Blacklist and Clustering Technique for Isolation of Blackhole Attack in Mobile Ad hoc Networks

Rama Sharma[1], Dr. Amardeep Gupta[2]
[1]*Research Scholar, Singhania University, Rajasthan, India*
[2]*Principal, DAV College, Dassua, India*

Abstract - The mobile ad hoc network is the decentralized and self-configuring type of network in which the mobile nodes can join or leave the network when they want. In the network, the malicious nodes enter which are possible to trigger active and passive types of attack. The blackhole attack is an active type of attack in which malicious nodes degrade the performance of the network to great extent in terms of throughput, delay, etc. In this research work, technique is proposed for detection and isolation of malicious node from the network. The proposed technique will be based on black list and clustering technique for the detection and isolation of malicious nodes. the performance of proposed technique is analyzed in terms of throughput, delay and packet loss which is increased at steady rate as compared to the existing technique.

Keywords - *Black hole, Black list, Clustering, RREP, RREQ*

I. INTRODUCTION

Wireless mobile network is the network which comprises of various small nodes which has numerous computing elements. The mobile nodes are very cheap and the amount of energy that is being consumed by them is also very small. There is very limited amount of energy present within these nodes as they are very small in size. There is very less processing capability of these nodes. Within these networks there are innumerable nodes present which are present in a very distributed manner. Various applications have deployed these types of networks present within them [1]. The physical parameters are measured here with the help of monitoring networks of the systems. The environment includes several parameters which can be computed and the overall weather conditions or any emergency situations can be identified. Within the applications, there are mainly mobile ad hoc networks applied which have helped in providing monitoring and surveying facilities to the applications [2]. Within these networks, the energy is provided to the mobile nodes such that the operations can be performed for gathering data from its surroundings. The networks are deployed in such locations in highly distributed manner and so it is impossible for the humans to change the batteries of those nodes once they are dead. The limited amount of energy present within the nodes results in their depletion. In order to resolve such issues which are mainly caused due to the depletion of mobile nodes, various techniques have been proposed which help in proposing mechanisms which can cause least energy utilization from the nodes. The increment in lifetime of the overall network is the major objective here [3]. There is a need to ensure the minimization of throughput or delay within the networks. The wireless sensor networks are decentralized in nature. Due to the absence of any central authority, this network is prone to various attacks. These attacks can be of active or passive types.

AODV Routing Protocol: Ad-hoc On-demand Distance Vector Routing Protocol (AODV) is the multi-hop type of protocol which helps in generating and handling the ad hoc network. The routes are generated to particular destinations by the AODV routing protocols. There is no need for the nodes to sustain those routes even in inactive state of communication [4]. The Route Request (RREQ) message is flooded in the network in order to provide a route to the destination for a node. The neighboring nodes are broadcasted with RREQ messages by the originating node. Either there is a very new route generated to the destination when a route has to receive the request or it itself is the path to the destination. Thus, a route reply (RREP) message is generated and sent to the source node in order to establish a path between the source and destination nodes. The routing tables of all the nodes present along the path are updated with the help of RREP messages [5]. This helps in keeping track of all the paths and shows that the packets can further also be routed in this network.

Black Hole Attack in AODV protocol: Within the AODV routing protocol, the routes can be generated only on the basis of the decisions made by the source node. The intermediate node replies to the RREQ packet within this process only in the case when the route towards the destination is completely new. A route reply (RREP) packet is unicasted back to the neighbor by the destination or intermediate node after the RREQ reaches the destination or the intermediate node with the availability of a fresh route. A route maintenance procedure is used to maintain the route once the route is

chosen or established. This process keeps continuing until it is not possible to reach the destination along each path from the source. It also keeps going until there is no need for the route anymore. Any loss of the link can be notified with the help of RERR (Route Error) message. The current sequence number and the sequence number of in RREQ packet plus one can be compared by the destination node while generating the RREP message [6]. The node that has the highest sequence number can be chosen once the number of RREP is received. However, when there is a blackhole attack occurring within the network and the source node broadcasts the RREQ message which the network, the blackhole node responds immediately with RREP message such that its sequence number is the highest in comparison to other nodes. The destination is after the black hole and it discards the other RREP packets which are arriving from all other nodes present in the network. As the route gets established, the source starts sending packets to the malicious node. Due to this, the malicious node which is a black hole node receives packets of data which are confidential [7]. After this, these packets are discarded or simply dropped within the network. Due to this, the nodes do not reach the destination due to the presence of black hole attack in the network.

II. LITERATURE SURVEY

Mohammed Baqer M. Kamel, et.al, (2017), have analyzed that MANET networks contain number of autonomous nodes that are directly connected with each other without any centralized controller. In this paper [8] to improve the existing AODV routing protocol security, authors have proposed a secure and trusted approach based on ad hoc on demand distance vector (STAODV). The new approach proves to be helpful in isolating the malicious nodes trying to attack the network and created a trust level between participated nodes. The proposed approach also help in examine and preventing the black hole attack in each incoming packet.

Pradeep R. Dumne, et.al, (2017), have discovered that infrastructure less property is adopted by MANET due to change in its nodes location. Mobile ad-hoc network (MANET) consist group of mobile nodes that make relation between each other without using any fixed centralized supervision of the network. In this paper [9], authors have proposed DSR mechanism- cooperative bait detection (CBDS) based scheme for malicious node detection. The proposed scheme uses hybrid defense architectures that help in finding the malicious node by using reverse tracing technique. The proposed and existing basic schemes are implemented on NS-2.35 in order to examine it on the basis of throughput and PDR.

P. Rathiga, et.al, (2016), have analyzed that there will be loss of packets due to different Denial of Service attacks such as black hole and gray hole. In this paper [10], the authors have proposed a novel black/gray hole detection technique. This technique is used in MANET Dynamic Source Routing (DSR) protocol for detecting black and gray hole attacks. Experimental results of proposed scheme shows that this hybrid black/gray hole detection approach detects and eliminates the attacks effectively. The results are improved in terms of throughput, packet drop rate, packet delivery ratio and routing overhead.

Ram Kishore Singh, et.al, (2016), have analyzed that MANET are based on the routing algorithms that adopts the changes of random network topology. In this paper [11], authors have presented the review of different routing protocols such as AODV, DSR and etc. They have also presented a behavior and counter measures of attacks in different layers. In order to provide security in MANET, number of researchers has developed different protocols and algorithms that help in removing the security issues. The authors have done main focus on making the unique algorithm approach that provides both security and improvement in performance of an AODV routing protocol. This unique algorithm approach is implemented in the network simulator NS2 in order to check its performance.

Sagar R Deshmukh, et.al, (2016), have identified that mobile ad-hoc networks (MANET) are growing fast due to promising growth in utilization of mobile devices. MANETs have properties of self configuration and infrastructure less makes them easily deployable, extremely dynamic in nature. In this paper [12], authors have proposed a new secure rooting mechanism based on AODV. The proposed mechanism helps in detecting and eliminating black hole attack and affected routes. They have also attached one RREP value that ensures that no attack exist along the path. The simulation results of proposed mechanism is tested and verified in NS2.

Mohamed A. Abdelshafy, et.al, (2016), have analyzed that MANET routing protocols are based on assumption that all nodes cooperate without maliciously disturbing the operation. In this paper [13], authors have introduced a new concept of Self-Protocol Trustiness (SPT). This scheme appeals the malicious node to give hidden statement of its malicious behavior. In order to oppose such attacks, authors have proposed Blackhole Resisting Mechanism (BRM) that can be built into any reactive routing protocol. The performance of proposed and existing routing protocol is compared using NS simulator which shows that proposed protocol is efficient in terms of reducing the effect of a blackhole attack.

III. RESEARCH METHODOLOGY

The mobile adhoc networks are the decentralized type of network in which malicious nodes enter the network which is responsible to trigger various type of attacks. The attacks are

broadly classified into active and passive attacks. The blackhole attack is the active type of attack which reduces network performance in terms of throughput, packetloss and delay. In this research work, technique is proposed which will detect and isolate malicious nodes from the network. The proposed technique consists of the following steps:-

1. Input: Mobile Nodes, Malicious noder

2. Output: Detection and isolation of malicious node

1. Deploy wireless adhoc network with finite number of mobile nodes
2. Source node sends route request packets in the network and start timer t to receive the route reply packets
3. Adjacent nodes of destination respond back with route reply packets
4. Source node check which node send route reply in minimum amount of time
5. Construct blacklist which has identification of node which sent route reply in least amount of time
6. Check trust value of each node on the basis of number of packets re-transmitted by each node
7. If (Node in the blacklist ==node which has least trust values
8. Malicious node=Node(i)
9. Divide whole network into fixed size clusters using location base clustering
10. Select cluster in each cluster which has maximum trust value
11. Data will be transmitted from source to destination through cluster head

IV. RESULTS AND DISCUSSION

The proposed technique is implemented in NS2 and compared with the existing techniques in terms of various parameters**.**

Table.1: Simulation Parameters

Parameter	Value
Network Area	800 m x 800 m
Simulation Time	18 second
MAC Type	802.11
Traffic Type	CBR
Routing Protocol	AODV
Data Rate	0.05 packets/ seconds
Number of Nodes	18
No. of Adversaries	1 to 3

Fig.1: Throughput graph

As shown in this figure 1, the existing throughput is shown by the red line and the proposed throughput is presented here by the green colored line. The time is given as x-axis and numbers of packets to be transmitted are shown at the y-axis. As per the graph, it is seen that the throughput of proposed technique is higher in comparison to the throughput of existing technique.

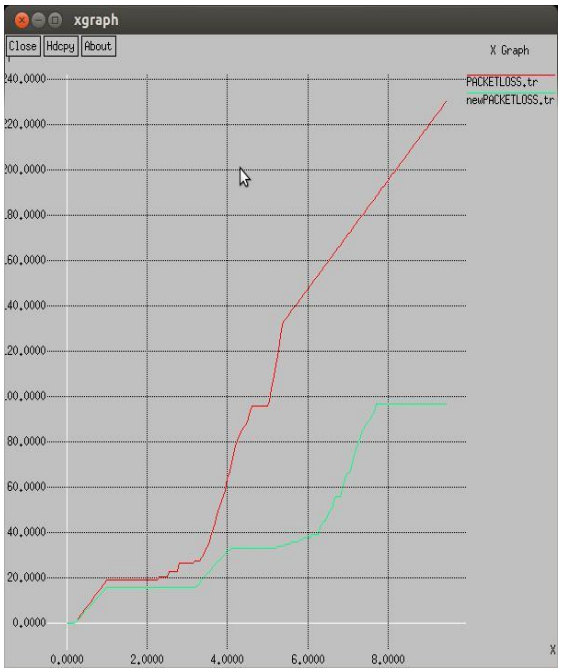

Fig.2: Packet loss Comparison

As shown in figure 2, the packet loss within the existing approach is shown by red line and the green line depicts the packet loss of proposed technique. The time is shown on x-axis and the packets being transmitted are shown on y-axis. As per the comparisons made the packet loss in the proposed technique is less in comparison to the existing technique.

V. CONCLUSION

In this research work, it has been concluded that blackhole attack is the active type of attack which can reduce the network performance in terms of certain parameters. The black hole attack is triggered by the malicious nodes which enter the network due to decentralized property of mobile ad hoc networks. In this research work, the black list and clustering technique is proposed which detects and isolates malicious node from the network. The results are analyzed in terms of throughput, delay and packet loss.

VI. REFERENCES

[1]. Juby Joseph, Vinodh P Vijayan," Misdirection Attack in MANETS Due to Selfish Nodes; Detection and Suppression using Longer Path Protocol", 2014 Vol.4

[2]. Dr. G. Padmavathi, Mrs. D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Mobile Networks", International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, 2009, pp. 1-9

[3]. Ju young Kim, Ronnie D. Caytiles, Kyung Jung Kim, "A Review of the Vulnerabilities and Attacks for Wireless Mobile Networks" Journal of Security Engineering, 2014, pp.241-250

[4]. Kalpana Sharma and M K Ghose, "Wireless Mobile Networks: An Overview on its Security Threats" IJCA Special Issue on "Mobile Ad-hoc Networks" MANETs, 2010, pp.42-45

[5]. Kalpana Sharma and M K Ghose, "Wireless Mobile Networks: An Overview on its Security Threats" IJCA Special Issue on "Mobile Ad-hoc Networks" MANETs, 2010

[6]. LV Shaohe, Wang Xiaodong, Zhao Xing," Detecting the Sybil Attack Cooperatively in Wireless Mobile Networks", Computational Intelligence and Security 2008, CIS '08 International Conference on Volume 1Suzhou, pp.442-446, IEEE 2000

[7]. Baviskar B.R, Patil V.N," Black hole attacks mitigation and prevention in wireless mobile network", International Journal of Innovative Research in Advanced Engineering (IJIRAE), Volume 1, Issue 4, pp. 167-169, May 2014.

[8]. Mohammed Baqer M. Kamel, Ibrahim Alameri, Ameer N. Onaizah, "STAODV: A secure and trust based approach to mitigate Blackhole attack on AODV based MANET", Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), 2017 IEEE 2nd international conference, vol.6, pp.1278-1288, 2017.

[9]. Pradeep R. Dumne, Arati Manjaramkar, "Cooperative Bait Detection Scheme to prevent Collaborative Blackhole or Grayhole Attacks by Malicious Nodes in MANETs", IEEE 2016 5th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions), vol. 9, pp. 486-490, 2017.

[10]. P.Rathiga, Dr.S.Sathappan, "Hybrid Detection of Black hole and Gray hole attacks in MANET", IEEE 2016 International Conference on Computational Systems and Information Systems for Sustainable Solutions, vol. 7, pp. 135-140, 2016.

[11]. Ram Kishore Singh, Parma Nand, "Literature Review of Routing Attacks in MANET", IEEE International Conference on Computing, Communication and Automation (ICCCA2016), vol. 6, pp. 525-530, 2016.

[12]. Sagar R Deshmukh, P N Chatur, Nikhil B Bhople, "AODV-Based Secure Routing Against Blackhole Attack in MANET", IEEE International Conference On Recent Trends In Electronics Information Communication Technology, vol. 7, pp.1960-1965, 2016.

[13]. Mohamed A. Abdelshafy, Peter J. B. King, "Resisting Blackhole Attacks on MANETs", 2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC), vol. 6, pp. 121-128, 2016.