Survey on Intrusion Detection System for Wireless Ad-hoc Network

Sameeksha Jain
CSE Department
AITR, Indore [M.P]
India

Amit Jain
CSE Department
AITR, Indore [M.P]
India

ABSTRACT
MANETs suffer from performance and security issues. Many contributions have been proposed but they are not sufficient to enhance the security and performance. Therefore the presented paper investigate techniques of wormhole attack deployment over wireless ad hoc network, and efforts made to avoid these attack .Finally a new IDS is presented for securing network as well as improving the performance in terms of routing overhead and throughput.

Keywords
MANET, Wormhole Attack, EAACK IDS, Delay per Hop, Hop count.

1. INTRODUCTION
MANET is a collection of node that forms a temporary network in which each node is connected to other node via a wireless link without any fixed infrastructure and centralized control [1]. In this wireless network nodes are free to move anywhere in network. Demands of this wireless network increase because wired network is expensive to deploy in some area like disaster area [2]. Major issues of MANET are related to power constraint, security, radio interference, node mobility, service discovery, bandwidth constraints, QOS and routing [3]. MANET used to solve many real life problem like communication in emergency response system, military and police network, personal area network, disaster area, conference and mining operation [4].

MANET divides the network into two types: Single hop and Multi hop. When two nodes are not in communication range of each other than they send data via intermediate nodes, [5]. Here we are considering AODV routing protocol, it is a reactive routing protocol in which nodes discover a path whenever it required. So For sending a data packet from source to destination they firstly need to find a route between the nodes. Such that at the time of routing it is easy for an attacker to attack the network because in MANET nodes can move anywhere in network and can also join and leave it. Thus, due to mobility malicious node can easily insert in the network.

A wormhole is nothing but shortcuts for long journeys across the universe. With the help of wormhole any one can go from one part of universe to another in short time. Wormholes are the theory of general relativity. But wormholes come up with, high radiation, due to the dangers of sudden collapse and dangerous contact with exotic matter [6]. A wormhole has at least two holes which are connected to a tunnel. Worm hole

Can connect two object/system for short time, worm hole link is not permanent they are temporary [7]. It is like a survey system that you might used in city where you going into a whole and came out from the other ends. For example Mouse hollows a surface and enters from one ends and come out from the other ends.

If the wormhole is traversable, object can travel from one hole to the other by passing through the tunnel. Traversable wormholes would allow object to travel from one part of the universe to another part of that same universe known as Intra universe or would allow travel from one universe to another universe called Inter-universe. Travelling through a wormhole link takes less time than travelling between the same distances in normal space [8]. We can say that wormhole is a shortcut to reach the destination, for example if we want to go from one place to another place than we choose a shortest path so we could reach earlier, so worm hole is like that.

2. BACKGROUND
In this chapter, we are discussing wormhole attack, method to deploy them, or types of wormhole attack.

2.1 Wormhole Attack
In wormhole attack a malicious node receives packets at one location in the network and transfer to another location in the network, where these packets are retransmitted to the network. In this, link is established between colluding node for sending data packet and it could be established via wired link or wireless link between two colluding attacker and create a illusion that they are one hope neighbour but in reality they are not neighbour. When node transfer a data via wormhole link than attacker are able to gain the confidential information, or drop the packet [9].

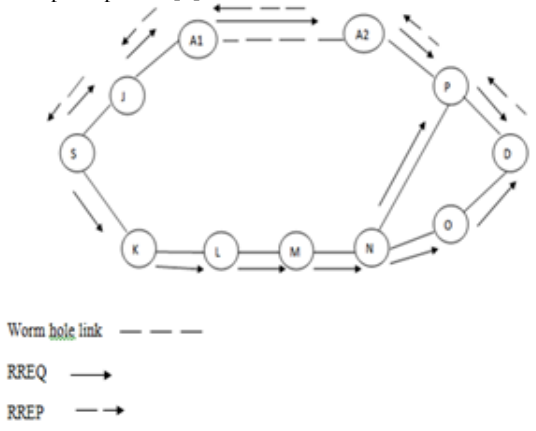

Fig 1: Wormhole Attack [10]

Fig 1 shows an example of the wormhole. In the figure, A1 and A2 are two attackers that are connected by high speed channel. When source S wand to send a packet to destination D than it send a RREQ packet for finding a route between source to destination, According to figure 1, S send a RREQ packet to its immediate neighbors J and K, J and K receive a

packet and send it to their neighbors. And node A1 which is the neighbor of J when Received the RREQ packet than it send a RREQ packet to the colluding node A2 via high speed channel, A2 rebroadcast the RREQ to its neighbor P, request which passes through a wormhole link reach at destination first because colluding node are connected through high speed channel. So D will choose route and send a RREP via a path D-P-J-S and ignore the other RREQ that arrive later. Then S sends a data packet via a path S-J-P-D to destination D.

2.2 Deployment of Wormhole Attack

Tunnel can be established between nodes by Packet Encapsulation, out of band hidden channel and high transmission power [11].

- **Wormhole using Packet Encapsulation:** This method work in hidden mode. Here several nodes exist between two malicious nodes and data packets are encapsulated between the malicious nodes. Hence it prevents nodes from incrementing hop counts. The packet is converted into original form by the second end point. This mode of wormhole attack is not difficult to launch since the two ends of wormhole do not need any cryptographic information, or special requirement such as high-power source or high bandwidth channel to launch a wormhole attack [12].
- **Wormhole using high power transmission:** It can launch by single malicious node which has a high transmission capability to attract the traffic, so legitimate nodes choose a path that contain malicious node for transfer the packet. The chances of malicious nodes present in the routes established between sender and destination node increases in this case. Also this type is referred as "black hole attack" in the literature [12].
- **Wormhole using Packet Relay:** One or more malicious nodes can launch packet-relay-based wormhole attacks. In this type of attack malicious node deliver data packets between two distant nodes and this way it creates illusion that two nodes are neighbor. This kind of attack is also called as "replay-based attack" in the literature [12].
- **Wormhole using Protocol Distortion:** In this type of mode, single malicious node attract the traffic for passing through it by distorting protocol rule, like nodes have to wait for sometimes before retransmitting. But malicious nodes don't follow this rule and retransmitted a packet again and again so it could reach to the destination first, Even if any request reaches the destination later. They will be dropped by destination [12].
- **Wormhole using out of band:** This two ended wormhole, a dedicated high bandwidth channel between two end points to form wormhole link [12].

2.3 Types of Wormhole Attack

Wormhole attacks are classified using different criteria based upon:

1) Its Implementation, 2) The medium used, 3) The attackers and 4) The location of victim nodes.

2.3.1 Classification based upon Implementation:

This is the major classification; Based upon implementation wormhole attacks can be classified into the following types. This classification relies upon the ways the attack is launched.

- **Using Encapsulation:** In this mode there a several node exist b/w malicious node, in this type of mode separate tunnel doesn't establish b/w malicious node ,and packet is transferred by normal path, Here attacker hide themselves in routing path means source doesn't know that malicious node present in routing path [2].
- **Using out-of-band channel:** This type of attack launch in participation mode. It uses an out of band channel between malicious nodes. This channel can be established by using a long range wireless link or a wired link. This type of attack is very challenging to launch and it required specialized hardware to deploy. Consider the scenario depicted in Figure 2 [2].

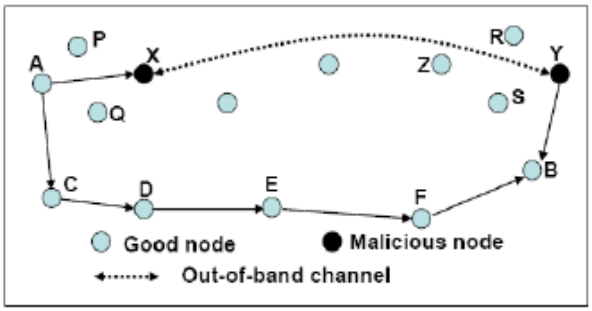

Fig 2: Wormhole attack using out of band channel [12]

Node A sends a RREQ to node B, and nodes X and Y are malicious nodes having an out-of-band channel between them. Node X tunnels the RREQ to Y, Node Y broadcasts the packet to its neighbors B. B gets two RREQs—A-X-Y-B and A-C-D-E-F-B. The first RREQ has lesser hop count than second one so it is chosen by B.

- **Using high power transmission:** Another type of attack Is launch by using high power transmission. It can launch by single malicious node, here when malicious node receive a RREQ packet it transfer the packet with high transmission capability (and this capability does not present to other node) to other node so it could reach to the destination first [2].
- **Worm hole using packet relay:** This is an another type of worm hole attack in which a malicious node relays packets between two far nodes and create a fake neighbor. It can launch by single and two or malicious node. For ex. Here Malicious node are representing by M, If we talk about attack which launched by single malicious node M and M within the transmission range of nodes A and B but nodes A and B doesn't exist in the transmission range of each other, here node transfer a data packet via a node M but nodes don't aware that node M is exist between them. Nodes A and B Feels that they are one hop away of each other. Than Node M can drop the packets or break this link. , In case of two colluding nodes M and M' are connect through a wired and wireless link and create a illusion that they are neighbors [2].

- **Via protocol deviations:** The attackers in such case create the wormhole by distorting the protocol rules, e.g. some of the protocols assume the nodes to wait for some time before retransmitting. But the attackers do not comply with this rule and keeps on broadcasting without back off and thus trying to arrive first at the destination and thereby avoiding any future legitimate requests to reach destination. Even if any other requests reach destination, they will be dropped, since a request passing through the colluder has already been received. Please note that some protocols only anticipate the first request and drops all copies of the same request that arrive in future [2].

2.3.2 Classification based upon Medium Used:

Wormhole attacks can be also classified as In-Band and Out-of-Band wormhole attacks.

- **In-band wormhole:** This attack launch in hidden mode. Attackers are using following methods for creating link between them e.g. Encapsulation, Packet relay and Protocol deviations [2][13].
- **Out-Of-Band Wormhole:** This attack launch in participation mode. Attackers are using following method to create a link between them e.g. Out-Of-Band Channel and High Transmission Mode [2][13].

2.3.3 Classification based upon Attackers:

- **Self-Sufficient:** Where colluders advertise themselves as normal nodes, all paths passes through them e.g. out-of-band channel or using high power transmission. Our approach focuses on detection of such type of wormhole nodes and attacks [2].
- **Extended Wormhole:** The colluders are hidden by themselves and extend the attacks beyond themselves to normal nodes e.g. encapsulation or packets relay [2].

2.3.4 Classification based upon location of Victim nodes.

- **Simplex:** Targeted node lies in range of only one attacker [2].
- **Duplex:** Targeted node lies in range of both the attackers [2].

2.4 Another type of Wormhole Attack

There are three types of wormhole attack closed, half open, and open. In which S and D are the source and destination nodes respectively. Nodes M1 and M2 are malicious nodes.

- **Open Wormhole**: In this type of attack both malicious node M1 and M2 are visible, nodes aware about the presence of malicious node, In this malicious node doesn't hide themselves in RREQ packet header [14].

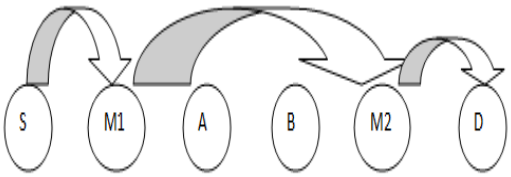

Fig 3: Open Wormhole [15]

Consider the scenario depicted in figure 3. Node M1 and M2 are visible and nodes A and B that exist between Malicious nodes M1 and M2 are kept hidden, so source(S) sends packet to destination(D) via the path S-M1-M2-D

- **Half-Open Wormhole**: In this one side of malicious node is hidden and other side of node is visible [14].

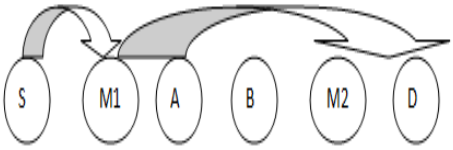

Fig 4: Half open Wormhole [15]

In this route discovery procedure, malicious node M1 is visible, although second node M2 is kept hidden, and node between M1 and M2 is also kept hidden. So packet is sent via path S-M1-D, Malicious nodes don't modify the content of packet they simply tunnel them from one location to other location [14].

- **Close Wormhole:** In this type of attack both malicious node M1 and M2 and the nodes exist between M1 and M2 are kept hidden. In this both source and destination node assume that they are direct neighbor .The attackers do not modify the content of the packet. Just, they simply transfer the packet form one side of wormhole to another side and it rebroadcasts the packet [14].

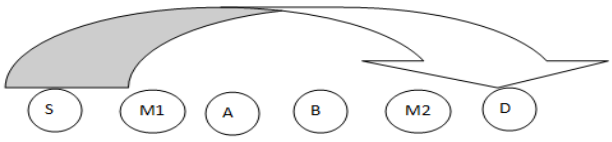

Fig 5: Close Wormhole Attack [15]

3. PROPOSED WORK

This chapter includes the involved work and the identified issues in the EAACK IDS. Here, we proposed new IDS that overcome the deficiency of EAACK and provide detection and prevention from the wormhole attack.

Here we identified the problem in EAACK (enhanced adaptive acknowledgement),which is an extension of AACK (Adaptive acknowledgment).This approach is designed to solve the three weakness of watch dog like limited transmission power, false misbehavior and receiver collision. It uses the concept of digital signature to prevent the attacker from forging acknowledgement packet. EAACK method work in 3 phases i.e. ACK, S-ACK, and MRA.

ACK is an end to end acknowledgement scheme. Its aim is to reduce network overhead, when no misbehavior node is detected. In case when misbehaving node is found than source switch to the S-ACK phase. Here every three consecutive node work together to prevent the misbehaving node. For every three consecutive node third node send an S-ACK packet to sender [16].

It addresses the following issues:

1. As per the previous method that are discussed above, we observed the issue in existing IDS that is network overhead which occurred because all acknowledgment packets are digitally signed before they are sent by destination node.
2. Existing IDS System which prevent forged acknowledgement and detect the malicious node. But it's not able to remove them. So we are proposing the new IDS that can reduce the network overhead and also can detect and remove the wormhole node.

For solving this problem we used a concept of DIFFIE HELLMAN Key Exchange Algorithm that reduces the network overhead. In this scenario sender and destination node both agree on the same key. After that Sender sends a packet which is encrypted by key that is shared between sender and destination node. So no one except destination node is able to decrypt the message, and no one will be able to modify the packet.

We can detect worm hole attack by collecting both the number of hops and delay per hop information for different path from source to destination because under legitimate situation delay for each packet is same along each hop. But in case of worm hole attack delay per hop increases because one or more node is present between malicious nodes or it is connected by the long wireless or wired link. If delay per hop of path is higher than the other path and number of hop count is less than it is known as wormhole path [17].

Here we introduced two steps for detecting the wormhole attack and for reducing the network overhead are:

1. **Step 1:**First of all both sender and destination node agree on key by using Deffie Hellman key exchange method, than sender send the dummy packet containing previous hop field, hop count and timestamp field at the time of route discovery that are encrypted by key which is shared between sender and destination node. Intermediate nodes add a packet which contains hop count and previous hop field.

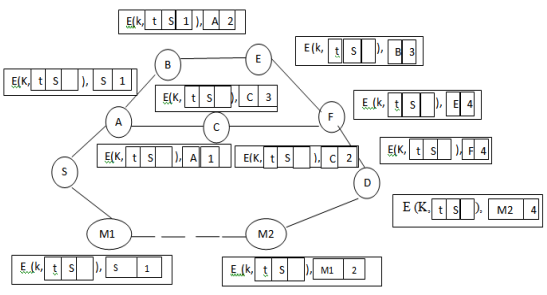

Fig 6: Request Roadmap

2. **Step 2:** When destination node get the requested packet than it doesn't immediately reply to requested path, instead firstly it collect the information of each route from source to destination and start detecting processes by comparing the time that is taken for sending the request along with number of hop for each path. If path has larger delay and smaller hop count than another path then this path is under wormhole attack. So destination node reply for only one path that has less delay and least number of hops. At the end this reply is again encrypted by a key that is shared between sender and destination.

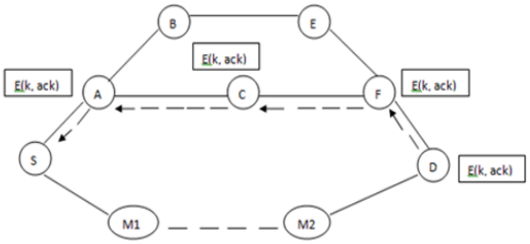

Fig 7: RREP Roadmap

4. CONCLUION AND FUTURE WORK

Wormhole attack is a complicated attack in MANET, which either drops the packet or halts the network. Here we discuss different type of wormhole attack and method to deploy them. Additionally observe the impact of attack in network, and also discussed the method to prevent attackers. Finally the key issues are addressed as network overhead. Moreover it a solution is introduced that could overcome the network overhead of EAACK IDS and also prevent worm hole attack, by using delay per hop and hop count information. In addition, overhead is reduced by using DIFFIE HELLMAN key exchange method. In future we implement the proposed concept using network simulator 2 environment and their performance analysis is reported.

5. REFERENCES

[1] Vandana C.P, Dr. A. Francis Saviour Devaraj "Evaluation of Impact of Wormhole Attack on AODV" Int. J. Advanced Networking and Applications Volume: 04 Issue: 04 Pages: 1652-1656 (2013) ISSN : 0975-0290.

[2] Zubair Ahmed Khan, M. Hasan Islam," Wormhole Attack: A new detection technique"978-1-4673-4451-7/12/$31.00 ©2012 IEEE

[3] Soo-Young Shin,Eddy, Hartono Halim "Wormhole Attacks Detection in MANETs using Routes Redundancy and Time-based Hop Calcu lation.

[4] Xia Wang, Johnny Wong "An End-to-end Detection of Wormhole Attack in Wireless Ad-hoc Networks" 2007 - ieeexplore.ieee.org

[5] T Divya Sai Keerthi,Pallapa Venkataram,"Locating the Attacker of Wormhole Attack by Using the Honeypot" 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications.

[6] http://www.space.com/20881-wormholes.html, by Nola Taylor Redd, SPACE.com Contributor | April 13, 2015 04:53pm ET

[7] https://wiki.eveonline.com/en/wiki/Wormholes

[8] http://www.slideshare.net/ayanbanerjee3517/wormholes

[9] Athira V Panicker, Jisha G," Network Layer Attacks and Protection in MANET A Survey" Athira V Panicker et al, (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 3437-3443

[10] Bounpadith kannhavong, hidehisa nakayama, yoshiaki nemoto, and nei kato," a survey of routing attacks in mobile ad hoc networks" 1536-1284/07/$20.00 © 2007 IEEE **85.**

[11] Yudhvir Singh, Avni Khatkar, Prabha Rani, Deepika, Dheer Dhwaj Barak "Wormhole Attack Avoidance Technique in Mobile Adhoc Networks", 978-0-7695-4941-5/12 $26.00 © 2012 IEEE

[12] Mohit Jain, Himanshu Kandwal," A Survey on Complex Wormhole Attack in Wireless Ad Hoc Networks", 2009 International Conference on Advances in Computing, Control, and Telecommunication Technologies.

[13] Viren Mahajan, Maitreya Natu, and Adarshpal Sethi,"analysis of wormhole intrusion attacks in manets"978-1-4244-2677-5/08/$25.00 ©2008 IEEE.

[14] Vikas Kumar Upadhyay, Rajesh Shukla," An Assessment of Worm Hole attack over Mobile Ad-Hoc Network as serious threats", Int. J. Advanced Networking and Applications Volume: 05 Issue: 01 Pages:1858-1866 (2013) ISSN : 0975-0290.

[15] Priya maidamwar and nekita chavhan "a survey on security issues to detect wormhole attack in wireless sensor network", International Journal on AdHoc Networking Systems (IJANS) Vol. 2, No. 4, October 2012

[16] Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami," EAACK—A Secure Intrusion-Detection System for MANETs", IEEE transactions on industrial electronics, vol. 60, no. 3, march 2013.

[17] Umesh kumar chaurasia,Mrs. Varsha singh," MAODV:Modified Wormhole Detection AODV Protocol", 978-1-4799-0192-0/13/$31.00 ©2013 IEEE.