International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 6, June 2017)

Three Step Malicious Node Detection Technique for Isolation of Blackhole Attacks in MANETs

Muntaha Manzoor Khan[1], Dr. Rakesh Kumar[2]
[1]Research scholar, [2]Professor and Director, Sachdeva Engineering College for Girls, Gharuan, Mohali, India

***Abstract*- The mobile ad hoc network has collection of nodes that are self-configured and the nodes can enter or leave the network as per the need. The network can be attacked by various malicious users due the decentralized nature. The various types of attacks are categorized as reactive and proactive according to their nature. The type of active attack that reduces the network's performance is terms of parameters such as throughput is known as the black hole attack. There is a need to recognize and separate the malicious node for which a novel technique is proposed in this paper which includes mainly three steps in it. The initial step involves the calculation of trust value, the second step involves the maintenance of the black list and the selection of cluster head is done in the final step. NS2 tool is utilized for implementing this proposed technique and as per the results the network throughput is increased, packetloss and delay is reduced in the network.**

***Keywords*-AODV, DSR, Blackhole, Ns2, Blacklist, Trust value**

I. INTRODUCTION

A network that allows the transferring of important information and does not involve any physical infrastructure is known as a mobile ad hoc network. As there is no physical design present within the network, this type of network is also known as infrastructure less type of network. The applications where there are no wired communications or wireless modes possible, the MANETs can be introduced to such applications. There can be a communication link set up with the help of a radio link and the nodes that have similar environment. There is a need to establish a secure path for providing communication amongst the nodes within the network [1]. There is a need to identify the other hub that to which the data can be transferred before establishing a secure communication.

For identification amongst each other, various credentials are to be given by the hubs that define them and provide their unique identities.

This helps in maintain authenticity and keeping the network secure and preventing the malicious users to enter the network area.

Before establishing communication, the node needs to ensure that the node present at the receiving end is not compromised and the data can be transferred safely. Attacks in MANET can be partitioned into two types they are active attack and passive attack [2]. In passive attack they include unauthorized listening in network and data is transferred without change. In active attack they extract information and they permit information stream between nodes.

A) Black hole Attack **:** Within this type of attack, a zero metric is presented by the attacker for all the destinations. The nodes that are present around the attacker are made to transfer all the received packets to it. Fake routing information is sent by the malicious hub which makes it look as an optimum route to transfer the data. So, the other nodes select the malicious node for transferring packets across the network. The packets received by the malicious hub are not sent further and are dropped within the network [3].

B) Wormhole Attack: The transferring of packets across the tunnels by diverting them from designated path and then further replaying them to the same path within the network is known as a wormhole attack. When the routing controlled messages are tunneled, the routing within the network is completely interrupted. A tunnel that is created between the two attacks is known as a wormhole which cannot be detected easily. It cannot be identified whether the path through which the packet is transferred belongs to that network or not. Without even knowing the important information related to the network, the wormhole attacks can destroy the network completely and thus are dangerous for the network.

C) Byzantine attack: The nodes that are present within the network and perform actions individually are compromised within this type of attack. The various actions such as generating routing loops, transferring the packets with the help of non-ideal paths occur within this attack. The routing services are degraded within the network through this attack as well [4].

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 6, June 2017)

D) Rushing attack: This attack is caused in case of wormhole attacks where the transmission paths are present between the two ends and two attackers participate within it. The propagation is done at higher speed as compared to the situations which involve simple multi-hop route.

E) Traffic Monitoring: There are different communications being carried out within the network which are identified within this attack. It uses the gathered information in such a manner that the attacks can be made to enter within the network on the basis of those actions being performed. Not only MANETs but all the types of networks are prone to this type of attack [5].

F) Eavesdropping: Within this attack, the unauthorized users can extract, read and transfer messages within the network. Mainly the wireless medium is present where such attacks are easily possible when the various hosts communicate with each other. RF is required for providing the wireless communication in most of the applications. The original message that is to be transmitted is eavesdropped here. Further any fake message is made to enter the network for causing problems or gathering important information.

G) Denial of service attack: The complete routing information is destroyed within this type of attack. Further the complete operation being performed also gets terminated due to this attack [6].

H) Gray-hole attack: During this type of attack numerous messages are dropped within the network. The gray-hole attack has two different phases. The hub advertises itself as having a route which is valid for providing communication from source to destination within the initial phase. The packets that are captured on the basis of a specific property are dropped by the node within the secondary phase.

The organization of this paper is in the following manner: Section 2 contains the review of related work. In Section 3 the proposed methodology which includes the Pseudo code of proposed technique is explained. Section 4 incorporates the discussion and also demonstrates the results .Section 5 states the Conclusion of this Research.

II. Literature Review

Chang, J.M. et.al proposed in this paper [7], that for providing proper communication between the numerous nodes, the basic need is to provide cooperation amongst them. The security of the network depletes once any malicious node enters the network due to which the routing process also gets affected. The detection as well as prevention of such malicious nodes which cause attacks such as gray hole or black hole attacks is a major concern.

For the purpose of solving various problems within this paper, a dynamic source routing mechanism known as Cooperative Bait Detection Scheme (CBDS) is utilized. The merits of proactive as well as reactive mechanisms are included within this method. As per the simulation results achieved there are different values acquired as per the presence of malicious nodes. Nadeem, A. et.al stated [8], that there are various types of attacks that enter the layers of the mobile ad hoc network layers. A survey of various attacks is present in the paper and further the intrusion detection as well as protection mechanisms are reviewed. There are various single types of attacks also known as point detection attacks which are one type of category in which the attacks can be divided. The second is the intrusion detection system (IDS) which involves range of attacks within it. On the basis of the proposed protection methods, comparative studies are made. The results evaluated show the properties of both of these techniques and their applications are defined accordingly. The further research areas are identified at the end. Yu, M. et.al recommended [9], that the detection and prevention of possible attacks on routing protocols is a major issue in securing the MANET. Mainly the internal attacks such as Byzantine attacks are discussed in this paper. In this paper, a novel algorithm is proposed which uses message as well as route redundancy for detecting internal attacks during route discovery. An optimal routing algorithm along with the routing metric is also proposed in this paper which combines the node's trustworthiness and performance properties. The existing routing protocols used in MANETs can be integrated and used for deriving the new proposed algorithms for MANETs. The advantages of the proposed attack detection and routing algorithm can be seen in the simulation results derived. The comparisons are made with some already known protocols to show the enhancements made in this work. Abbas, S. et.al intended [10] that due to the complex nature of MANETs and the resource constraint nodes, there is a need of lightweight security solutions. In MANETs Sybil attacks are a serious threat because these networks need unique, distinct as well as persistent identities for each node to make their security protocols viable. A new lightweight scheme is proposed here, which provides new properties that further help in recognizing the Sybil attackers present within the network. There is no involvement of third-party required within this study such as any hardware. There are various experiments performed and it is seen through the results that the proposed technique accurately identifies the Sybil attack within the network. Kannhavong, B. et.al resolved [11], that routing in MANET is a challenging task because of its various unique properties.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 6, June 2017)

A trusted condition is provided with the help of modified routing protocols within the mobile ad hoc networks. The major issue is generated within the network once there are malicious nodes present within the network. Attacks enter the network due to this. In this paper, all the possible attacks are discussed in details and discussions are made related to the state-of-art of the security problems. The routing attacks such as link spoofing and colluding misdirectional attacks are studied well. Also, the ways to prevent or remove such attack from the network are proposed in the existing MANET protocols. Liang,Y et.al explained in this paper [12], that there is a need to analyze the performance of mobile ad hoc networks in terms of throughput when malicious nodes are present within it. Here, the numbers of legitimate nodes are n and malicious nodes are m. For providing transmission amongst the legitimate nodes the delay constraint D is utilized. The performance of malicious nodes is analyzed within various types of attacks a proper analysis of the models is done under such scenarios. In the passive attacks situation, the information-theoretic approach is used for security purposes in case of attacks such as eavesdropping. The active attacks have to ensure more number of conditions is fulfilled on numerous malicious nodes as compared to the passive attacks for achieving same throughput. Zhao,Z. et.al suggested [13], that the dynamic nature of MANETs has resulted in making it vulnerable to numerous attacks in its infrastructure. The routing attacks result in damaging the MANET to greater extent and so they have been receiving greater attention in today's research. In this paper, to handle the various routing attacks in a systematic manner, a risk-aware response mechanism is proposed. This approach is based on the extended Dempster-Shafer mathematical theory of evidences. This method introduces a notion which enlists the important factors required. The experiments achieved show the effectiveness of this proposed approach on the basis of certain performance metrics.

III. Proposed Methodology

As the MANETs have decentralized nature, they are more prone to various attacks. Different active and passive attacks occur within the network due to presence of malicious nodes within the network. In this paper, a novel approach for identifying and isolating the malicious node from the network is proposed. The black hole attack is triggered within the network through this technique. There are three steps involved here.

1. The trusted value for each node is computed within the initial step. The numbers of packets that are re-transmitted within the network are computed here.
2. The secondary step involves the application of source node to prepare the list of nodes which may be malicious on the basis of sequence number which it collects from the nodes
3. In the third step, the clustering technique is been applied in which cluster head is selected which has maximum trust value. The data will be transmitted from one node to another through cluster head. This approach leads to isolation of malicious node from the network

A) Pseudo Code of proposed Technique

- Input: A network which contains malicious nodes in it.
- Output: The identification of the malicious node present within the network.

The source as well as destination node are defined within the network.

Within the network, the route request packets are flooded by the source node.

Source collects the route reply packets

Assign Trust value ()

1. Trust value=number of packets re- transmitted per unit time

Return (trust value)

Maintain blacklist ()

2. check sequence number of each node and time

If (Sequence number is exceptional high)

If (Time is minimum)

Blacklist=node;

End

End

If (node not in blacklist && maximum trust value)

Node =cluster head

Else

Node= cluster node

End if

End if

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 6, June 2017)

IV. Results And Discussion

Proposed technique is been implemented in NS2 by considering parameters which are described in table 1

Table 1.
Parameter values

Parameter	Value
Antenna type	Omi directional
Link layer	LL
Queue	Priority queue
Mac	802.11
Number of nodes	21
Area	800*800
Range	18 meter
Frequency	2.4 Ghz

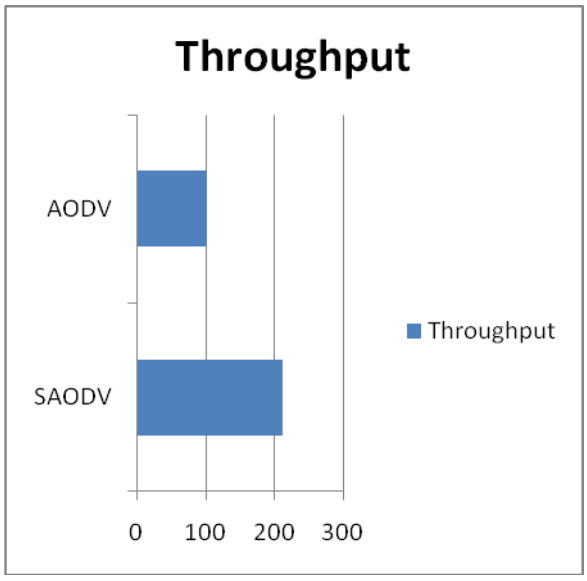

Fig 1: Throughput Comparison

As shown in figure 1, comparisons are made related to the throughput of the existing as well as proposed techniques. In case where the malicious node is present within the network, the throughput is enhanced within the network as per the simulation results.

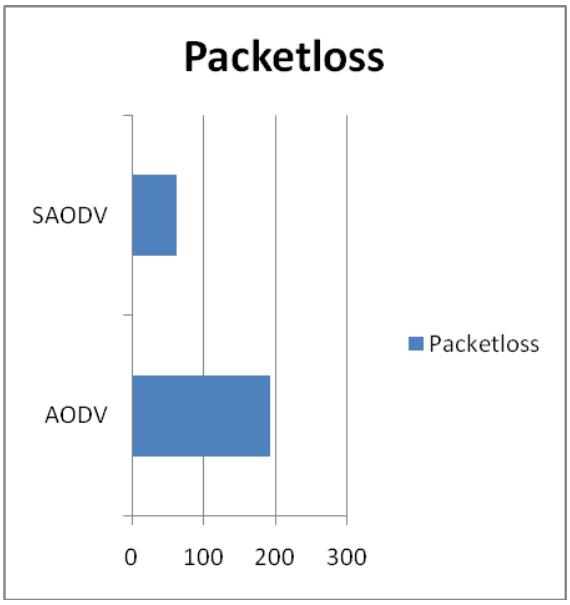

Fig 2: Packet loss Comparison

As illustrated in figure 2, the novel technique that provides routing of data with the help of AODV protocol is compared with the existing approach. There is reduction of packet loss within the network as shown through the various results.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 6, June 2017)

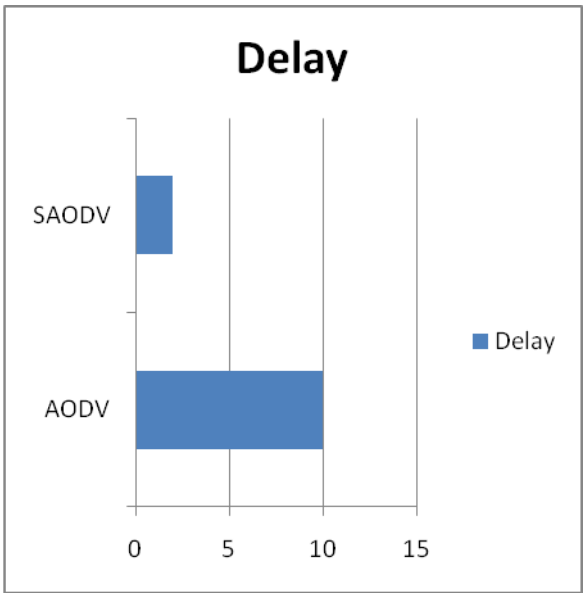

Fig 3: Delay comparison

As shown in figure 3, a comparison is made between the novel approach as well as the existing approach. The network delay is minimized in case when the malicious node is isolated from rest of the network as per the evaluations.

V. Conclusion

The performance of the network is minimized due to the presence of black hole attack in it. The proposed technique is based on three steps, and these steps are trust value calculation, blacklist technique and clustering phase used for node isolation. It is been analyzed that network throughput is reduced 28 percent, delay is reduced to 15 percent and packetloss is reduced to 30 percent. In future technique will be proposed which is based on IDS system which reduce node detection time

REFERENCES

[1] Liu, W., Lou, W., and Fang, Y. (2005), "An efficient quality of service routing algorithm for delay-sensitive applications," Computer Networks., vol. 47, no. 1, pp. 87–104.

[2] Leung, K. K., and Wang, L.C., (2002), "Integrated link adaptation and power control to improve error and throughput performance in broadband wireless packet networks," IEEE Trans. Wireless Communication., vol. 1, no. 4, pp. 619–629.

[3] Papadimitratos, P., and Haas, Z., (2002), "Secure routing for mobile ad hoc networks," SCS Communication Network Distribution System Model Simulator Conf., pp. 27–31.

[4] Perrig, A., Canetti, R., Song, D., and Tygar, J. D., (2001), "Efficient and secure source authentication for multicast," NDSS, San Diego, CA, pp. 90–100.

[5] Hu, Y.C., Perrig, A., and Johnson, D. B., (2003), "Rushing attacks and defense in wireless ad hoc network routing protocols," ACM WiSe, pp. 30–40.

[6] Perlman, R., (1988), "Network layer protocols with Byzantine robustness," Mass. Inst. Technol., Cambridge, MA, MIT LCS, TR-429.

[7] Chang, J.M., Tsou, P.C., Woungang, I., Chao, H.C., and Lai, C.F., (2015), "Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach", IEEE Systems Journal, Vol. 9, No. 1.

[8] Nadeem, A., and Howarth, M. P., (2013), "A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks", IEEE Communications Surveys & Tutorials, Vol. 15, No. 4.

[9] Yu, M., and Zhou, M., (2009), "A Secure Routing Protocol Against Byzantine Attacks for MANETs in Adversarial Environments", IEEE Transactions On Vehicular Technology, Vol. 58, No. 1.

[10] Abbas, S., Merabti, M., Llewellyn-Jones, D., and Kifayat, K.,(2012),"Lightweight Sybil Attack Detection in MANETs", IEEE.

[11] Kannhavong, B., Nakayama, H., Nemoto, Y., Kato, N., and Jamalipour, A., (2007), "A Survey Of Routing Attacks In Mobile Ad Hoc Networks", IEEE.

[12] Liang, Y., Vincent Poor, H., and Ying, L., (2011)," Secrecy Throughput of MANETs Under Passive and Active Attacks", IEEE Transactions On Information Theory, Vol. 57, No. 10.

[13] Zhao, Z., Hu, H., Ahn, G. J., and Wu, R., (2012), "Risk-Aware Mitigation for MANET Routing Attacks", IEEE Transactions On Dependable And Secure Computing, Vol. 9, No. 2.