International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 04, April-2017

A Review on Detection and Prevention of Wormhole Attacks in Manet

Ranjit Singh[1] ,
[1]Department of Computer Engineering & Technology
Guru Nanak Dev University,
Amritsar

Anil Kumar[2]
[2]Department of Computer Engineering & Technology
Guru Nanak Dev University,
Amritsar

Abstract **- Mobile ad-hoc network is self-organizing wireless network composed of different nodes communicate with each other without having established infrastructure. It generally works by broadcasting the information and used air as medium. Its nature of broadcasting and transmission medium also help attacker to disrupt network. Many kind of attack can be done on such Mobile Ad Hoc Network. The emphasis of this paper is to study wormhole attack, some detection method and different techniques to prevent network from these attack. This analysis able to provide in establishing a method to reduce the drawbacks like reliability, message overhead, delay and clock synchronization and to become more faster.**

Keywords: Encapsulation, Integrity, Confidentiality, Impersonators.

1. INTRODUCTION

A Mobile Ad-hoc network is made up of number of wireless mobile nodes that can communicate with one another directly or indirectly without any need of a network infrastructure or any centralized administration. In Mobile Ad-hoc network, number of mobile users can communicate over relatively bandwidth constrained wireless links so it is a self-directed network. Network topology changes dynamically because the nodes are mobile and it is difficult to retract them over time. Mobile Ad-hoc network is distributed network in which all activities of network are executed by the nodes themselves; activities performed by the network like to adapt topology and delivery of messages etc. i.e., all routing functionality is merged into mobile nodes. There are two types of communication: direct and indirect; in direct communication, nodes that are in radio range of one another can interact with each other directly while in indirect communication, nodes interact with each other with the help of intermediate nodes in order to route their packets. Wireless interface is used through which each node communicates. Because the network is fully distributed, so no fixed infrastructure is used as access points and base stations i.e. it can work without any fixed infrastructure. The topology of the network keeps on changing as nodes used are mobile nodes, so they enter and leave the network continuously. One of the important research areas in MANETs is establishing and maintaining the ad hoc network with the help of routing protocols.

Fig1. Mobile Ad hoc Network

A. Security Principles

Security includes a group of investments that are sufficiently funded. In MANET, each and every networking functions such as routing and packet forwarding, are execute by nodes themselves in a self-organizing manner. In favor of these reasons, securing a mobile ad -hoc network is extremely challenging. The goals to check if mobile ad-hoc network is secure or not are as follows:

1. Availability: Availability refers to assets which are accessible to authorized parties at proper times. Availability applies equally to data and to services. It gives the survivability of network service in spite of denial of service attack. It is also means sharing information so as to make sure consistency among redundant resources.
2. Confidentiality: Confidentiality makes sure that computer-related possessions are accessed only by authorized parties. It means, only those who should have access to somewhat will actually get that access. If we have to maintain confidentiality of some confidential information, we need to carry on them confidential and secret from all entities that do not have privilege to access them. Confidentiality is occasionally called secrecy or privacy.
3. Integrity: Integrity means that resources can be customized only by authorized parties or only in authorized manner. Modification includes writing, deleting and creating, changing status. Integrity assures that a message being passed is never corrupted.
4. Authentication: Authentication enables a node to make sure the identity of peer node it is communicating with. Authentication is fundamentally guaranteed that participants in communication are not impersonators they are authenticated. Authenticity is ensured because only the

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 04, April-2017

rightful sender can generate a message that will decrypt correctly with the shared key.

5. Non Repudiation : Non repudiation is the property which ensures that sender and receiver of a message cannot deny that they have ever sent or received such a message. This is useful when we want to discriminate if a node with a few undesired function is compromised or not.
6. Anonymity : Anonymity means all the information that can be used to recognize owner or present user of node should default be kept private and not be distributed by node itself or the system software. It provides the all probable information that can be used to identify the vendor.
7. Authorization : This property assigns dissimilar access rights to different types of users. For example a network management can be performed by network administrator only. Authorization is a procedure in which an entity is issued a credential which privileges and permissions it has and cannot falsify by the certificate authority. It is also used to allocate different access rights to different rank of users.

2. WORMHOLE ATTACK

The wormhole attack is the most severe attacks of MANET. It is a kind of DOS attack which is very effective in network layer. Network routing is being affected by this attack along with this location based security of Ad-hoc is also compromised. "Wormhole attack" is a co-operative attack because there is a need of two nodes that will act in co-operation. In this attack, at two different edges of the network, two collaborating attacker nodes will occupy their strong strategic locations. In this way they are occupying dominant positions in a network so that they (nodes) can cover complete network and present to have the smallest path for transferring data. By using direct wireless link these two attacker nodes are linked together which is known as wormhole tunnel. At one end of wormhole tunnel, one node will collect packets in its local area and then those packets are transmitted to the other node at the other end of tunnel then this node will play again with those packets. The attacker nodes are connected together via tunnel that is created using high speed transmission links such as Ethernet cables or wireless optical links. If this pair of nodes will forward every packet legitimately then it means that they are supporting the faster communication and routing within the network. However, this is not the case as these attacker nodes, either drop all packets which are intended to them, alter those packets or selectively transfer some packets.
In wormhole attack, malicious nodes give misconception to both sender and receiver of being close neighbours but they are actually far distant away by tunneling packets between two attackers. Wormhole can be established by using a single long-range wireless link or through wired link between two colluding attackers. The attacker may create tunnel even for packets not addressed to itself as of broadcast nature of the radio channel.
In figure 2, two malicious nodes are there **X** and **Y** that will de-capsulate data packets in aim to falsify the route lengths.

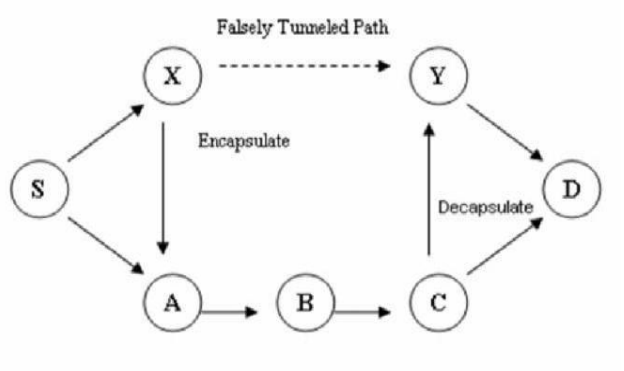


Fig 2: Wormhole Attack

Let us suppose that node S wants to communicate with node D and commences route discovery process by broadcasting RREQ packets. The RREQ packet will be encapsulated by node X on receiving it from S and tunnels it to Y via an existing data route XABCY. After that when Y will receive the encapsulated RREQ for D then it will show that it had only travelled SXYD. The packet header will not be updated by both attacker nodes X and Y and two routes from source node S of unequal length will be found by destination node D i.e. 4 and 3. If RREP will be tunnelled back to X from Y, S would falsely consider the path to D via X is better than the path to D via A which result into tunnelling that will further prevent honest intermediate nodes from correctly incrementing the metric used to measure path lengths.

2.1Types of Wormhole Attack:[15]

- Wormhole using Encapsulation (In-band channel): In this, one malicious node will transfer the route request packets to another malicious node via one or more nodes present in the network
- Wormhole using out of band channel: In this, by using either wired link or long range wireless link two malicious nodes are directly connected to each other.

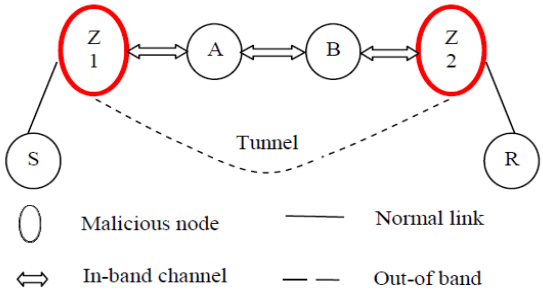


Fig 3: Variants of Wormhole Attack (In and Out band channels)

- *Open wormhole attack:* In this attack, for discovering the RREQ packets malicious nodes keep on examining the wireless medium. If the malicious nodes are present in the network, it is supposed that malicious nodes are present on path by other nodes on the network and they are their direct neighbours.
- Closed wormhole attack: In this attack, neither capture packet nor packet field head are modified by the attacker instead attackers take advantage from processing packets in order to find a route known as route discovery. In

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 04, April-2017

route discovery process, attacker tunnels the packet from one side of the network to another side of the network and re-broadcast packets.

- Half open wormhole attack: In this attack, malicious node will modify only one side of packet and the other side of the packet will not be modified in subsequently route discovery procedure.
- Wormhole with high power transmission: In this attack, in order to broadcast a packet, malicious node will use maximum level of energy transmission. With the help of route discovery process malicious node will get a Route Request (RREQ), after that, it will broadcast the Route Request (RREQ) at a maximum level of energy of it power so the other node on the network which are on the normal power transmission and lack of high power capability hears the maximum energy power broadcast they rebroadcast the packet towards the destination. By doing this malicious node can get more chances to create a route between source and destination without using colluding.

3. LITERATUE REVIEW:--

The goals of Ad hoc networks and mainly MANET have in current years not just seen widespread use in commercial and domestic application regions but have also become the focus of intensive study. Applications of MANET range from simple wireless home and office networking. Security aspects play an important role in all of these application scenarios given the vulnerabilities inherent in wireless ad hoc networking from the very fact that radio communication takes place. The above paper contents various literature surveys, which cover all dimensions of study.

Dhruvi Sharma, Vimal Kumar and Rakesh Kumar[1] proposed paper throws light on wormhole attack that is vulnerable attack in which two or more malicious nodes form a tunnel like structure to relay packets themselves. This type of attack may cause selective forwarding, fabrication and alteration of packets being sent. In this paper, an identity based signature scheme along with clusters is proposed for protecting network from wormhole attack. The proposed scheme does not require distribution of any certificate among nodes so it decreases computation overhead. Cluster based architecture is used in which cluster heads are chosen in such a way that they cannot be malicious. This scheme operates in three phases. Simulation results show the improved performance of proposed scheme in terms of throughput, packet delivery ratio and end-to-end delay.

Elham Zamani and Mohammadreza Soltanaghaei [2] proposed a new protocol named M-AODV which is a type of overhearing backup protocol based on AODV. After that, security of proposed protocol is assessed, the authors simulate both protocols (M-AODV and AODV) under black hole and wormhole attacks, using no security solution. The proposed protocol is based on overhearing the neighbours and constant comparison of the information of main and alternative tables and proposed protocol is found to be safe and some attacks are tested on it. Wormhole attack is detected by overhearing the nodes. The results show that M-AODV has been improved in terms of packet delivery ratio, and the delay has been reduced as well, but the amount of overhead had been increased. M-AODV also improves the quality and security of networks. When security measures are taken, the proposed method has attributes such as overhearing, immediate updating, local repair, and two routing tables. It is assumed that the proposed protocol may act like some other secure methods, such as neighbour overhearing (NEVO) and Packet Travel Time (PTT), which have some of these features as well and may be secure against some attacks. Thus, in simulations, the proposed protocol is proved to be secure against wormhole and black hole attacks.

Amit Kumar and Sayar Singh Shekhawat [3] proposed Wormhole attack is one such attack in which two or more nodes can collectively access the bandwidth and communication can be perturbed. In this paper, a wormhole infected network is defined and in order to perform the reliable communication in attacked network the work model is offered. Network model is generated for optimizing the communication to identify the safe communication node. The authors also discuss how to generate the safe path in attack based mobile network. Finally, the presented model has provided the optimized parameter adaptive communication. Results show the improved performance of model in terms of the communication throughput and reduced the loss.

Ashish Kumar Jain and Ravindra Verma [4] proposed how to defend against wormhole attack using combination of parameters like energy, number of connections and buffer length of a node. Based on these parameters trust value of a node is computed. Then this trust value of node is compared with threshold value of network trust. Based on this comparison it can be found that whether that selected node is either malicious or legitimate. The proposed methodology consists of two phases: First of all, do analysis of network parameter and threshold computation and secondly the security implementation on the existing routing protocol. Results are analysed by extending AODV protocol and the performance of the proposed routing protocol is evaluated and compared with the AODV under attack. According to the comparative outcomes the performance of the proposed trust based security approach is much efficient and adoptable against wormhole attacks in MANET.[5] Rajan Patel et.al.in 2015 (IEEE) describes Defending Against Wormhole Attack in MANET In this paper, survey is done on various techniques used for detection of wormhole attack and authors propose an approach for detection and prevention of wormhole attack. A proposed approach for defending against wormhole attack is based on the Hash based Compression Function (HCF) which is actually using any secure hash function to compute a value of hash field for RREQ packet and proposed approach looks very promising compared to other solutions proposed in literature. [6] Dhruva Patel et.al.in 2015 describes A Brief Analysis on Detection and Avoidance Techniques of Wormhole Attack in MANET

This paper describes how different security layers are influenced by various security threats. MANET is susceptible to various threats due to its mobility and self-routing nature so, different layers in network can be infected by different attacks. There are number of attacks and each attack has its own impact on different layers like some can cause harm to

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 04, April-2017

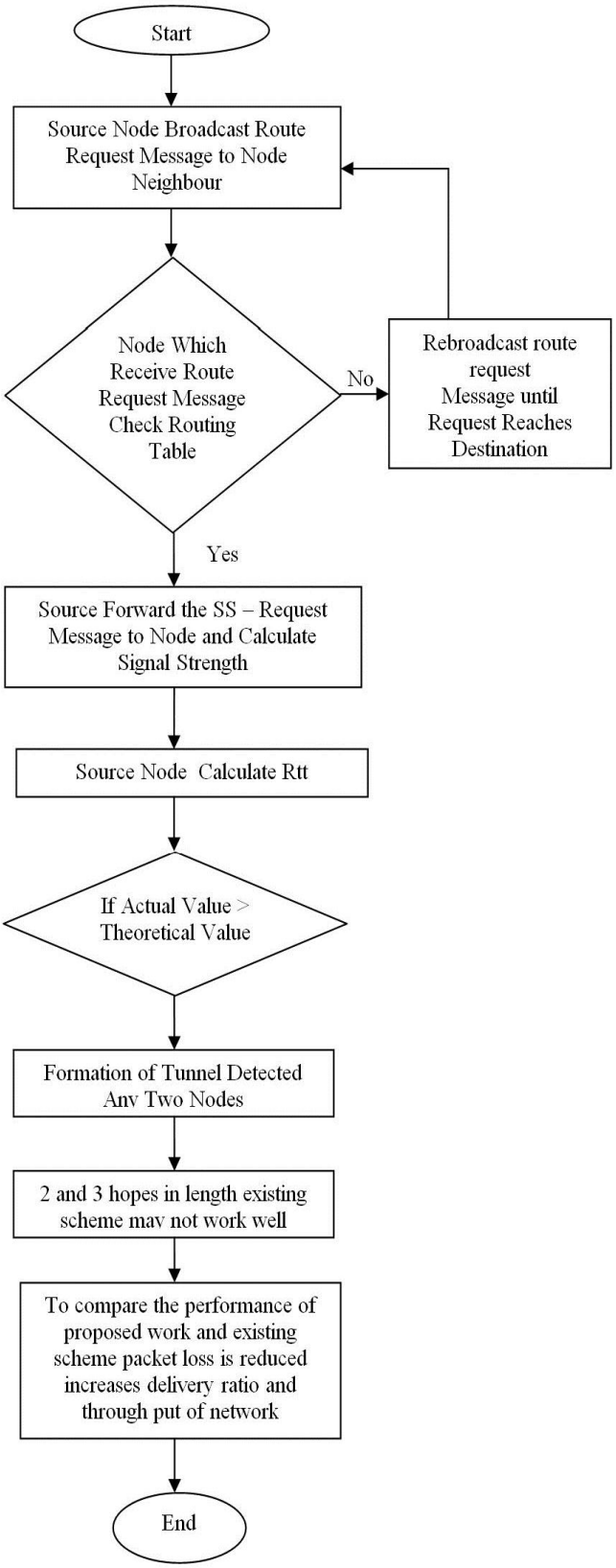
particular network layer only while others can attack other layers i.e. it depends on the nature of attack how it reacts. Now, Wormhole attack is a network layer attack which can completely disturb the communication channel and it is found to be very serious threat among all attacks. In this paper, authors throw light on wormhole attack and various existing detecting and preventing techniques are discussed. In those techniques, wormhole attack is detected using AODV and DSR routing protocols. And it is recommended to use other routing protocols like TORA, ZRP for detecting wormhole attack.

[7] Anju J et.al.in 2014 (IEEE) describes An Improved Clustering-based Approach for Wormhole Attack Detection in MANET In this paper, wormhole attack launched by exploiting AODV protocol in MANET, is detected and eliminated in two phases. In the preliminary phase, wormhole attack is detected based on timing analysis and hop count. After the attack is suspected, presence of attack is confirmed by using Clustering based approach and this approach also helps in localizing the attacker nodes. The entire network is partitioned into different clusters and each cluster will have a Cluster Head, which controls all the nodes in the cluster and plays the role of a controlling authority in MANET. NS3 simulator is used for evaluating the performance of proposed system in which characteristics of normal AODV are compared with proposed clustering based approach. Out of band wormhole attacks that are launched by exploiting AODV routing protocol are eliminated effectively in the proposed clustering based algorithm.

4. PROPOSED WORK

The source forwards the SS-REQ message to the nodes in the path asking the nodes to calculate the signal strength. The nodes reply to the source node with SS-REP message and also forwards the calculated signal strength with the ID of their neighbour (with respect to which the signal strength has been calculated). The source node calculates the reverse trip time taken to receive the CREP. If the actual value is more than the theoretical value, then the formation of the tunnel is detected. If any two nodes have formed the tunnel, then the signal strength between them must be less than the threshold value.

Representation of flow chart



International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 04, April-2017

5. CONCLUSION:--

Wormhole attacks can degrade network performance significantly in ad hoc network and harms the network security. The detection of wormhole attacks is quite complicated. In this paper we have basically surveyed the existing methods and approaches which will help us in future to design an enhanced approach for detecting the wormhole attack in Mobile Ad Hoc network. Overall a significant amount of work has been done on solving wormhole attack problem. It is the fact that we can't say one solution is applicable to all situations. There is choice of solution available based on cost, need of security may lead better result, but can be costly, which may affect other networks necessities. Similarly some network requires more security like the military area network. A standard and customary solution is still lacking, although several very useful solutions applicable to some networks have been described.

REFERENCES:--

[1] Dhruvi Sharma, Vimal Kumar, Rakesh Kumar, "Prevention of Wormhole Attack Using Identity Based Signature Scheme in MANET ", Computational Intelligence in Data Mining. Volume 2. Volume 411 of the series Advances in Intelligent Systems and Computing pp 475-485. 10 December 2015, Springer.

[2] Elham Zamani and Mohammadreza Soltanaghaei, "The Improved Overhearing Backup AODV Protocol in MANET" ,Journal of Computer Networks and Communications Volume 2016 (2016), Article ID 6463157, 8 pages. Hindawi

[3] Amit Kumar, Sayar Singh Shekhawat, "A Parameter Estimation Based Model for Worm Hole Preventive Route Optimization", IJCSMC, Vol. 4, Issue. 8, August 2015, pg.80 – 85International Journal of Computer Science and Mobile Computing.

[4] Ashish Kumar Jain, Ravindra Verma, " Trust-Based Solution for Wormhole Attacks In Mobile Ad Hoc Networks", Volume-4, Issue-12, November- 2015, Global Journal Of Multidisciplinary Studies.

[5] Rajan Patel, Anal Patel, Nimisha Patel, "Defending Against Wormhole Attack in MANET", Fifth International Conference on Communication Systems and Network Technologies, 2015 IEEE.

[6] Dhruva Patel, Parth Trivedi, M. B. Potdar, "A brief Analysis on Detection and Avoidance Techniques of Wormhole Attack in MANET" , Volume 117 - Number 16, International Journal of Computer Applications, 2015.

[7] J. Anju, C. N. Sminesh, " An Improved Clustering-Based Approach for Wormhole Attack Detection in MANET", Proceedings of the 2014 3rd International Conference on Eco-friendly Computing and Communication Systems, Pages 149-154, IEEE.

[8] M. B. Mojtaba Ghanaat Pisheh Sanaei, Ismail Fauzi Isnin, "Performance evaluation of routing protocol on aodv and dsr under wormhole attack," *International Journal of Computer Networks and Communications Security*, vol. 1, no. 1, pp. 1–6, 2010.

[9] D. B. J. Yih-Chun Hu, Adrian Perrig, "Packet leashes: A defense against wormhole attacks in wireless networks," in *IEEE, INFOCOM*. IEEE, 2003.

[10] D. J. J. S. Fei Shi, Weijie Liu, "Time-based detection and location of wormhole attacks in wireless ad hoc networks," in *2011 International Joint Conference of IEEE TrustCom-11,IEEE ICESS-11,FCST-11*.IEEE, 2011.

[11] N. C. Debdutta Barman Roy, Rituparna Chaki, "A new cluster based wormhole detection algorithm for mobile adhoc networks," *International Journal of Network Security and Its Applications*, vol. 1, no. 1, 2009.

[12] J. D. P. B. I. S. Rutvij H Jhaveri, Ashish D Patel, "Manet routing protocols and wormhole attack against aodv," *IJCSNS International Journal of Computer Science and Network Security*, vol. 10, no. 4, 2010.

[13] Z. A. Khan and M. H. Islam, "Wormhole attack: A new detection technique," in *International Conference on Emerging Technologies (ICET),2012*. IEEE, 2012, pp. 1–6.

[14] A. K. Sunil Taneja, "A survey of routing protocols in manet," *International Journal for Innovation, Management and Technology*, vol. 1, no. 3, 2010.

[15] Dhara Buch, Devesh Jinwala "PREVENTION OF WORMHOLE ATTACK IN WIRELESS SENSOR NETWORK". International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.5, Sep 2011. DOI: 10.5121/ijnsa.2011.3507 85