Simulation and Analysis of Blackhole Attack in MANETs for Performance Evaluation

Bobby Sharma Kakoty
Department of Computer Science & Engineering
Don Bosco College of Engineering and Technology
Assam Don Bosco University, Guwahati, India

Abstract - Mobile Adhoc Network is a very powerful, flexible, dynamic, infrastructure less network, in which all the mobile nodes have the right to move around. Every node is recognized as host as well as guest at the same time. There is no central server due to which MANETs are very vulnerable to several kinds of threats. Out of all these attack, one of the most severe attacks is packet drop attack. Packet drop attack may be the consequence of several causes. But most important kind of *Daniel of Service* attack which is known as *Blackhole* attack is considered as most serious cause of *packet drop*. When MANET is suffered from such kind of attack, all of a sudden, network performance is degraded. The efficiency of MANET is totally dependent on co-operation of nodes. If the nodes don't forward the packets to its neighbor, automatically throughput of the network will decrease. This paper includes functionality of Blackhole attack, routing in MANETs with or without Blackhole attack. Finally through simulation it justifies that network performance is degraded in presence Blackhole malicious node.

I. INTRODUCTION

Mobile Adhoc Network (MANETs) consists of some collection of mobile nodes that co-operate within the network zone to forward packets. The performance of MANET depends on the accuracy of packet forwarding nature of nodes. Such kind of network doesn't depend on predefined network infrastructure. They have dynamic topology. There is no central server to monitor the intrusions or any other activities happened in the network. Due to the absence of centralized monitoring mechanism to observe network functionality, in most of the cases MANETs have to depend on routing protocol [6] [8]. Though the nodes rides freely over the wireless network but they suffer from limited resources including bandwidth, memory, processing time and open medium.

Each node should bear the responsibility of packet forwarding to next hop for proper delivery of packets from source to destination. MANETs are also self-organized. These kinds of networks are used vastly in some crucial work area like battlefield or some disaster prone region or in some tactical region etc. where network infrastructure is not guaranteed.

Though MANET is very flexible in its applications, but it is very much vulnerable to different kind of attack in comparison to wired network [15]. So security issues may occur in various points like lack of central monitoring, frequent change of network topology, node mobility, open medium etc. At the same time it is again vulnerable to various kind of attack like behavioral based attack, location based attack, security attack such as Denial of Service attack, impersonation, eavesdropping, Sybil attack, wormhole attack, sinkhole attack, Blackhole attack etc [15]. This paper is mainly emphasized on Blackhole attack in MANETs and it contains the following sections.

Section II briefly describes about few related works. Section III contains Routing in MANETS with and without Blackhole node, section IV contains AODV and Blackhole attack for packet drop. Finally section V shows the simulation result with different condition for different evaluation parameters.

II. RELATED WORKS

In [2], author presents simulation and analysis of Blackhole attack in MANETs with reactive routing protocol AODV. Author also shows the workability of AODV protocol in MANETs regarding RREQ, RREP and explains how Blackhole attack is associated with RREQ and RREP message. The attacker generates fake RREP message to sender and then drop the packets instead of forwarding these to original destination. For simulation, they had used Qualnet simulator, with 40 numbers of randomly allocated wireless nodes. The performance parameters are evaluated in terms of packet delivery ratio and throughput with respect to node mobility. But it has dropped some important factors like how packet delivery ratio, throughput of a network etc. are changing with increased number of malicious node as well as change of pause time of the nodes.

In [15], author explains about the effect of Blackhole malicious node in MANETs. Author explains about the different security issues and security attack in MANETs. For simulation purposes, NS 2 had been used. Simulation was done for two scenarios, in case of first scenario, number of nodes participated in the network are kept constant

while number of Black hole nodes are increasing up to certain numbers. On the other hand, in the second scenario, number of Blackhole nodes and number of other nodes were changing in such a way that their ratio remains constant. Network performance parameters are measured in terms of packet loss with increased number malicious nodes, packet delivery ratio with respect to node mobility in presence of Blackhole malicious node and impact of end to end delay with varying number Blackhole nodes and node mobility. Here also author did not consider another important factor of MANETs i.e. pause time. How pause time impact the network in presence of Blackhole malicious node.

III. ROUTING IN MANETS WITH AND WITHOUT BLACKHOLE NODE

Generally routing in MANET is done either by table driven routing protocol or adhoc on demand distance vector routing protocol. In case of table driven process, each and every node in MANETs maintains some up-to-date information about the network. Every node has the information about latest network topology, any changes happened to the network is generally propagated to the network, accordingly node updates their routing table [1]. But this kind of protocol creates several problems to the network in terms of bandwidth overhead, wastage of battery power of the nodes, entry of unnecessary redundant route etc.

Due to these difficulties, adhoc on demand distance vector (AODV) routing protocol is preferred. In this protocol, routing tables are dynamically created when needed. So, whenever source node wants to send data to destination, it tries to establish the path through several ways by sending some RREQ packets. When destination sends a RREP packet to source through shortest path, the source sends data through this path. Though it looks very simple, but this kind of protocol suffers from several vulnerabilities of attack. If the path cannot be established then RERR messages is generated. AODV protocol is very much acquainted with dynamic network condition, low processing and memory overleaf, less bandwidth wastage with small control messages. Due to these kinds of reasons AODV becomes one of the most popular protocol in MANETs.

Whenever a RREQ packet is generated by the source, every node that receives the RREQ packet will check whether this packet is meant for them or not. If so, immediately they will generate RREP message, otherwise every node tries to forward the packet to their neighbor to reach destination [2], if their routing table doesn't contain valid entry to destination. If the routing table contains valid entry to destination then next step is to check the destination sequence number. Usually destination sequence number is maintained by every node. Its value depends on network traffic and participation of node in packet forwarding. If the destination sequence number is same for more than one RREP then it goes for the specific path where number of hops to reach destination is lesser [4] [3]. Thus higher the sequence number implies the fresh route to destination. In case if the source receives multiple RREP then it decides the path where sequence number is higher[3].

IV. AODV AND BLACKHOLE ATTACK FOR PACKET DROP

Blackhole attack for packet drop is one of the active DoS attack in MANETs in which malicious node sends forged RREP packet to source to establish a false path so that it can absorb all the packets sent from source to destination without delivering the packets to actual destination[6]. Lots of related works are going on for establishing a secure MANETs in several ways[9][10][11][12].

Here the malicious node sets a higher sequence number to show its existence and establish a spurious route to the source before the actual RREP message achieved from the neighbor. In case of same sequence number, of course, the sender accepts a path having small hop count. Accordingly sender assumes that route discovery process was over and ignores other RREP messages and start sending packets to malicious node. In this way malicious node attack all RREQ messages and finally receives most of the packet to itself and doesn't forward the packet to other node.

In case of route discovery process of AODV, the sender sends a RREQ control packets to all probable neighbor to have route to destination. If within the specific time route is not established, the sender may again try to establish a route by broadcasting another RREQ and repeats the same till maximum TTL(time to Live) value is achieved[4]. Blackhole attack exploits the property of AODV by establishing a false route to the source to drag the packets towards it. It never forwards the packets to other nodes, instead of that it consumes the incoming packets in itself or drop the packets[5].

V. NETWORK PERFORMANCE IN PRESENCE OF BLACKHOLE ATTACK

Since Blackhole attack either tries to drop the packet instead of forwarding the packet to destination or consumes intercepted packet silently, so it becomes a very dangerous denial of service attack for the network. The actual effect of black hole attack is strongly based on type of protocol used in the network. It losses the packet abruptly. As a result mainly the packet delivery ratio and the throughput of the network reduced abnormally along with some

other network performance parameters. To observe this we have established a simulation environment using NS 2.32 as follows:
Here the performance of network parameters are evaluated with implementation of varied number of black hole nodes. Also performance is evaluated with varying pause time as well in different node speed with implementation of black hole nodes. For performance evaluation, Ns 2.32 is taken. Simulation is done for random waypoint model in a rectangular field. Reactive protocol AODV is taken as routing protocol with CBR traffic type, transmission range of 100 m, packet size 512 byte, data rate of 100 kb/s, for an area of 1000m X 1000m. The simulation is done for 300s for 30 nodes. Initially, network performance parameters are observed by gradually increasing number of black hole nodes with constant pause time and node speed as in figure(1-5). Then the simulation is done with varying pause time and node speed with constant number of malicious nodes i.e. 20%
Different performance matrices are observed as follows:

5.1. Packet delivery ratio(PDR)-

Packet Delivery ratio is the most important factor of a network based on which network performance can be easily determined. Normally it is determined by dividing the number of packets received by the destination through the number of packets originated by the application layer of the source (i.e. CBR source).. Figure 1 shows that as number of Blackhole node increases, packet delivery ratio of the network gradually decreases for moderate velocity of the nodes as well as for constant pause time. But when the pause time is varying for fixed number of mobile nodes and fixed number of Blackhole malicious nodes(20% of total nodes), packet delivery ratio is changing differently like zigzag. It is shown in Figure 2. But in Figure 3 explains that as the node velocity increases for fixed number of nodes and fixed number of malicious nodes (Blackhole nodes), packet delivery ratio decreases on average basis.

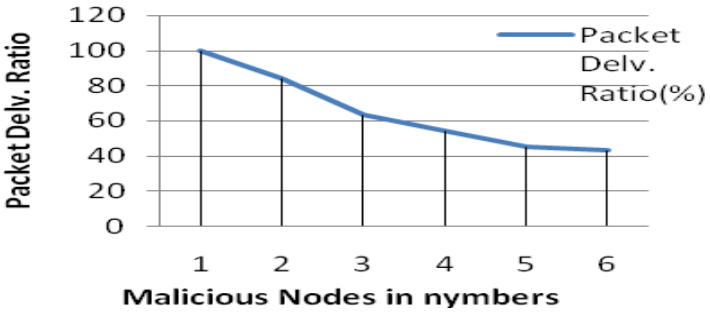

Figure 1. Packet Delivery Ratio with increased number of blackhole nodes

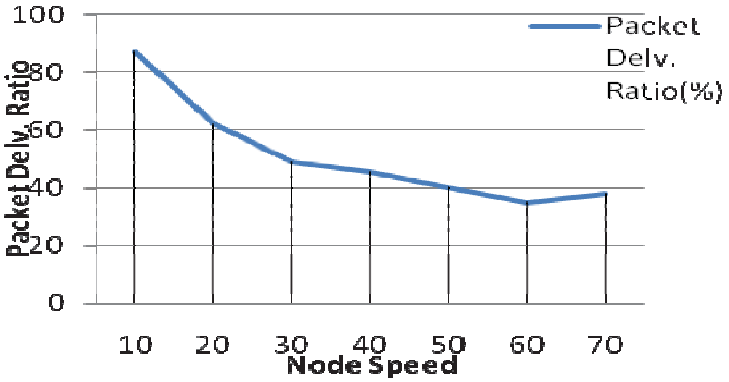

Figure 2. Packet Delivery Ratio with different pause time in X Axis with blackhole malicious node.

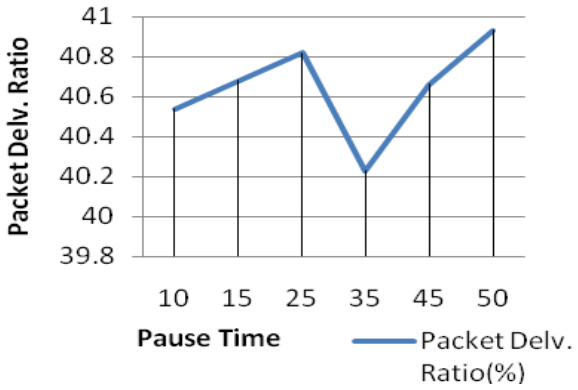

Figure 3. Packet Delivery Ratio for varying node velocity in X Axis with blackhole malicious node.

5.2. Throughput-

It is also another important factor to calculate network performance as it is determined by the average rate of successful message delivery. It is measured as bits per sec. It can be calculated by number of packets delivered per time slot as in the following formulae.

Throughput= (Total number of delivered data packets/Total simulation time)

So, from Figure 4, it is clear that as the number of malicious (blackhole) nodes increased, throughput of the network decreases gradually. Again from Figure 5, when network contains varied number of pause time with fixed number of mobile nodes and fixed number of Blackhole malicious nodes (20%), it is observed that initially throughput of the network decreases with increased number of pause time. But after certain limit, throughput again starts increasing with increase of pause time as higher pause time implies more stable network. Similarly throughput of the network drastically decreases with increase of node velocity up to certain node velocity, after that it slightly increases the throughput and maintain constant throughput for some speed. Figure 6 explain the same.

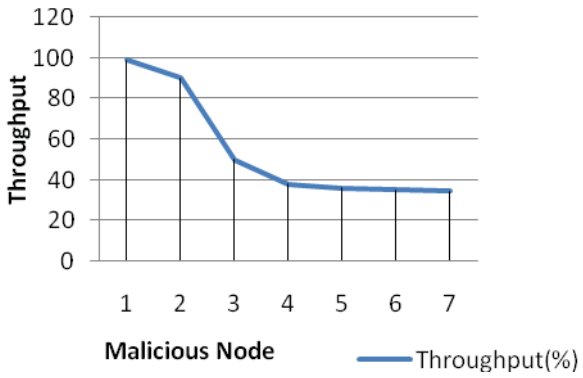

Figure 4. Throughput of the network with increased number of Blackhole malicious nodes

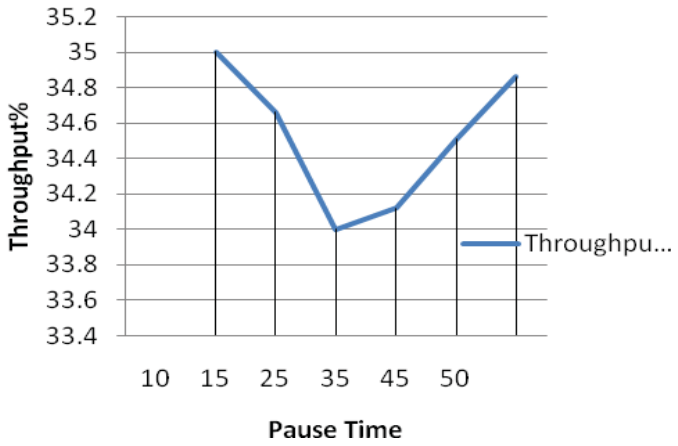

Figure 5. Throughput of the network with varying pause time with fixed number of Blackhole malicious nodes

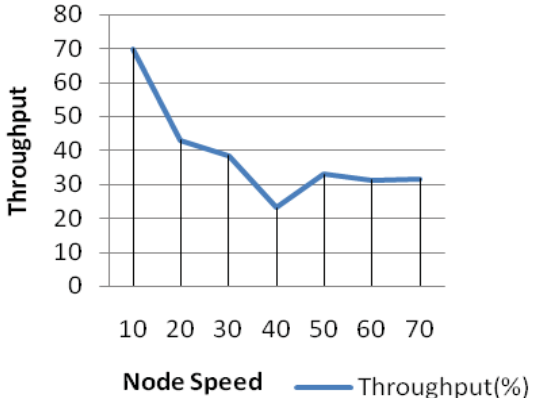

Figure 6. Throughput of the network with varying node velocity with fixed number of Blackhole malicious nodes

5.3. Dropped Data Packet-

Like packet drop ratio, dropped data packet also determines network performance. It can be measured as follows:

Dropped Data Packet(%)=((Number of packets sent - number of packets received) / Total Number of packets sent)*100

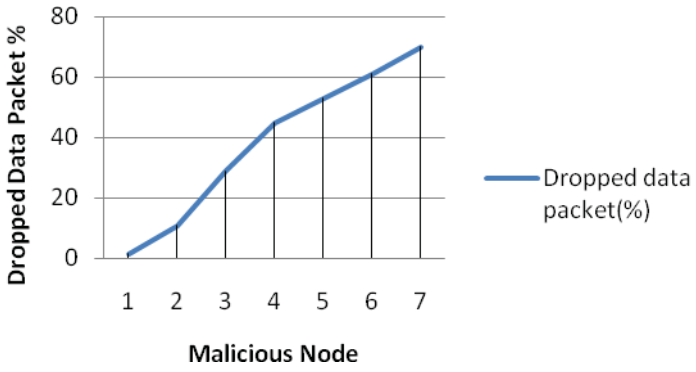

Figure 7. Dropped data packet(%) with increased number of Blackhole malicious node

5.4 Routing Overhead-

This factor is used to measure the bandwidth consumption of a routing protocol. Bandwidth utilization is one of the most important factors as it is limited to a network. So, it shows the amount of bandwidth consumed by the routing message. From the statistics it is observed that routing overhead increases with increased number of malicious nodes in a network due to excess packets generation for malicious activities. Moreover it increases when network topology is changing frequently.

Routing overhead=(Total number of routing packets/Total number of delivered data packets)*100

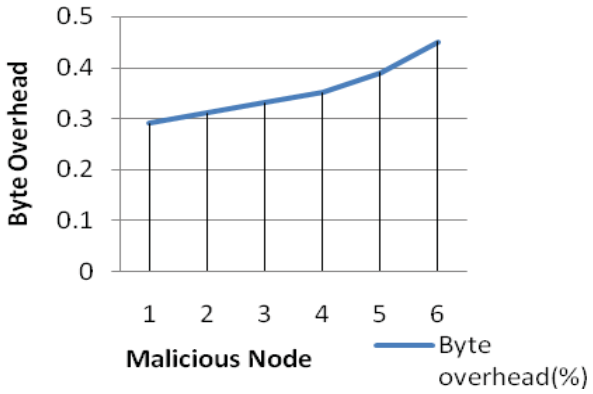

Figure 8. Routing overhead with increased number of Blackhole malicious node

VI. CONCLUSION

From the simulation it is observed that presence of Blackhole node in MANETs, drastically changes the network performance in terms of higher loss in packets as well as generating lower throughput. It is very difficult to apply traditional attack prevention scheme such as cryptographic technique or general authentication technique due to dynamically changing topology with decentralized node distribution. So, in the next paper, a distributed packet drop attack detection methodology, which is based on the co-operation of neighbor nodes of a particular node which is suffered from packet drop attack, will be presented. So, packet drop attack will detect and confirm not only by the node which has been suffering but also it is confirmed by the different neighbors of that node.

REFERENCES

[1] P. Ning and K. Sun, "How to Misuse AODV: A Case Study of Insider Attacks Against Mobile Ad-Hoc Routing Protocols", *Proc.of the 2003 IEEE Workshop on Information Assurance United States Military Academy*, West Point, NY., June 2003.

[2] Sheenu Sharma, Roopam Gupta, "Simulation Study Of Black hole Attack In The Mobile Ad Hoc Networks" *Journal Of Engineering Science And Technology* Vol. 4, No. 2 (2009) 243 – 250 © School Of Engineering, Taylor's University College

[3] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour And Yoshiaki Nemoto, "Detecting Black hole Attack On AODV-Based Mobile Ad Hoc Networks By Dynamic Learning Method" *International Journal Of Network Security*, Vol.5, No.3, PP.338–346, Nov. 2007

[4] Weichao Wang, Bharat Bhargava, Mark Linderman, "Defending Against Collaborative Packet Drop Attacks On Manets"

[5] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon And Kendall Nygard, "Prevention Of Cooperative Black Hole Attack In Wireless Ad Hoc Networks"

[6] N. H. Mistry, D. C. Jinwala And M. A. Zaveri, "MOSAODV: Solution To Secure AODV Against Black hole Attack", *(IJCNS) International Journal Of Computer And Network Security*, Vol. 1, No. 3, December 2009

[7] J. Hubaux, L. Butty´An, And S. Capkun, "The Quest For Security In Mobile Ad Hoc Networks," *Proceedings Of The 2nd ACM International Symposium On Mobile Ad Hoc Networking & Computing*, 2001.

[8] Elmar Gerhards-Padilla, Nils Aschenbruck, Peter Martini Marko Jahnke, Jens T¨Olle, "Detecting Black Hole Attacks In Tactical Manets Using Topology Graphs" *32nd IEEE Conference On Local Computer Networks*

[9] B. Awerbuch, D. Holmer, C. Nita-Rotaru, And H. Rubens, "An On-Demand Secure Routing Protocol Resilient To Byzantine Failures", *Proceedings Of The 3rd ACM Workshop On Wireless Security*, 2002.

[10] J. Deng, R. Han, And S. Mishra, "INSENS: Intrusion-Tolerant Routing In Wireless Sensor Networks", Department Of Computer Science, University Of Colorado, Tech. Rep. CU-CS-939-02, 2002.

[11] Y. Hu, A. Perrig, And D. Johnson, “Ariadne: A Secure On-Demand Routing Protocol For Ad Hoc Networks”, *Proceedings Of The 8th ACM International Conference On Mobile Computing And Networking*, 2002.

[12] P. Papadimitratos And Z. Haas, “Secure Link State Routing For Mobile Ad Hoc Networks”, *Proceedings Of The IEEE Workshop On Security And Assurance In Ad Hoc Networks*, 2003.

[13] Djamel Djenouri, Nadjib Badache, “Struggling Against Selfishness and Black Hole Attacks in MANETs”.

[14] Sukla Banerjee, “Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks“, *Proceedings of the World Congress on Engineering and Computer Science 2008 WCECS 2008*, October 22 - 24, 2008, San Francisco, USA

[15] Akanksha Saini, Harish Kumar, “Effect Of Black Hole Attack On AODV Routing Protocol In MANET”, *ISSN : 2229-4333(Print) | ISSN : 0976-8491(Online)*, IJCSt Vo l. 1, IS Su e 2, deCe m b e r 2010