This paper focuses on the wormhole attack, its classification and the modes by which they are launched. This paper summarizes various detection techniques proposed for wormhole attack and also present the effect of wormhole attack on various performance parameters.

Keywords: *MANET, WORMHOLE*

1. Introduction

Mobile ad hoc network (MANET) is a type of ad hoc network, which is infrastructure less network. Mobile ad hoc network consist of a collection of wireless mobile nodes that are capable of communicating with each other. Nodes communicate with each other with the help of intermediate nodes. It has dynamic topology i.e. nodes are free to move independently, nodes can join or leave the network whenever needed. Though it is an infrastructure less network hence prone to many attacks.

MANET characteristics and key challenges are presented in [13].

Basically attack is defined as an attempt to destroy or disrupt the normal functionality of the network and violate the basic security goals such as confidentiality, authentication, integrity, availability and non-repudiation. Various security issues are present in Mobile Ad hoc networks [2]. Attacks are of two types: 1) **passive attack**- which does not destroy or disrupt network but uses the useful information, it violate confidentiality.

2) **Active attack**- which steal, destroy, manipulate the useful information and as well as disrupt the operations of network. Wormhole attack and black hole attacks are active attacks.

2. Wormhole Attack

Worm Hole attack consist of two nodes the attacker nodes that are connected to each other with a link basically this link is known as tunnel. The attacker node present in the network at one side captures the packet from the legitimate node and encapsulate the packet and with the help of tunnel transmit it to the other attacker node or malicious node present in the network. It consists of one or two malicious nodes and a tunnel between them.

Wormhole nodes fake a route that is shorter than the original one within the network means it create illusion for the legitimate node so they believe that the route is shorter than the original one. But it is not necessary that the route through wormhole nodes may be shorter. Figure 1 shows example of wormhole [1]. In given Figure 1, here we have two malicious node A and B connected with each other with the help of a link, the link can be

ISSN: 1738-9976 IJSIA

wired or wireless, the link is referred as tunnel, "the wormhole tunnel" through which attacker nodes communicate with each other and all traffic passes through this tunnel.

The tunnel can be formed via in-band channel or by out-of band channel or through high transmission power. In the Figure 1, node 3 and node 7 are represented as source and destination respectively. So now the source node 3 will forward the packet to the legitimate neighbour *i.e.*; node 2 in this way intermediate nodes between node 3 and node 7 *i.e.*, 2, 6, 5 will forward the packet from source to destination. In the absence of malicious nodes the legitimate path from node 3 to node 7 will be 3-2-6-5-7 so number of hops the packet travels is 3(three).

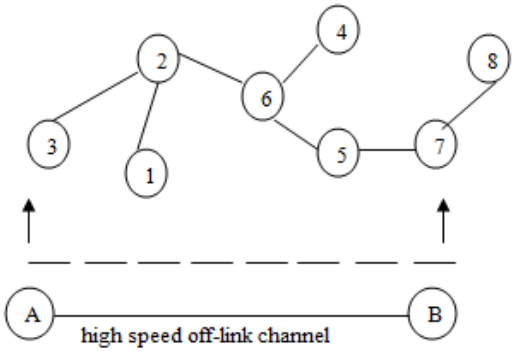

Figure 1. Example of Wormhole Attack

Now when wormhole nodes are present as well as they are malicious nodes so now the nodes A and B will get activated and these nodes create an illusion to source and destination that they are immediate neighbours and they can hear each other request so transmission take place between node 3 and node 7 via node A and node B.

3. Types of Wormhole Modes

The wormhole attack can be launched by given below modes they are listed below as;

Packet Encapsulation or In-band Channel: in this type of mode the malicious node captures the packet from legitimate node or source node and encapsulate the packet header of the original packet and destinate it to the other malicious node. After receiving the encapsulated packet the other malicious nodes either drop the packet or forward the packet to other nodes which are present in the network. The attacker nodes are within the network.

Out-of Band Channel: in this type of mode the malicious nodes are connected to each other via an outer link. A channel with high bandwidth is placed between the nodes at the two ends so as they can create wormhole link.

High Power Transmission: in this type of mode when the source node forward the packet the attacker node captures it and transmit it to the destination node with a high power, it enforces the nodes to follow the path (the wormhole link) and so that all traffic passes to this link.

4. Classification of Wormhole Attack

Recent studies has classified the wormhole attack on various ways, these attacks are classified on the basis of these ways they are listed below [1, 5].

In the way these nodes are implemented; The medium chosen by these nodes; In the way they attack; on the bases of their visibility.

Here discussing the type of attacks on their visibility bases. So they are classified simply as:

1. Open wormhole attack/ exposed

2. Half open wormhole attack
3. Closed wormhole attack/ hidden

Open Wormhole Attack: open wormhole attack is also known as exposed attack; in this type of attack the malicious node include their identity in the packet header. Whenever a node want to forward the packet it updates its packet header and encapsulate its identity the nodes follow the route discovery procedure. When the malicious node captures the packet it includes its identity in the packet header as the other authentic nodes do. Hence the legitimate nodes are aware of the presence of the wormhole nodes, these wormhole nodes may not be necessary be malicious. Here both the malicious nodes are visible.

Closed Wormhole Attack: also known as hidden attack, this of attack does not update the packet header at the time of route discovery process hence the legitimate nodes are unaware of their presence. These nodes capture the packet and transmit the encapsulated packet to the other malicious node with the help of tunnel. After receiving the packet the other malicious nodes either forward the packet or discard the packet. Here other the malicious nodes are invisible.

Half Open Wormhole Attack: in this type of attack the malicious node at one side of the network update its identity in the packet header at the time of route discovery process. Here one malicious node is visible and other is invisible to the legitimate nodes in the network.

5. Impact of Wormhole Attack

The impact of wormhole on the network is very severe, as it affects the overall performance of the network by decreasing the throughput of the network by dropping the packets. Not only it affect the throughput but also various parameters of the network.

6. Literature Review

Till now various techniques have been proposed for prevention and detection of wormhole attack.In [1], in this paper the impact of wormhole attack is descripted as well as a concise detail of wormhole attack and its types are explained. Also present various detection and prevention techniques. It explains how the network is affected and the throughput degrades as a result of dropping packets.

In [2], a review on prevention of wormhole attack in MANET is provided. Information related to the security issues is also included. Wormhole and its modes of operation and types are also explained in a concise and precise manner.

In [3], a method known as wormhole attack prevention (WAP) algorithm was proposed. In this method the node maintains a neighbour node table and monitors the behaviour of its neighbours. This method uses a special timer known as WPT. This method failed to detect the false positive alarm.

In [4], a concept called a complex wormhole is introduced to improve the wormhole attack. From the view point of attacker the author finds the pros and cons of particular mode. This paper provides the full image of the wormhole including the way they are operated as well as their classes. Also provide information related to the effect of wormhole on both the routing protocols (proactive and reactive).

In [5] and [6], the authors provide a deep study on wormhole attack and also explains the various proposed techniques for prevention as well as detection of wormhole attack. Explain the wormhole and its variants and the consequences this attack have on both types of routing protocols.

In [7], author introduced a method known as multi-layered detection mechanism for wormhole attacks in AODV. This technique is capable of detecting the wormhole nodes at the early stage of route discovery process, it is layered structures which consist of the four main layers in this approach and each layer in the architecture have a predefined tasks.

In [8], the author proposed a novel approach for securing AODV based MANET using neighbour node analysis approach against wormhole attack. In this approach for secure transmission nodes monitors its neighbour nodes behaviour. Each node maintains a table. It identifies the attack and also removes the wormhole link.

In [9], in this paper the author provides a comparative study on the evaluation of various performance parameters such as throughput, end to end etc. between the two routing protocols namely AODV AND DSR against wormhole attack.

In [10], in this paper the routing protocol DSR is modified to detect and prevent wormhole attack in MANET. The proposed approach concentrate on the detection of the malicious (misbehaving) nodes which are responsible for the occurrence of wormhole attack in network and try to figure out this attack. The performance parameter evaluated here are namely; jitter, throughput and delay.

In [11], this technique is an improvement to the previous method "WAP". The new technique is able to detect the false positive alarm known as WADP, (wormhole attack detection and prevention.). It provides the two way verification by integrating WADP with node authentication in modified AODV.

In [12], in this paper throughput performance analysis is carried out between the two attacks one is the wormhole and other is Sybil attack the routing protocol here is AODV. The analysis result shows that the wormhole attack is more severe than the Sybil attack.

In [13], this paper present a brief introduction to the three attacks namely, the wormhole, black hole and gray hole attack. For the analysis only two attacks the black hole and gray hole are considered. For this firstly two networks are established, one checks the behaviour of normal AODV protocol under various performance parameter and the other checks the behaviour of the protocol under some malicious behaviour.

In [14], in this paper an overview of wormhole attack as well as previous work is presented. A brief introduction to the reactive protocols namely, AODV, DSR, DYMO, ANODR is described. Paper focuses on the analysis of the behaviour of the protocol for the three modes namely; all pass, all drop and threshold of the wormhole attack in the mobility and non-mobility domain.

In [15], paper presents the overview of AODV routing protocol, and analysis the various security threats which affect the on demand routing protocols. Each security attack has been described here in brief.

In [16], a survey of wormhole attack in DSR routing protocol is done. Describes the various detection and prevention techniques and also provide solutions to these techniques.

In [17], this paper presents the two techniques one for the black hole attack and other for wormhole attack. An intrusion detection technique is to detect black hole attack in AODV and hop count analysis to detect and prevent wormhole attack.

The table 1 summarizes the various detection techniques for the wormhole attack in mobile ad-hoc network. The various detection techniques have been implemented to detect the presence of wormhole attack. In spite these detection techniques have several disadvantages too. Given table 1 represents the advantages and disadvantages of these techniques. .

Table 1 summarizes various detection techniques of wormhole attack [5-6]

Table 1. Summarizes the Detection Techniques

TECHNIQUES	ADVANTAGES	DISADVANTAGES
Distance and location based approach: geographical and temporal in (2003) [18],[19]	Both are proposed where strict clock synchronization and global positioning system coordinate all nodes.	Restrict the maximum transmission distance of packets.
Directional Antenna in (2004) [20]	Requires low synchronization.	Each node is equipped with special hardware. Directional errors.

LITEWORP in (2005) [21]	Guard node is used to detect the wormhole if one of its neighbour is behaving maliciously.	Not always possible to find guard node for particular link.
SAM(Statistical analysis method) in (2005) [22]	No need of synchronization. Clustering needed for mobility. PAM function is used.	False alarm is not handled.
Delphi in (2006) [23]	Detects both hidden and exposed attacks.	Can't detect the location wormhole and False alarm.
HMTIs in (2006) [24]	No synchronization. False alarm is detected.	Jitter to be calculated. Can detect only short ranged wormhole.
EDWA in (2006) [25]	For both detection and identification. No need of clock synchronization. No special hardware required.	Effective only when both source and destination are near.
WAP(Wormhole attack prevention) in (2008) [3]	Synchronization needed only at source node. Detect both hidden and exposed attack.	Failed to detect false positive alarm.
DAW(Detecting wormhole attack) & SAW(Security against wormhole) in (2008 & 2009) [26],[27] resp.	Trust based model is used to detect intrusion. Arithmetical method analysis wormhole attack. Also identifies wormhole tunnel.	Failed to detect false alarm detection.
MLDW in (2013) [7]	Allow early detection of wormhole attack during the route discovery phase. Doesn't require special hardware or clock synchronization.	Maximum overhead.
WADP in (2014) [11]	Detect false positive alarm.	Failed to detect of hidden attack

7. Conclusion

This paper present an overview of wormhole attack, explains the type of attack and the modes by which they are operated and also the impact of wormhole attack on network. It provides the concise and precise description of wormhole attack. Paper also focuses on the various ways to detect and prevent this attack, describes the effect of wormhole attack on the various performance parameters. Hence we can conclude that the security against wormhole attack is a challenging task as various techniques have been implemented and proposed but still it is very severe attack.

References

[1] S. Upadhyay and B. K. Chaurasia, "Impact of wormhole attacks on MANETs", International Journal of computer science & Emerging Technologies (E-ISSN: 2044-6004) vol. 2, no. 1, (**2011**) February.
[2] P. Sharma, H. P. Sinha and A. Bindal, " A Review on Prevention of Wormhole Attack in Mobile Ad-hoc Network ", International Journal of Research in Information Technology, vol. 2, no. 3, (**2014**) March.
[3] C. Sun K, Doo-Young, L .Do-hyeon, and J. Jae-il, "WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks," in proceedings of 2008 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC 2008).
[4] M. Azer, S. El-Kassas and M. El-Soudani," A Full Image of the Wormhole Attacks Towards Introducing Complex Wormhole Attacks in wireless Ad Hoc Networks," International Journal of Computer Science and Information Security, vol. 1, no. 1, (**2009**) May.
[5] R. Maulik and N. Chaki," A comprehensive Review on Wormhole Attacks in MANET", in proceeding of 9th International Conference on Computer Information Systems and Industrial Management Applications, (**2010**), pp. 233-238.
[6] R. Maulik and N. Chaki," A Study on Wormhole Attacks in MANET", in International Journal of Computer Information Systems and Industrial Management Application ISSN 2150-7988 volume 3 (**2011**) pp. 271-279.

[7] C. P. Vandana and A. F. S. Devaraj, "MLDW- A MultiLayered Detection mechanism for Wormhole attacks in AODV based MANET", in International Journal of Security, Privacy and Trust Management (IJSPTM) vol. 2, no. 3, (**2013**) June.
[8] S. Goyal and H. Rohil, "Securing MANET against Wormhole Attack using Neighbour Node Analysis", in International Journal of Computer Applications (0975-8887) vol. 81, no. 18, (**2013**) November.
[9] R. Ahuja, A. B. Ahuja and P. Ahuja," Performance Evaluation and Comparison of AODV and DSR Routing Protocols in MANETs Under Wormhole Attack", in proceedings of the 2013 IEEE Second International Conference on Image Information Processing (ICIIP-2013).
[10] Y. Singh, A. Khatkar, P. Rani, Deepika and D. D. Barak," Wormhole Attack Avoidance Technique in Mobile Ad hoc Networks", in Third International Conference on Advanced Computing & Communication Technologies, (**2013**).
[11] J. Biswas, A. Gupta and D. Singh, "WADP: A Wormhole Attack Detection and Prevention Technique in MANET using Modified AODV routing Protocol", 9th International Conference on Industrial and Information Systems (ICIIS), (**2014).**
[12] Z. Kasiran and J. Mohamad, "Throughput performance Analysis of the Wormhole and Sybil Attack in AODV", Fourth International Conference on Digital Information and Communication Technology and its Application Publication, (**2014**), pp. 81 – 84.
[13] M. K. Parmar and H. B. Jethva, "Analyse impact of malicious behaviour of AODV under performance parameters", in International Conference on Advanced Communication Control and Computing Technologies (ICACCCT), (**2014**).
[14] G. Garg, S. Kaushal and A. Sharma, "Reactive protocols analysis with wormhole attack in ad-hoc networks", in International Conference on Computing, Communication and Networking Technologies (ICCCNT), (**2014**).
[15] A. K. Abdelaziz, N. Mehdi and G. Salim, "Analysis of security attacks in AODV", in International Conference on Multimedia Computing and Systems(ICMCS), (**2014**).
[16] H. Kumari, G. Vyas and S. Dhankar," A Survey of Wormhole Detection and Prevention Technique in DSR Protocol", in International Journal of Engineering, Management & Science (IJEMS), (**2014**).
[17] K. Patidar and V. Dubey, " Modification in routing mechanism of AODV for defending black hole and wormhole attacks", Conference on IT in Business, Industry and Government (CSIBIG), (**2014**).
[18] Y. C. Hu, A. Perrig and D. B. Johnson, "Packet Leashes: A Defence against Wormhole Attacks in Wireless Ad Hoc Networks", In IEEE INFOCOM, (**2003**).
[19] S. Capkun, L. Buttyan, and J. Hubaunx, "SECTOR: Secure Tracking of Node Encounters in Multi-hop Wireless Networks", In proceedings ACM Workshop on security of Ad Hoc and sensor networks, (**2003**).
[20] L. Hu and D. Evans", "Using Directional Antennas to prevent Wormhole Attacks", In Network and Distributed System Security Symposium, San Diego California, USA, (**2004**).
[21] I. Khalil, S. Bagchi and N. B. Shroff, "LITEWORP: A lightweight countermeasure for the wormhole attack in multihop wireless networks", In Proceedings of International Conference on Dependable Systems and Networks, (**2005**).
[22] N. Song, L. Qian and X. Li, "Wormhole Attacks Detection in Wireless Ad Hoc Networks: A Statistical Analysis Approach", In Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium, (**2005**).
[23] H. S. Chiu and K. Lui, "DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks", In Proceedings of International Symposium on Wireless Pervasive Computing, (**2006**), pp. 6-11.
[24] M. A. Gorlatova, P. C. Mason, M. Wang, L. Lamont and R. Liscano, "Detecting Wormhole Attacks in Mobile Ad Hoc Networks through Protocol Breaking and Packet Timing Analysis", In IEEE Military Communication Conference, (**2006**).
[25] X. Wang and J. Wong, "An End-to-End Detection of Wormhole Attack in Wireless Ad-hoc Networks", Department of Computer Science Iowa State University, (**2007**).
[26] K. S. Win, "Analysis of Detecting Wormhole Attack in Wireless Networks", World Academy of Science, Engineering and Technology, vol. 48, (**2008**), pp. 422-428.
[27] M. S. Sankaran, S. Poddar, P. S. Das and S. Selvakumar, "A Novel Security model SaW: Security against Wormhole attack in Wireless Sensor Networks", In Proceedings of International Conference on PDCN, (**2009**).

