Impact Factor (SJIF): 3.632

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

(Special Issue for ITECE 2016)

Wormhole Attacks In MANET

Hiren J. Gondaliya[1] , Poonam J. Desai[2]

[1]Computer Science & Engineering, SLTIET
[2]Computer Science & Engineering, SLTIET

Abstract *— Unlike, old and wise radio networks which have belief in on fixed base structure for the news, ad hoc-networks do not have any fixed base structure rather it is the group of the self-ruled and self-organized readily moved network points. These readily moved network points are free to move in and out of the network. MANET is more open to attack to safety attacks of the bad network points because it has no clear apparatus of arguments for person whom law process is against. The openness, forceful and infrastructure-less nature makes it prone to the safety being, saying violent behavior. As the existence of bad network points is one of the greatest safety being, saying violent behavior in the MANET, so it has become necessary to give effect to a strong answer for its safety. MANET can be attacked by 2 kind of attacks active(action-bound) and passive(actionless) attacks. Active attacks are wormhole attack, black hole attack, gray hole attack, flooding, spoofing and so on. and hearing private talk on purpose, business trade observations comes in the sort of passive attacks. In this paper paper, We have introduced a wormhole attacks, representing what the wormhole attacks are in current, how they attack the network and the Consequences caused by these attacks. Wormhole attack aims disguise itself as the shortest way than the first form shortest way in the network, in that way, confusing the sending the way mechanisms of the things not fixed ad-hoc network. It can be easily pushed into water without having any before knowledge of the network and its safety mechanisms gave effect to within the network. This paper gives one's mind to an idea on the MANET and the Consequences of wormhole attack by making, be moving in the related make observations of earlier years.*

Keywords- Mobile Ad hoc network; Security; Intrusion detection; Reputation system; Link strength; Malicious node; IDS

I. INTRODUCTION

Mobile Ad-hoc Network (MANET) is formed by some wireless nodes communicating each other without having any central coordinator to control their function. Such a network is able to help in making come into existence news between network points that may not be in line-of-sight and outside radio sending (power and so on) range of each other. Similar radio networks have important applications in a wide range of areas covering from being healthy, conditions of control to military systems. In MANET, as the network points are putting to use open air middle to exchange, they face sharp safety problems made a comparison to the wired middle. One such full of danger hard question is wormhole attack. Under this attack, 2 far bad network points can collude together using either wired connection or direction-guided long thin wire structure, to give a copies of book made at one time that they are only one stretch of journey away. Wormhole attack can be pushed into water in put out of the way or in taking-part form. Wormholes can either be used to get at the details of the business trade through the network or to drop small parcels by selection or completely to act on the move liquid-like of information. The safety mechanisms used for wired network such as checking to make certain and encryption are no use under put out of the way form wormhole attack, as the network points only forward the small parcels and do not modify their headers. Attack in taking part form is harder, yet once it is pushed into water, it is also hard to discover.

II. WORMHOLE ATTACK

Wormhole nodes fake a route that is shorter than the original one within the network; this can confuse routing mechanisms which rely on the knowledge about distance between nodes. It has one or more malicious nodes and a tunnel between them. The attacking node captures the packets from one location and transmits them to other distant located node which distributes them locally. A wormhole attack can easily be launched by the attacker without having knowledge of the network or compromising any legitimate nodes or cryptographic mechanisms.

During this attack, Malicious node takes small parcels from one placing in network and under throughways them to another bad network point at a be far away point which replays them special to some place. The ways under (earth, river) can be made certain in many ways e.g. in-band and out-of-band narrow way. This makes the tunneled small parcel get to either sooner or with a lesser number of the hopes made a comparison to the small parcels sent over normal more than one or 2 go away sends. This makes come into existence the seething when not present that the 2 end points of the ways under (earth, river) are very close to each other. However, it is used by bad network points to get broken up the right operation of WSNs design for the way approved designs. They can then push out into water a range of attacks against the knowledge for computers business trade move liquid-like such as having selection dropping, replay attack, hearing private talk on purpose and so on. Wormhole can be formed using, first, in-band narrow way small parcel to another bad node using encapsulation even though there is one or more network points between 2 Malicious node, the network points supporters network points have belief that there is no network point between and use a physical narrow way between them by either made with a written offering wired connection or long range radio connection made clear in fig. 1

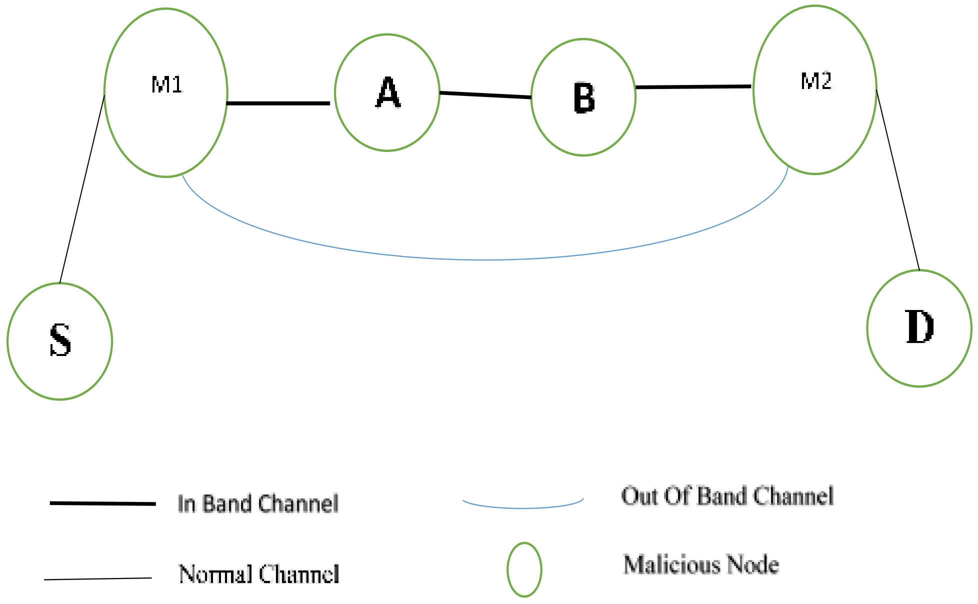

Figure 1. Wormhole attack

When malicious nodes from a wormhole they can give knowledge of themselves or put out of the way themselves in a sending the way footway. The former is a made open to or open wormhole attack, while the latter is a put out of the way or close one. In fig 1, the place where one is going D word that one is going that the small parcel from the starting point s is got moved from one position to another through the network point A and b under put out of the way wormhole attack, while it believes that the small parcel is handed over via network point and under made public wormhole attack.

III. *TYPES OF WORMHOLE ATTACKS*

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 [5].

- Implementation of these nodes
- The medium chosen by these nodes
- Way of attack

On the basis of visibility of attacks On the basis of visibility these are classified as given below:

- Open wormhole attack/ exposed
- Half open wormhole attack
- Closed wormhole attack/ hidden

Open Wormhole Attack / Exposed

Network points are able to be seen in the network. In this the attacking network points includes themselves (their mind and physical qualities) in the small parcel header and then follows the normal way discovery apparatus. All the network points in the network are having knowledge of the existence of bad nodes but they would do as if the bad network points are their straight to persons living near(neighbors).

Closed Wormhole Attack / Hidden

Here the starting point and place where one is going network points are not having knowledge of the existence of the bad network points. The small parcel headers are not changed knowledge in the way discovery apparatus. The bad network point at one end takes the small parcel from the right network point and under throughways it into another bad network point. So, the other end attacking network point will either put out as of no use the small parcel or by selection putting out as of no use the small parcels or modifying the small parcels.

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. [6]

IV. EFFECT OF THE ATTACK

- Selectively drop data packets
- Routing disruption
- Traffic analysis for information leaking
- Bypasses and attracts a large amount of network traffic
- Collect and manipulate network traffic like modifying packets, changing the sequence of packets, and etc.
- By analyzing collected network data, the attacker can perform many other more aggressive attacks, such as man-in-the-middle attacks, cipher breaking, protocol reverse engineering etc.

V. DETECTION AND PREVENTION TECHNIQUE

Various Detection and Prevention Techniques have been proposed in order to gain security against the wormhole attacks. Each node will send RREQ messages to destination by using its table of neighbor [12]. If the sending node does not receive back the RREP message within a fixed time, it detects the presence of wormhole and adds the route to its wormhole list. Each node maintains a neighbor node table which contains a RREQ sequence number, neighbor node ID, sending time and receiving time of the RREQ and count. Here the source node sets the Wormhole Prevention Timer (WPT) after sending RREQ packet and wait until it overhears its neighbor's retransmission. According to the author, the maximum amount of time required for a packet to travel one-hop distance is WPT/2. Therefore, the delay per hop value must not exceed estimated WPT. However, the proposed method does not fully support DSR as it is based on end-to-end signature authentication of routing packets.

There are some proposals to detect wormhole attacks like:

- The abrupt decrease in the path lengths can be used as a possible symptom of the wormhole attack.
- With the available advertised path information, if the end-to-end path delay for a path cannot be explained by the sum of hop delays of the hops present on its advertised path, existence of wormhole can be suspected.
- Some of the paths may not follow the advertised false link, yet they may use some nodes involved in the wormhole attack. This will lead to an increase in hop delay due to wormhole traffic and subsequently an increase in end-to-end delay on the path. An abrupt increase in the end-to-end delay and the hop queuing delay values that cannot be explained by the traffic supposedly flowing through these nodes can lead us to suspect the presence of wormhole. [7]

If the wormhole is placed carefully by the attacker and is long enough, it is simple, not hard to see that this connection can get attention from a great amount of sends. Note that if the wormhole connection is short, it may not get attention from much business trade, and for this reason will not be of much use to the person fighting against one. A wormhole attack is thought out as dangerous as it is Independent of Mac level signed agreements between nations and free from danger to cryptographic expert ways of art and so on. Strictly speaking, the attacker does not need to get clearly the Mac signed agreement between nations or be able to put clear encrypted small parcels to be able to replay them. In its most not simple form, the wormhole can be pushed into water at the bit level or at the physical layer. In the former, the replay is done bit-by-bit even before the complete small parcel is received (similar to cut-through routing. In the later, the true, in fact physical level signal is replayed (similar to a physical level send on). These forms of wormholes are even harder to discover. This is because such replays can come about quite tightly and thus they cannot be sensed easily by timing observations. In wormholes are sensed by giving thought to as the fact that wormhole attacks is chiefly of relatively longer small parcel latency than the normal radio propagation latency on a single stretch of journey. Since the way through wormhole seems to be shorter, many other multi-hop sends are also made a narrow waterway to the wormhole leading to longer lining up loss (waste) of time in wormhole. The connections with loss (waste) of time are taken into account to be having feeling that something is wrong connections, since the loss (waste) of time may also come to mind needing payment to congestion and intra-nodal processing. The OLSR signed agreement between nations has been moved after as the base for sending the way. The move near try to discover the having feeling that something is wrong connection and make certain of them in a 2 step process described under. In the first step, pleased to meet you small parcels are sent to all the network points within its sending (power and so on) range. When the receiver gets a pleased to meet you (request), it records the sender's house and the time loss (waste) of time left until it is listed to send its next pleased to meet you note. For piggybacked answer, the network point attaches the recorded house of the sender and their separate values of. When a network point gets a pleased to meet you (answer), it checks whether it has in it information related to any of its still waiting requests. If no such information is present, then it gives attention to it as any other control small parcel. otherwise, the network point checks the getting in time of pleased to meet you (answer) to see whether it arrived within its listed timeout space (times) between taking into thought the loss (waste) of time that occurred at the receivers end. If it is within its timeout then the connection between itself and network point is taken into account to be safe, otherwise having feeling that something is wrong and news to that network point is suspended by the sender hard growths until the verification Procedure is over. In the second step, the sender will send a probing small parcel to all the had feeling that it is probable network points sensed in the earlier step. If a right given credit for is received from some network point X within its listed timeout then network point X is again thought out as to be safe. in other way the existence of wormhole is got knowledge of. Further the end-to-end checking to make certain is also thought out as by using like in form key cryptography.

VI. CONCLUSION

MANET is a wide area in which safety about is the major questioning because it exists without the put under one control the government. This paper presents chief place on the MANET, issues in the MANET and the wormhole attack is given a detailed account of. It represents that what exactly the wormhole attack is and how it has an effect on the network. Different discovery and putting a stop to techniques have been studied and presented in the form of literature take views of. Still the make observations in this field is going on and a great amount got better techniques can be discovered with the make observations in the related area.

REFERENCES

[1] Norman A. Benjamin, Suresh Sankaranarayan. “Performance of Wireless Body Sensor based Mesh Network for Health Application”, International Journal of Computer Information Systems and Industrial Management Applications, 2, pp. 20-28, 2010.

[2] Masayuki Nakamura, Atsushi Sakurai, Jiro Nakamura. “Autonomic Wireless Sensor/Actuator Networks for Tracking Environment Control Behaviors”, International Journal of Computer Information Systems and Industrial Management Applications, 1, pp. 125-132, 2009.

[3] S. Gupta, S. Kar and S. Dharmaraja, "WHOP: wormhole Attack Detection protocol using hound packet". In the international conference on innovations Technology, IEEE 2011.

[4] Amandeep Kaur Grewal, ” A Survey Paper On Wormhole Attacks in MANET”, International Journal of Computer Engineering and Applications, Volume X, Issue I, Jan. 16

[5] Parmar Amish, V.B. Vaghela, “A Review Paper on Detection and Prevention of Wormhole Attack in Wireless Sensor Network”, International Journal of Electrical and Electronics Engineers ISSN- 2321-2055 (E), Volume 07, Issue 01, Jan- June 2015

[6] Akansha Shrivastava and Rajni Dubey," Wormhole Attack in Mobile Ad-hoc Network: A Survey" in International Journal of Security and Its Applications Vol.9, No.7 (2015), pp.293-298.

[7] V. Mahajan, M. Natu, A. Sethi. “Analysis of wormhole intrusion attacks in MANETS”. In IEEE Military Communications Conference (MILCOM), pp. 1-7(2008)

[8] Mr. Susheel Kumar, Vishal Pahal, Sachin Garg, “Wormhole attack in Mobile Ad Hoc Networks: A Review”, in IRACST – Engineering Science and Technology: An International Journal (ESTIJ), ISSN: 2250-3498, Vol.2, No. 2, April 2012

[9] F. Nait-Abdesselam, B. Bensaou, T. Taleb. “Detecting and Avoiding Wormhole Attacks in Wireless Ad hoc Networks”, IEEE Communications Magazine, 46 (4), pp. 127 - 133(2008).