International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue IX, September 2017- Available at www.ijraset.com

Tree Based Method Used For The Detection And Perevention Of Malicious Nodes In Manet

Sukanya Kargaiyan[1], Neelam Joshi[2]
[1]*Research Scholar,* [2]*Assistant Professor, Department of Computer Science & Engineering, Maharana Pratap College of Technology Gwalior, India*

Abstract: ***A Mobile Ad-Hoc Network (MANET) is an infrastructure much less or a self-configured accumulating of mobile nodes that can indiscriminately regulate their geographic places such that those networks have dynamic topologies and random mobility with restricted assets. It commonly works by broadcasting the statistics. Its nature is broadcasting so there's a threat to disrupt community via attacker. The variety of attack can be performed in MANET. The greater extreme is the wormhole attack. Here we're reading about the wormhole attacks its types. In previous work, they detected wormhole attack by using Route Request (RREQ) and Hop Count technique. Malicious node always provides less hop count as compared to the normal path. Hop Count in the wormhole channel is always constant and this can be used to detect the wormhole attack but it is difficult to detect. For detecting wormhole, we proposed tree-based method to detect and prevent an attacker. Construct a tree of network in which source node behaves as a root node and other neighboring nodes are as children. When source send data to destination it search for the paths which should be shortest path. The valid path has established for the transmission of data which protect it from the attacker.***
Keywords: Mobile ad hoc network (MANET), RREQ, IDS, Wormhole Attack, Attacker node, Tree.

I. INTRODUCTION

Wireless networking is the platform for running with the current technology widely utilized in numerous applications. MANET is a of wireless mobile node, consists of each wireless transmitters and receivers, which dynamically forming a quick network and communique amongst transmitter and receiver is by way of the use of bi-directional hyperlink. Either at once, if nodes in MANET are within verbal exchange range or not directly method transmitter node depend on intermediate node, for forwarding data to destination node. Various feature of MANET, overcomes the problem in contemporary application of wireless network.

Such as dynamic topology and decentralized network feature of MANET, way all the nodes are loose to transport randomly. The self-configuring potential of nodes in MANET, Minimal configuration and quick development, makes MANET geared up to be used in emergency situation, wherein an Infrastructure is unavailable, or tough to put in network, in conditions like natural failures, military conflicts. Due to these various unique characteristics, MANET is becoming popular among all other wireless application as well as widely implemented in industry. Network security has vital importance in every wireless network technology.

But open medium and faraway distribution of nodes make MANET at risk of diverse styles of attacks. So it's far important to broaden a efficient secure intrusion-detection gadget (IDS) to protect MANET from numerous attacks. IDS is one of the Research subject in MANET, basically researchers are specializing in growing a new detection, prevention and response mechanisms for MANET [1].

Fig.1 MANET

II. INTRUSION DETECTION SYSTEM

The IDS is a technique for detecting the attacks by using reading and continuously monitoring community features. Intrusion detection arises as a essential protective mechanism in MANETs. IDSCHss. These nodes can forward the intrusion facts to pals while wished. Another approach inside the IDS is to put in IDS for self and neighbor nodes to check for malicious neighbor nodes present. The global IDS may be deployed for clusters of mobile nodes where CH node is accountable for worldwide ID for its cluster [2]. Three extraordinary additives of IDS encompass data collection, detection, and reaction [3]. The data series is chargeable for transferring data to a not unusual layout, data storage and sending data to the detection module. The IDS gathers the audit data and cross check the data if you want to find any attack within the network, with the established data used for auditing the IDS could be labeled ad host and network based [4. A network based totally typically present in the gateway of the network and examines the packet while the host primarily based machine uses the operating system information to study the attacks within the network. IDS classifications is of numerous types mainly consists of Active and passive IDS, The active attack is set for automated blocking off of suspecting attacks which presents real -time remedial action for respective detecting attacks. A passive IDS is a machine that's deployed to for tracking and reading network traffic activity and offer warning to the nodes regarding vulnerabilities and attacks. A knowledge-based totally IDS which includes the database of preceding attacks signatures and recognized system vulnerabilities for taking responsive moves. Anomaly-based IDS is the procedure of gathering records associated with the performance of legal nodes over a span of time which accompanied through exam implemented to observed conduct to decide with a highest degree of self assurance that the conduct of intruder nodes now not authorized. Even though false alarm rates is a number one hassle for growing the IDS particularly the anomaly based intrusion detection device, but the machine has completely met the favored goals compared to the signature based device [5]. Specification based ID which frames specs that seize legal nodes behavior any version from the framed specification marked as an attack [6].

III. WORMHOLE ATTACK

It is a intense attack in ad hoc networks in which malicious nodes form a virtual channel among them. Attackers pass the packet through virtual channel and replay them into the network. It can be launched even if the network communication uses cryptographic techniques. Wormhole may exists at bit level (the reply is done bit by bit even earlier than the whole packet arrived), same as cut through routing by or at physical layer. In fact, nodes around the wormhole antenna realize that they can transmit packets with other wireless nodes located next to the other antenna and consider them as immediate neighbors. Lunching wormhole attack can be done easily. It is not depend on Medium Access Control (MAC).layer protocol and cryptography techniques aren't sufficient to save you it, as wormhole attackers do not create separate packets, but virtually replay packets that exist already at the network by passing all cryptographic tests. It is due to the wormhole attacker no needs to break into wireless nodes or realize the mechanism of communication used by the network.

The packets can be transmitted over the wormhole link and reach to destination without any changes or dropping of any packets, the existence of wormhole is not harmful, and even have benefit by enhance the network connectivity and makes a shorter path to transfer packets between sender and receiver otherwise far off area. If the distance of tunnel is longer than transmission range, nodes near the wormhole antenna look for faster and shorter reliable paths by using the wormhole tunnel. Wireless networks running any dissimilarities of shortest path routing will find out this kind of paths and finally use them to broadcast data.

Wormhole attack turn off and on the signal replayed by the adversary and it completely changes the network connectivity and then suddenly creates or destroys a lot of shortest paths within the network and upset maximum of routing protocols. Wormhole can get the RREQ packet through the tunnel and then play a denial of service attack by ignoring to broadcast any packets in on-demand routing protocols. In routing protocols which discover neighbors, the attacker can do frequent neighbor and path changes, it makes nodes consume the energy and wastes communication bandwidth. When the wormhole node is exist, it replay the scheme, mostly wormhole used to obtain network traffic, then spoof the packets, drop packets, or act as man in the middle attacks. In this way, when the traffic gathered, it helps to break encryption and security mechanisms of the network. Impact of wormhole attack is measured in terms of style of pairs whose shortest paths are affected.Wormhole attacks have more impact, when two antennas are placed far apart, because of more paths and more traffic in the network; as a result, more damages are done to the transmitted packets by the wormhole link. In Figure 2 two red nodes N1 and N2 are wormhole and the dotted line connects two nodes is a long wormhole link. The blue nodes are regular nodes and that they consist greater hops to transmit packets to destination.

When the attack happens, nodes placed in region A recall nodes in vicinity B as friends and vice versa. Overall, to messing up with the routing protocols, by means of the usage of wormholes, adversary in a position to break any protocol is predicated on geographic

proximity. At the same time, every single one of localization algorithms which employ network connectivity would fail by the alteration of the network topology based on wormhole links.

It can be the main impact of wormhole, due to its position which can be exploited as a useful function in numerous application as well as protocols. [7]. on the opposite hand, out of band location systems like Global Positioning System (GPS) can't be available or unusable because of the environment [7].

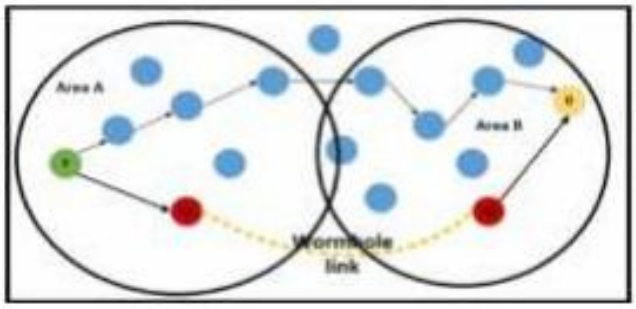

Fig.2 Demonstration of wormhole attack

IV. WORMHOLE ATTACKS

Shabina Parbin et al. [2016] In this paper, our proposed a trust and reputation management scheme for find out the trusted location in MANET environment. MANETs operates without fixed framework and all nodes in network perform like a router in sequence to forward information next receiver. Since the pivotal factor rein want, MANETs are furthermore pregnable routing attacks as in opposition to some networks. Routing is one of the maximum extreme attacks of wormhole attacks which might be less difficult to be applied nonetheless harder detection. Generally, it operates in phases; inside the first section, wormhole channel nodes generally tend to attract increasingly more traffic route, and with the aid of other phase, they loss the grid through changing or losing the grid site visitors. In MANETs, numerous writers have applied diverse outcomes to prevent attacks [8].

Samreen Banu Kazi et al. [2016] in this paper, MANETs does not require any rigid network infrastructure each unmarried node acts as both sender and receiver. Self configuring capacity of node makes it trendy. The open medium and huge distribution of nodes make MANET defenceless to malicious attackers, so it is important to expand proficient intrusion detection plan to shield MANET from attacks. The proposed intrusion detection system (IDS) “Secure IDS to Detect the Malevolent node in MANETs” is implemented for MANETs which uses the DSR routing protocol [9].

H.Ghayvat et al. [2016] In this paper, the proposed protection approach is to locate and mitigate wormhole attack. It is secured Ad hoc on AODV technique which correctly finds wormhole attack present in a MANET and Digital signature is used to save you it. This method is primarily based on a calculation of tunneling time taken by using tunnel to analyze the behavior of wormhole. Afterward, it decides a few static threshold value. Based upon this tunneling time and threshold value, it comes to a decision whether or not given node is wormhole node or straightforward node. A digital signature and hash chain algorithm is implemented to mitigate the wormhole node [10].

Chitra Gupta et al. [2016] in this paper, the proposed technique discovers an alternative route to the target node. Because the shortest path can have the malicious attacker. The implementation of the secure route discovery protocol is carried out the usage of NS2 and with the aid of modification of the AODV routing protocol [11].

Dhruvi Sharma et al. [2016] This paper offers detail study of wormhole attack, algorithms to locate them that has been proposed to date and also directs the reader toward the areas that can be explored and work upon in future. Security of different networks has always been a primary concern as its necessary to protect the resources being shared and communication being done among the legitimate users.

If we let down our safeguards, an attacker can rework the routing protocol and interrupt the network operations thru mechanisms consisting of packet drops, flooding, data fabrication and many others. MANET is a shape of network whose dynamic topology, decentralizing governance and other such capabilities are generally in favour of many security attacks [12].

Ankit Agrawal, et al. [2014] This paper proposes and evaluates a singular Coordinated Node Monitoring & Response (CNMR) Based IDS via AACK for AODV protocol It is a multistep manner in which the node & its transmission are in control of some monitoring node. This node can generate responses on the basis of threshold. This quantity of reaction can be taken as principal attention for identity of intruder's node. Our high concern by using featuring new updates for safety is to demonstrate better ID fees with minimized

overall performance troubles. A T the initial level of our research the work is getting better results in comparison with other existing mechanisms [13].

V. PROPOSED WORK

In previous work, they used Route Request (RREQ) and Hop Count technique to detect wormhole attack. But these procedures are not adequate to notice and avoid wormhole attack in the network. Malicious node always provides less hop count as compared to the normal path. Hop Count in the wormhole channel is always constant and this can be used to detect the wormhole attack but it is difficult to detect.

For discovering wormhole attacker in MANET, we proposed tree-based method to distinguish and avoid an attacker. When a node in the network has a few data which is to be securely spread to the destination. Then we construct a tree of network in which source node behaves as a root node and other neighboring nodes are as children. When source send data to destination it search for the paths which should be shortest path. We consider that malicious node always reply first for the shortest path to traverse all the traffic towards itself. So we check the left and right children of malicious node or who reply first on the basis of tree which we formed earlier. Then request the neighbours that are this path is suitable or not. Then all neighbour which is child node check this and reply root node if it is valid then send data otherwise all child update that information and protect the data from getting into the wormhole channel.

A. Step 1: Initialize the network
B. Step 2: Select sender S and destination D nodes
C. Step 3: if source has data to send to the destination Then construct a tree T in which source node is a root node
D. Step 4: if it has neighbours
   1) Then make all neighbour nodes as a child node
   2) Else tree has no child
E. Step 5: request for shortest path
F. Step 6: if we get reply from the node
   1) then we traverse T.left and T.right
   2) else request again
G. Step 7: if path is valid
   Then neighbours check and reply to source node
H. Step 8: update the routing table
I. Step 9: Exit

VI. RESULT ANALYSIS

A. Throughput

The transfer of information lying on information measure is result as output. The graph represents an output graph among base approach moreover as projected approach. The output of the projected approach is better than the present approach.

Throughput (kbps) = (Receive size/(stop time - start time)*1/60

Fig.3 Throughput Graph

B. Routing Overhead

It is the whole wide variety of control packets inside the network at some stage in the transmission of data from source to destination. The graph shows that the routing overhead is less in the proposed work which is greater in existing technique.

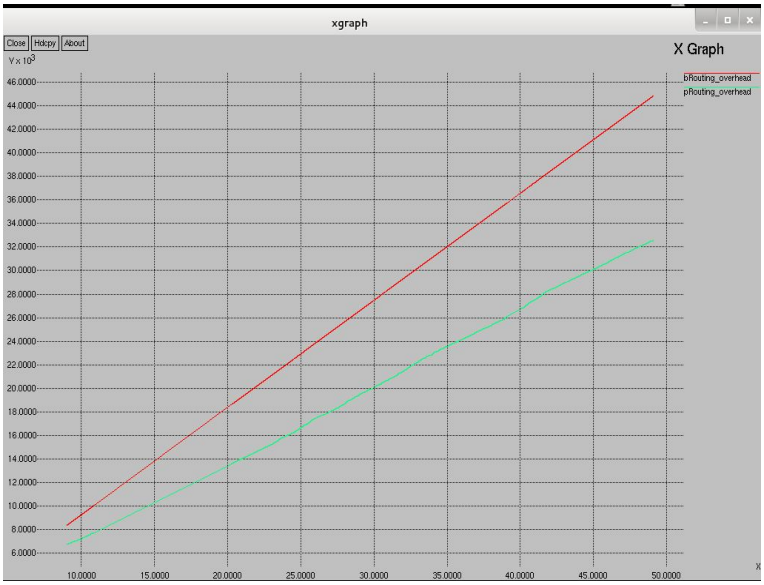

Fig.4 Routing Overhead

C. Packet Delivery Ratio

It is the definition in which the total numbers of received packets calculated in terms of send packets. It is in the percentage form which has no unit. The graph shows that a PDR graph among base method as well as proposed method. This PDR rate is best in proposed than existing approach.

PDR = No. of packets received / No. of packets sent

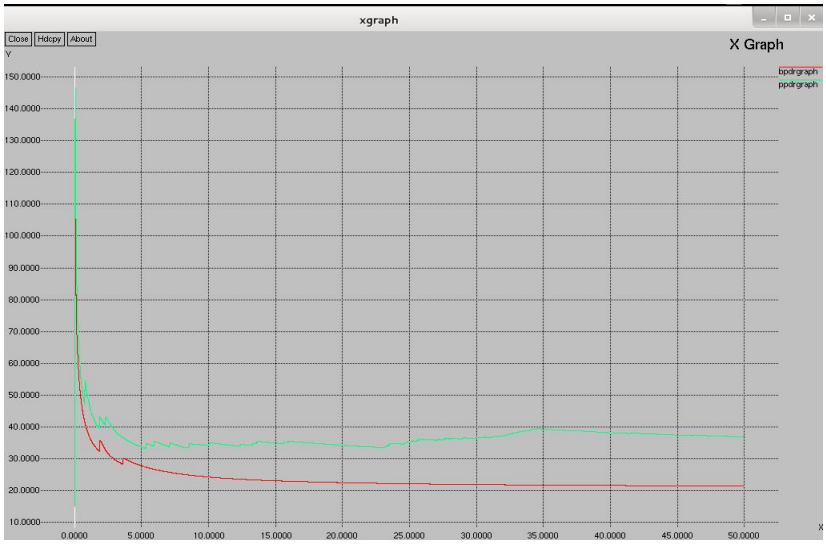

Fig.5 PDR Graph

VII. CONCLUSION

Today's Mobile Ad hoc Networks (MANETs) became a popular concern for scientists, and different learning has been made to performance enhancement of ad hoc networks. In MANET, the nodes are compromised for data forwarding to each other for communication with the others node which are away from their communication range. The mobile nodes converse with each other not including any infrastructure. One of these attacks called Wormhole Attack that two opposition node collaborate together to transmit the packets in out of band channel. In the proposed work, we enhance the performance of the network by generating the valid path in the form of tree.

REFERENCES

[1] Ranjit j. Bhosale, Prof. R.K.Ambekar "A Survey on Intrusion detection System for Mobile Ad-hoc Networks" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (6) , 2014, 7330-7333.

[2] Nish Dang & Poona Mitta, 2012 Cluster based intrusion detection system for MANETS, International Journal of Computer Applications & Information Technology. [

[3] Sen, S., & Clark, J.A., 2008, Intrusion Detection in Mobile Ad Hoc Networks, Guide to Wireless Ad Hoc Networks, Springer.

[4] Y. Zhang and W. Lee, 2000, "Intrusion Detection in Wireless AdHoc networks", Proc. 6th Int',l. Conf. Mobile Comp. Net., MobiCom , pp.275 -283

[5] Garuba, M., Liu, C. & Fraites, D., 2008, Intrusion Techniques: Comparative Study of Network Intrusion Detection Systems. In Proceeding of Fifth International Conference on Information Technology: New Generation, IEEE.

[6] Meenatchi , K. Palanivel "Intrusion Detection System in MANETS: A Survey" International Journal of Recent Development in Engineering and Technology , (ISSN 2347 - 6435 (Online)) Volume 3, Issue 4, October 2014).

[7] MEHDI ENSHAEI, DR. ZURINA BT HANAPI "A Review on wormhole attacks in MANET" Journal of Theoretical and Applied Information Technology 10th September 2015. Vol.79. No.1, ISSN: 1992-8645.

[8] Shabina Parbin, Leeladhar Mahor "Analysis and Prevention of Wormhole Attack Using Trust And Reputation Management Scheme in MANET" 978-1-5090-2399-8/16/$31.00_c 2016 IEEE

[9] Samreen Banu Kazi, Mohammed Azharuddin Adhoni "Secure IDS to Detect Malevolent Node in MANETs" International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) – 2016.

[10] H.Ghayvat, S.Pandya, S.Shah, S.C.Mukhopadhyay, M.H.Yap, K.H.Wand " Advanced AODV Approach For Efficient Detection And Mitigation Of WORMHOLE Attack IN MANET" 2016 Tenth International Conference on Sensing Technology.

[11] Chitra Gupta, Priya Pathak "Movement Based or Neighbor Based Tehnique For Preventing Wormhole Attack in MANET" 2016 Symposium on Colossal Data Analysis and Networking (CDAN).

[12] Dhruvi Sharma, Rakesh Kumar "Reviewing the impact of Wormhole Attack in MANET" 2016 1st International Conference on Innovation and Challenges in Cyber Security (ICICCS 2016).

[13] Ankit Agrawal, Megha Patidar, Mayank Kumar Sharma "Performance Evaluation of Coordinated Node Monitoring & Response (CNMR) Based IDS for MANET" 978-1-4799-3064-7/14/$31. 00©20 14 IEEE.