© 2018 IJSRST | Volume 4 | Issue 8 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

Performance Evaluation and Prevention of Black hole attack in MANET

Vimala Manohara Ruth P, Kavita Agrawal, Sumanth Paruchuri, Vamshi Krishna Gundu
Department of Computer Science and Engineering, Chaitanya Bharathi Institute of Technology, Hyderabad, Telangana, India

ABSTRACT

Mobile Ad-hoc NETwork (MANET) is a collection of mobile nodes which are wire-less, self-organized and infrastructure-less where communication between the nodes is through radio waves. Therefore, security becomes a highly challenging issue in MANET's. Malicious nodes in the network may lead to security breach and degrades the performance of the network. In black hole attack, malicious node will advertise itself as having a fresh route towards destination and starts dropping the packets thereby degrading the performance and reliability of the network. In this paper, the performance metrics of a MANET such as Throughput, Packet Delivery Ratio and Packet Loss are evaluated using single and multiple malicious nodes. A fake routing protocol is proposed to prevent black hole attacks imposed by both single and multiple black hole nodes. Simulation results show that the proposed protocol provides better performance in terms of packet delivery, throughput and packet loss in presence of black holes and helps in prevention of black hole attack.

Keywords : Black hole, Fake routing protocol, MANET, Network Animator, NS2.

I. INTRODUCTION

MANET is are suitable for Military networking requirements, safety/rescue operations, wearable computing and communications, satellite-based information delivery and finally in scenarios requiring rapidly-deployable communications with survivable, dynamic networking mobile data exchange (RFC 2501). There are many issues in MANET such as Routing, Attack, Topology Management, Context awareness, Identity Management, Power Management, etc. Due to the openness in network topology and the absence of centralized administration in management, MANETs are vulnerable to attacks from Black hole nodes. The packet loss due to the Black hole nodes has been detected and to be isolated from the mobile ad-hoc network to increase the reliability of the network. The proposed work is to prevent attacks from Black hole nodes and improve the security performance of the whole network, especially in terms of packet delivery ratio, average end-to-end delay. To overcome this, a Dynamic trust prediction model is proposed. This model is used to calculate the trust value, which is based on the nodes historical behavior as well as the future behavior. By using this, one can detect the untrustworthy nodes, obtain a reliable packet delivery route and alleviate the attacks from Black hole nodes that provide a flexible and feasible approach to choose the shortest route that meets the security requirements of data packet transmission.

II. RELATED WORKS

Fan-Hsun Tseng et al., [1] provided a survey of attacks and countermeasures in MANET. The countermeasures are features or functions that reduce or eliminate security vulnerabilities and attacks. First, they have given an overview of attacks according to the protocol layers, and to security attributes and mechanisms. Then they presented preventive approaches following the order of the layered protocol layers. They also put forward an overview of MANET intrusion detection systems (IDS), which are reactive approaches to thwart attacks and used as a second line

of defense.

Rakesh Kumar Singh et al., [2] provided an overview about the security issues and available detection techniques in Mobile ad hoc networks. They identified the existent security threats an ad hoc network faces, the security services required to be achieved and the countermeasures for attacks.

Sushama singh et al., [3] introduced trusted AODV routing protocol whose trust value is calculated using tangent hyperbolic function. The results showed performance improvement as compared to standard AODV protocol.

Vimal Kumar et al., [4] proposed a technique that uses coming route reply table (CRRT) to detect black hole attack. This table is maintained by source node and it stores destination sequence number and ID of replied node. This information is used for detecting black hole attack in MANETs. The simulation result of proposed technique improves PDR and throughput of network.

Sandeep Dhende et al., [5] proposed a secure AODV protocol (SAODV) for detection and removal of black hole and gray hole attacks in MANET. The proposed method simulated using NS-2 and the proposed methodology is more secure than the existing one.

Arvind Dhaka et al., [6] proposed a scheme that uses Cseq and Rseq packets to identify and prevent black hole and gray hole attack in MANETS. If Rseq is equal to Cseq then and then only the source node allows connection to the network layer. If Rseq is not equal to Cseq then the sender of Rseq is detected as malicious node. The simulation result showed that the PDR increases and delay decreases by significant amount.

Meenakshi Sharma, et.al, [7] designing mechanism for eliminating effect of multiple black hole nodes by using novel scheme. In this scheme, detection is possible using fake RREQ message and modified RREP message. When the black hole node gets RREQ message it replies to the source node with minimum hop count. In case, the source identify black hole node and tells its neighbor node that it is malicious node. The analyzing result shows the comparison between novel scheme and standard AODV. After prevention more number of packets will be transmitted so, throughput of novel scheme is higher and end to end delay is lower than original AODV.

III. METHODOLOGY

The steps involved in the proposed algorithm for performance evaluation are:

1. Create a MANET
2. Implementation of AODV routing protocol [8,9]
3. Insert nodes into the network
4. Introduce malicious node into the network
5. Send packets from source to destination
6. Display moment of nodes and packets in NAM
7. Evaluate performance metrics
8. Generate graphs using Xgraph

The steps involved in proposed algorithm for black hole prevention are:

1. Create MANET
2. Implement Fake routing protocol
3. Insert mobile nodes and malicious nodes into the network
4. Source broadcasts RREQ (Route Request message) with its own ID (SSN (Source Sequence number)) [10] in place of DSN (Destination Sequence Number)
5. Intermediate Nodes sends RREP (Route Reply message) packet having highest SSN
6. If (RREP(SSN)>RREQ(SSN)) [10] is true then node is blacklisted and other nodes are notified. Otherwise normal routing process of AODV is involved
7. Display results in NAM and terminal

The proposed multiple black hole nodes detection mechanism algorithm:

1. The source node broadcasts the fake RREQ packet with its own source sequence number and address in the destination sequence number and destination address in the RREQ packet fields respectively [11].
2. When legitimate nodes receive the fake RREQ packet, it will compare the source sequence number in fake RREQ packet it received with the sequence number of the source described in the table.
3. As the source node sends its own sequence number, it will be more obvious that it will be the latest or fresh one. The intermediate node will have the source sequence less than the described in fake RREQ packet. So it will not reply with RREP packet.
4. But, if there exists any black hole node in the network then it will reply with the RREP packet and advertises itself as having the shortest path with highest source sequence number.
5. The source node will then detect the black hole nodes exist in the network. And then send the packet [12] having the list of black hole nodes to the rest of the nodes.

Network Simulator-2 (NS-2)

NS-2 is a packet –level simulator and essentially a centric discrete event scheduler to schedule the events such as packet and timer expiration.

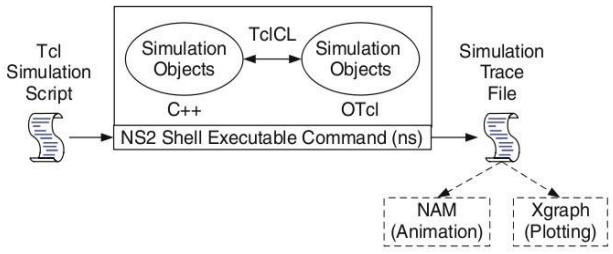

Fig 1. Working of NS-2

Network Animator (NAM)

NAM provides a visual interpretation of the network topology created. The application was developed as part of the VINT project. Its features are as follows. Displays the NAM application and its components. Provides the visual interpretation of the network created. Can be executed directly from a tcl script. Controls include play, stop, ff, rw, pause, a display speed controller and a packet monitor facility.

It presents information such as throughput, number packets on each link. Provides a drag and drop interface for creating topologies.

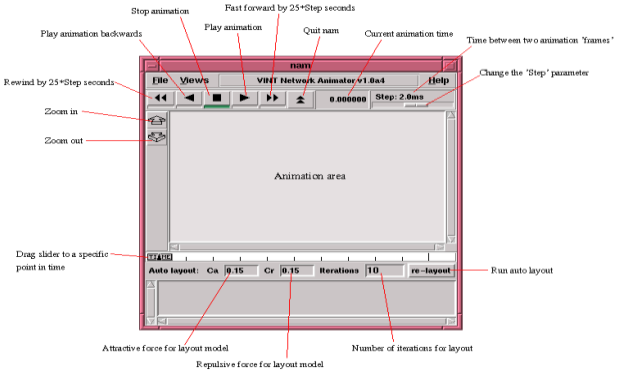

Fig 2. Network Animator

IV. RESULTS

Performance Evaluation

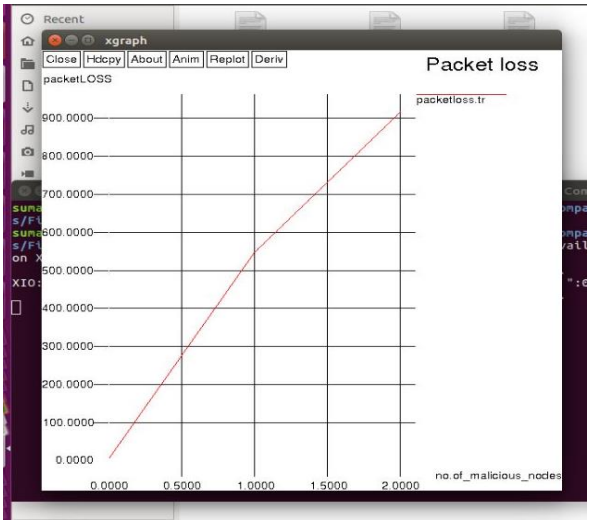

Fig 3. Malicious nodes X Packet loss

The above figure is a graph drawn between number of malicious nodes and packet loss, it is observed that as the number of malicious nodes in the network increases, the packet loss increases. When there is no malicious node at all the packet loss is almost zero, when there is a single malicious node the loss gradually increased to around 500 packets, when there is another malicious node the packet loss increased very rapidly to 900.

Packet loss= No. of packets sent – No. of packets received

Table 1. Packets dropped by one and two malicious nodes

No of nodes in the network	Packets dropped by 1 malicious node	Packets dropped by 2 malicious nodes
20	742	976
50	1187	1226
100	1094	1119

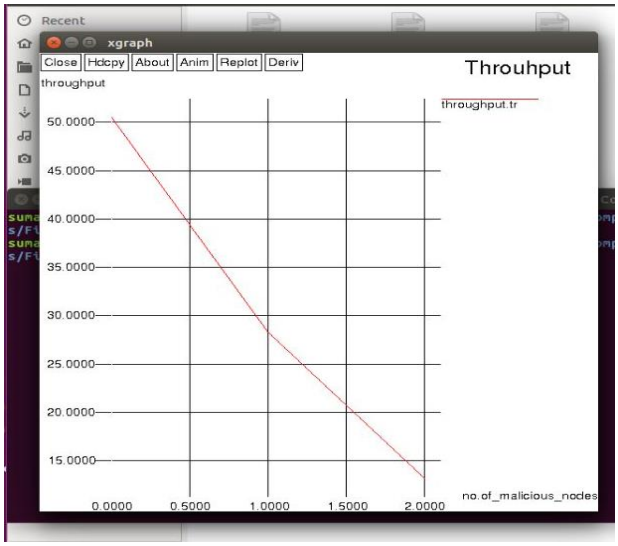

Fig 4. Malicious nodes X Throughput

Throughput = No. of packets received/Simulation time
Throughput is inversely proportional to time, so as the time taken to a packet to reach destination increases, throughput decreases. When there is no malicious node the throughput is very high around 50, when there is a single malicious node throughput has decreased to 28. When there are two malicious nodes there is no enough throughput , it is decreased below 15.

Table 2. Throughput in the presence of one and two malicious nodes

No of nodes	Throughput for 1 malicious node	Throughput for 2 malicious node
20	1782	943
50	186.48	146.62
100	520	430

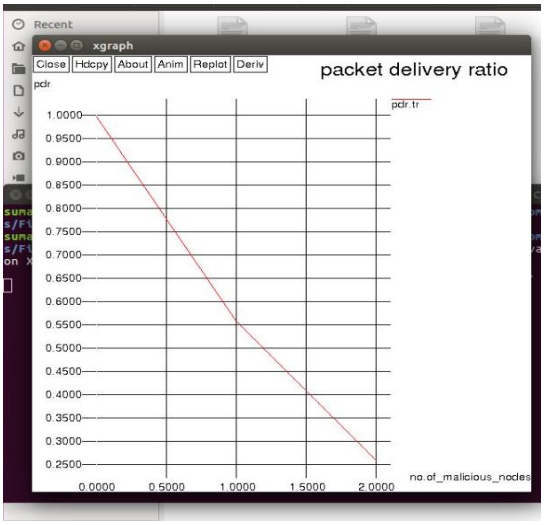

Fig 5. Malicious nodes X PDR

Packet Delivery Ratio (PDR) = number of packets received/number of packets sent

When every packet reaches the destination from source then the packet delivery ratio is one as number of packets sent is equal to number of packets received. It is observed from the graph that when there is no malicious node the packet delivery ratio is maximum to one, which means all the packets are reached from source to destination. As the malicious nodes in the network increased the packet delivery ratio gradually decreased, when there are two malicious nodes the delivery ratio is below 0.25.

Table 3. PDR in presence of one and two malicious nodes

No of nodes	PDR for single malicious node	PDR for two malicious node
20	40.02	21.2
50	4.19	1.04
100	11.70	9

Prevention Evaluation

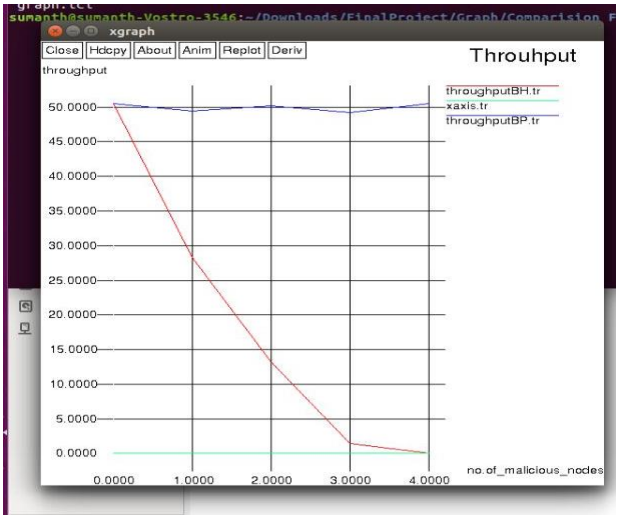

Fig 6. No. of malicious nodes X Throughput

From the above graph it is observed that the throughput is decreasing when there is a blackhole attack which is shown by red color line. When prevention is done throughput is good which is shown by a blue line.

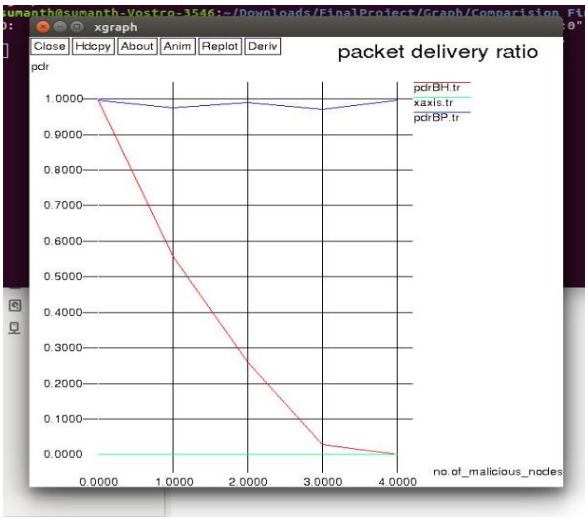

Fig 7. No. of malicious nodes X packet delivery ratio.

From the above graph it is observed that the packet dellivery ratio is decreasing when there is a blackhole attack which is shown by red color line. When prevention is done packet delivery ratio is good which is shown by a blue line.

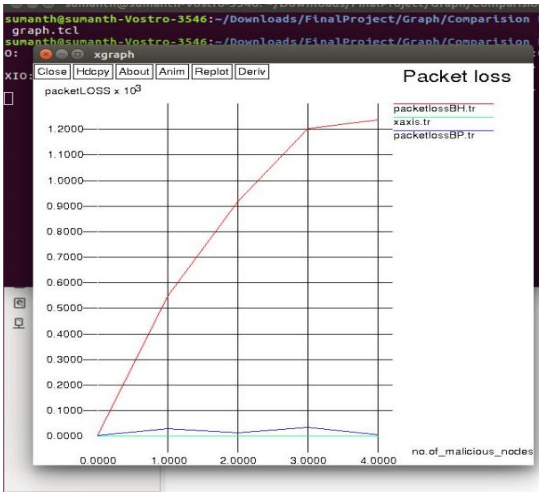

Fig 8. No. of malicious nodes X packet loss

From the above graph it is observed that the packet loss is increasing when there is a blackhole attack which is shown by red color line. When prevention is done packet loss is very less which is shown by a blue line.

IV. CONCLUSION

Black hole attack in MANET is analyzed using AODV routing protocol. The main criteria is analyzing the system performance with no black hole, single black hole and multiple black holes and at the end preventing the black hole attack from consuming the packets thereby increasing the performance of the network.

The following parameters were evaluated to measure the performance of the MANET:

(a) Throughput
(b) Packet Delivery Ratio
(c) Packet loss

It is observed that the routing of data Packets in the mobile ad hoc networks using AODV routing protocol

is affected when there is a Black hole attack due to which the efficiency of the network degrades. In the prevention of black holes this technique assumes that the source node is an intelligent node which uses the sequence number concept to detect the multiple black hole nodes in MANET. This detection mechanism is effectively implemented using NS 2.35.

V. REFERENCES

1. Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao, "A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks", Human-centric Computing and Information Sciences,Springer, New York, pp. 1-16, 2011.
2. Rakesh Kumar Singh, Rajesh Joshi and Mayank Singhal, "Analysis of Security Threats and Vulnerabilities in Mobile Ad Hoc Network (MANET)", International Journal of Computer Applications (0975 – 8887) Volume 68– No.4, April 2013.
3. Sushama Singh, Atish Mishra and Upendra Singh, "Detecting and Avoiding of Collaborative Black hole attack on MANET using Trusted AODV Routing Algorithm", Symposium on Colossal Data Analysis and Networking (CDAN), 2016.
4. Vimal Kumar and Rakesh Kumar, "An Adaptive Approach for Detection of Blackhole attack in Mobile ad hoc Network", Procedia Computer Science, vol. 48, pp. 472–479, 2015.
5. Sandeep Dhende, Sandeep Musale, Suresh Shirbahadurkar and Anand Najan, "SAODV: Black Hole and Gray Hole Attack Detection Protocol in MANETs", IEEE WiSPNET Conference, 2017.
6. Arvind Dhaka, Amita Nandal, and Raghuveer S. Dhaka, "Gray and Black hole attack identification using Control Packets in MANETs", Procedia Computer Science, vol. 54, pp. 83–91, 2015.
7. Meenakshi Sharma and Davinderjeet Singh, "Implementation of a Novel Technique for a Secure Route by Detection of Multiple Blackhole Nodes in Manet", International Journal of Current Engineering and Technology, vol. 4, no.1, pp. 56-59, February-2014.
8. Nishu Kalia and Harpreet Sharma, "Detection of Multiple Black hole nodes attack in MANET by modifying AODV protocol", International Journal of Computer Science and Engineering, 2016.
9. Uma Rathore Bhatt, Abhishek Dangarh, Akanksha Kashyap, Aishwarya Vyas "Performance analysis of AODV & DSR Routing protocols for MANET", Fourth International Conference on Communication Systems and Network Technologies, 2014.
10. Umang, B V. R. Reddy and M .N. Hoda, "MNI-AODV: Analytical Model for Attack mitigation using AODV routing in ad hoc networks", International Conference on Computing for Sustainable Global Development (INDIACom), 2014.
11. Chang Wu Yu, Tung-Kuang Wu and Rei Heng Cheng, "A Distributed and Cooperative Blackhole Node Detection and Elimination Mechanism for Ad Hoc Network", PAKDD Workshops, Nanjing, China, 22-25, pp. 538-549, 2007.
12. E.A. Mary Anita and V. Vasudevan, "Blackhole Prevention in Multicasting Routing Protocols for Mobile Ad hoc Networks using Certificate Chaining", International Journal of Computer Applications, Volume 1, pp. 21-28, 2011.