ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
Vol. 2, Issue 11, November 2015

Wormhole Attack in Mobile Adhoc Network and Its Detection Countermeasures

Parvinder Kaur[1], Dr. Dalveer Kaur[2], Dr. Rajiv Mahajan[3]

Research Scholar, Department of Research Innovation and Consultancy, PTU, Jalandhar, Punjab [1]

Assistant Professor, PIT University Campus, PTU, Jalandhar-Kapurthala Highway, Punjab, India. [2]

Professor, GIMT, Amritsar, Punjab, India [3]

Abstract: In any network the priority is to establish communication between the nodes. The Mobile Adhoc Network being wireless adhoc network is prone to many types of attacks. Wormhole is one of the security breaching attack that doesn't require any special type of resource to launch it .Wormhole makes itself the part of the legal path without giving of warning and try to disrupt the communication. In this paper we analyze the wormhole attack, types and detection countermeasures.

Keywords: Wormhole, Inbound, Outbound, Delphi, MAODV.

I. INTRODUCTION

Mobile Adhoc Networks are networks which maintain themselves because it is wireless type of networks. These types of networks are formed when the need arises. Each mobile node is self sufficient with resources that require communicating within the network. This type of networks are cost effective but has limited bandwidth, speed memory type of resources [1]. Due to mobilization nature of manet; it is prone to many types of attacks. In this communication take place within the radio transmission range. In Manet the transmission and communication occur in unsecure network. The data can be easily hacked or modified by the hackers. Nodes are joining and leaving the network anytime.

So the network is prone to different attacks like rushing, blackhole, DDOS, byzantine, wormhole [1].Wormhole attack is security breaching attack. In normal routing data transfer take place by authorized nodes whatever legal path is created in the routing table that path is followed by the source to destination. But in the wormhole the malicious node become the part of legal path and wormhole try to disrupt the regular or normal communication [2].

II. WORMHOLE ATTACK

Wormhole attack is one of the serious attack on the routing protocols.

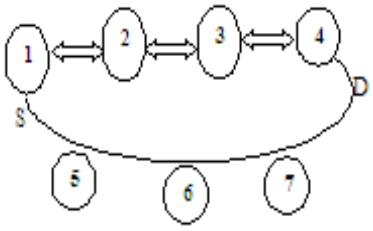
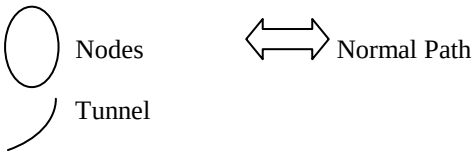


Fig. 1. Wormhole Attack in Manet



In wormhole attack, two colluding nodes are placed between source and destination. These nodes are known as malicious nodes which are responsible for the creation of the shortest path. The long tunnel is formed by using the long range radio transmission medium. This shortest path or tunnel created by the malicious nodes is known as wormhole attack. Wormhole attack is also known as silent attack because nodes are part of the legal path.

III. TYPES OF WORMHOLE ATTACK

On the basis of the transmission medium and its affect on the data, wormhole attack is divided into two parts.

A. Inbound Wormhole Attack

An inbound is also known as hidden attack. The nodes create the long tunnel by hiding their identity in the created path [3] .The tunnel is formed using long wireless range. It is more harmful attack. Inbound wormhole attack is difficult to identify.

B. Outbound Wormhole Attack

An Outbound wormhole uses the long range transmission medium to set this type of attack [3]. The long tunnel is created by two colluding malicious node. Nodes are part of the created path. But the legal nodes can't judge that there exists malicious nodes in the created path.

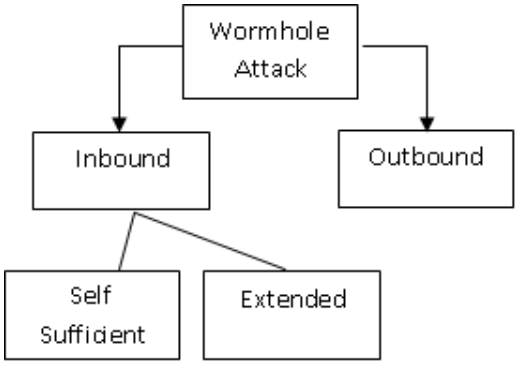


Fig. 2. Types of Wormhole Attack in Manet

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 2, Issue 11, November 2015

IV. METRICS TO DETECT WORMHOLE ATTACK

Wormhole presence in the routing protocol can be measured based on different metrics which are defined as follow:

A. *Strength*

It defines the amount of traffic attracted by malicious nodes known as wormhole attack [1] [3]. The larger the traffic attracted stronger is the wormhole attack.

B. *Attraction*

It defines the decrease in the path length. Smaller attraction means wormhole attack is strong [1] [3].

C. *Length*

Length defines the difference between original and advertised path [1] [3].

D. *Robustness*

Robustness defines persistence of wormhole attack in case of topology changes [1] [3].

V. WORMHOLE AFFECTS ON DATA

Wormhole is responsible to change the flow of the data between sources to destination. Wormhole can affect the data transfer by different means which are as follow:

A. Route Change:

A malicious node hack the data from one location and can change the original path between source and destination.

B. Eavesdropping

Wormhole may intercept private line so as to harm the private data carried through the private lines.

C. Unknown Destination

Wormhole can transfer the data to unknown destination that is not a part of the path or network.

D. Spy on Information

Wormhole can spy on the legal contents to know the secret activities performed between the neighbour nodes.

E. Decrease the Hop Count of Nodes

Wormhole is responsible for decreasing the hop count value between source to destination. Hop count defines the number of nodes destination away from the source.

F. Slow Down the Network Speed

The main purpose of wormhole attack to disrupt the transfer of data between source to destination. The disruption can be created by slowing down the data transfer between nodes.

G. Jamming of Data

Wormhole is also responsible for blocking the data from source to destination.

VI. WORMHOLE DETECTION COUNTERMEASURE

A. *Local Connectivity Based Algorithm*

To detect the wormhole attack the required information is that the volume of nodes must know the information about the neighbouring nodes [4]. In this method no cryptography, H/W Synchronization is needed. In this each node maintains the information about neighbours of neighbours. If the hop count of any node becomes three that node is wormhole node because each node can have only two common neighbours.

B. *MAODV*

Modified Wormhole Detection is based on AODV protocol. It uses the concept of both hop count and delays [5]. Because the delay for the nodes under the wormhole is more than the delay of total number of nodes in the legal path.

In this time stamp value is not changed by the intermediate nodes because it is only changed by the sender only. Based on this, time delay can be calculated for the legitimate and wormhole.

C. *Delphi(Delay Per Hop)*

It is known as delay per hop attack. The user attempt is to analyse wormhole attack using the delay parameter. Delphi works at the sender location. In Delphi, sender attempt to collect the delay, hop and the disjoint paths information from source to destination. DREP and DREQ messages are send to collect the information [6].

These two packets are forwarded three times and collect the information about the path which has loss hop count because the delay per hop is more in this case.".

D. *AODMV*

In this first source try to find the paths which are connected or which are not connected by broadcasting to the neighbours [7]. Every time same path is used for sending the message.

1. In the first step, there are multiple paths from source to destination. Then source stores the multiple path information in its routing table for future reference .Based on the time value of two available paths the round trip time of third established paths can be calculated.

2. In the second step, calculate the RTT of all the neighbour nodes which are one hop away from the source. In this step we actually calculate the total travelling time of the packet.

3. In the third step, calculate the average of all the one hop nodes of source. This calculated time is known as maximum round trip time (RTT) for one hop node.

4. In the forth step, Multiple maximum round trip time with established hop path .It will give time to travel the packets from source to destination.

5. In the fifth step, compare the total RTT with estimated round trip time. If total time is less than the estimated time than there is no wormhole otherwise there is wormhole.

6. After finding the wormhole that particular path is marked as a wormhole .It is known as blacklisting.

DOI 10.17148/IARJSET.2015.21112

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 2, Issue 11, November 2015

TABLE I

Wormhole Detection Scheme	**Requirements**	**Comment**	**Future Work**
Local Connectivity Based	Based on Density of Nodes.	Usable for detect wormhole attack within the unit disk graphs.	Work can be expanded non-unit graphs also.
MAODV	Based on Time stamp.	Usable for detect Inbound/Outbound types of attacks.	Enhancement of algorithm it should be able to detect the wormhole in case all the paths are affected by wormhole.
Delphi	Based on the Hop Count and Delay.	Usable for detect both kind of wormhole attacks Inbound/Outbound.	Message overhead is more because of additional DREQ and DREP are used. Both are forwarded three times to check the reliability and wormhole attack. so there is a need to decrease the header size in case of wormhole.
AODMV	Based on Averaging of RTT established source path.	Usable to detect the wormhole attack in Mobile Adhoc Network and Wireless Adhoc Network.	Simplification in method calculation is required.

VII.CONCLUSION

In this paper, we have presented wormhole attacks, its types, affects and detection schemes. Each solution is itself self sufficient to detect the wormhole attack. But these algorithms can be made more efficient by doing research on the drawbacks in the future.

REFERENCES

[1] Maulik, R., & Chaki, N. (2010, October). A comprehensive review on wormhole attacks in MANET. In Computer Information Systems and Industrial Management Applications (CISIM), 2010 Int'l Conference on (pp. 233-238). IEEE.
[2] Ghanbarzadeh, Y., Heidari, A., & Karimpour, J. (2012). Wormhole Attack in Wireless Ad hoc Networks. International Journal of Computer Theory And Engineering, 4(2).
[3] Mahajan, V., Natu, M., & Sethi, A. (2008, November). Analysis of wormhole intrusion attacks in MANETS. In Military Communications Conference, 2008. MILCOM 2008. IEEE (pp. 1-7).IEEE.
[4] Maheshwari, R., Gao, J., & Das, S. R. (2006, September). Detecting wormhole attacks in wireless networks. In Wireless Mesh Networks, 2006. WiMesh 2006. 2nd IEEE Workshop on (pp. 109-111). IEEE.
[5] Chaurasia, U. K., & Singh, V. (2013, August). MAODV: Modified wormhole detection AODV protocol. In Contemporary Computing (IC3), 2013 Sixth International Conference on (pp. 239-243). IEEE.
[6] Chiu, H. S., & Lui, K. S. (2006, January). DelPHI: wormhole detection mechanism for ad hoc wireless networks. In Wireless pervasive computing, 2006 1st international symposium on (pp. 6-pp). IEEE.
[7] Raju, V. K., & Kumar, K. V. (2012, September). A simple and Efficient mechanism to detect and avoid wormhole attacks in mobile ad hoc networks. In Computing Sciences (ICCS), 2012 International Conference on (pp. 271-275) IEEE.