Black Hole Attack in Mobile Ad Hoc Network – Analysis and Detection

K. Sreelakshmi, Santosh Anand, Somnath Sinha

Abstract--- Mobile Ad Hoc Network (MANET) is susceptible to different type of attacks due to its mobility and other limitation. Black hole attacks are one type of severe active type of attack which occurs in network layer and directly affect the network parameter. This paper analyzes the severity of this attack by implementing the attack using NS2 simulator. Also the available prevention mechanisms and their effectiveness are discussed. This paper also suggests a new approach for detection and prevention of MANET against black hole attack.

Keywords--- MANET, AODV Routing Protocol, Ad hoc network, Black hole.

I. INTRODUCTION

MANET is susceptible to different type of attacks [1]. So in MANET we always give importance to routing protocol which are energy efficient [2] and can protect the network from different types of attack. AODV is widely used routing protocol in MANET. AODV routing protocol is vulnerable to malicious attacks due its flexibility (on demand) in route discovery method. Due to the on-demand path discovery nature of AODV [3], it uses various metrics it its RREQ, RREP and RERR packets. A malicious node easily changes the contents of these packets to launch the attack. The protocol uses sequence number in RREQ and RREP messages for understanding the freshness of the route. A neighbor node always increases the destination sequence number greater than the most recent one before forwarding a RREQ or sending a RREP to the source node. This helps in maintaining an up to date route in case a new route is discovered or some existing routes are broken due to the node mobility or power drainage. A malicious node takes advantage by increasing the destination sequence number to act as a genuine node having newest path towards the destination. These changes are done in the RREP message. Hence by increasing sequence number an attacker easily invalidates the genuine route to the destination and creates a path towards it. Another parameter called Request ID used for recognizing any duplicate route request is also very vulnerable to attack. Request ID is incremented each time a new route request packet (RREQ) is sent by a source node. A malicious node can easily increment the request ID of an existing RREQ packet to show that it is the most up to date RREQ and will be able to initiate a fake route discovery through itself. Another vulnerability of AODV is the IP address of the node which can be easily changed by a malicious node which can use a genuine node's IP or any restricted IP address not in used. Moreover it can also alter a RERR message by replacing the IP address of the broken or unreachable node by an active node's IP address or some other IP address which is reachable through itself. The vulnerabilities of AODV towards Black hole attack leads to packet drop or network congestion which are to be prevented to guarantee the protocol's performance under such scenario. In the next section we discuss major prevention mechanisms of Black hole attack. The remaining paper is structured as follows. Section 2 elaborates the related research work done the detection and prevention of black hole attacks. Section 3 represents network model and assumption. The methodology and algorithms are discussed in section 4. And the last section highlights the conclusion and future work.

II. BACKGROUND

Numerous techniques are proposed in the literature of Black hole attack detection and prevention. Some are based on redundant route and sequence number comparison, others rely on neighborhood based detection techniques. However the crucial aspect of these techniques are the high network overhead, greater end to end delay (in dense network), high false positive and exposure to cooperative black hole attacker. Our aim in this study is to represent the most common detection and the prevention schemes for black hole attack which can be categorized into four different forms.

DPRAODV Scheme

In Detection, prevention and reactive AODV scheme mainly the sequence number in the RREP packet is checked against a threshold value in routing table. The threshold value is the calculated average of the sequence numbers in the routing table for RREP packet over a specific time interval.

If the RREP sequence number is higher than the threshold value the node is considered as malicious. This method limits the increase in sequence no by periodically calculating the threshold value over time. Hence any abnormal or unexpected increase in sequence number is encountered easily.

A false ALARM message is generated for this node to the neighbor and other nodes in the network so that any further communication with the malicious node is stopped. This method has shown increased packet delivery ratio but at the same time the overhead and end-to-end delay is also increased than AODV[4]

Manuscript received February 01, 2012. (Fill up the Details)

K. Sreelakshmi, Department of Computer Science, Amrita School of Arts and Sciences, Mysuru. Amrita Vishwa Vidyapeetham, Karnataka, India. (e-mail: sreelakshmicdas1996@gmail.com)

Santosh Anand, Department of Computer Science, Amrita School of Arts and Sciences, Mysuru. Amrita Vishwa Vidyapeetham, Karnataka, India. (e-mail: santoshanand.jha@gmail.com)

Somnath Sinha, Department of Computer Science, Amrita School of Arts and Sciences, Mysuru. Amrita Vishwa Vidyapeetham, Karnataka, India. (e-mail: ssin.mca@gmail.com)

Sequence Number Comparison

With this method sequence number between the route reply of the next neighbor of the source and the sequence number generated by it are compared. If the difference is too high an abnormality is detected and the intermediate node is considered as malicious. Here two different tables one for route request and another for route reply is maintained during communication. Each time a new packet is reached the sequence number is updated in these tables according to the packet type (RREQ/RREP). It is simple and effective way [7] of detecting the malicious node and preventing the network from this attack. However a careful listener of the channel can achieve the last sequence number in the table and remains undetected as the channel is open. [6]

ERDA (Enhancement Route Discovery for AODV) Scheme

In this method no modification is done in the AODV routing protocol. Rather a few parameters are added in the routing table which is specifically 1) *rrep_table*to track RREP [7] packet, 2) *mali_list*to trace any malicious or suspected node entry and 3) *rt_upd* table to control the routing table update. The source node before transmitting packets checks the sequence number and updates the malicious list. It can be Implemented very simple way by removing false entry and replace with the new one. This method fails when attackers send fake reply packets also [3].

Intrusion Detection System (IDS)

This technique is either network based or host based. In this technique some nodes are considered as IDS nodes which are selected for observing the RREQ and RREP packets in their transmission range. Two tables one for RREQ packets and another for calculating suspicious values for a node are maintained in the vicinity of the IDS node. A node which does not broadcast any RREQ message but sends RREP is considered as suspicious and a value is added for this node in the second table. This node will be treated as block and this information is sent to all other neighbors in the network. If any RREP with the same node id is received the packet is discarded. This method uses a pre-collected set to compare the behaviorof network or host for detecting the attacks. The major drawback of this method to detect collaborative black hole attack [8].

The above Black hole detection and prevention schemes are easy to implement as they require minimum overhead and increases the true positive rate than the other existing technique.

In the next section we have designed a single black hole attack model in which the attacker increases the sequence number in the RREP packet to launch the attack. This model is a representation of realistic black hole attack scenario where there are up to 8 single black hole nodes launching attacks in a network of 200 nodes randomly spaced. Since the target of the black hole attacker is to drop data packets coming through it we have shown the packet delivery ratio and throughput variation in the network under the attack also we varied the node density to show the attack intensity in the network.

III. NS2 IMPLEMENTATION

NS2 is good option for testing the effect of black hole attack in MANET. Here we use a scenario (figure 1) by creating a black hole and tested it in AODV protocol. The simulator environment is described in table1. Malicious nodes try to attract the data packets to pass through it by claiming fresh route through it and subsequently drop all the data packets, hence decrease the network performance. We have done some changes in aodv.cc file to implement the attack.

Table1: Simulation Parameters

Parameters	Values
NS2	Versions 2.35
Simulation area	1000x500 (sq.m)
Simulation time	150s
Mac Layer	802.11
Routing protocol	AODV
No of Nodes	200
Malicious Nodes	1,2,3,4,5,6,7,8,

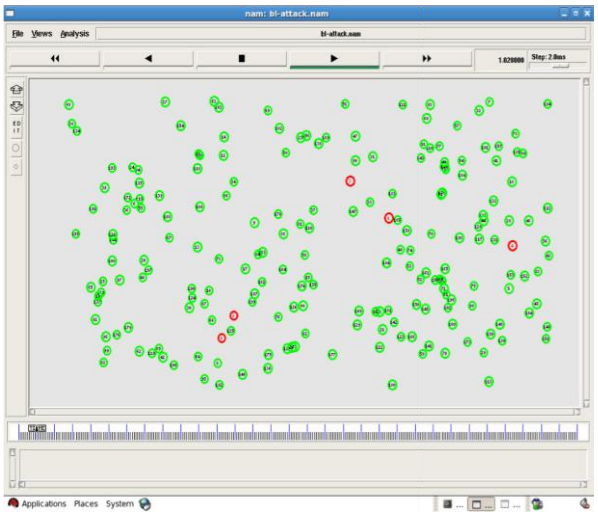

Figure 1: Simulation scenario in NS2 with 200 nodes and 5 malicious nodes with random distribution

IV. EXPERIMENTAL DATA AND RESULTS

In this paper black attack is implanted and network parameters e.g. throughput and packet delivery fractions are studied with the MANET having 200 nodes. From figure 2 and figure 3 we see the variation of throughput and PDF when no of attackers varies. We consider random arrangement of nodes and the attackers while experimenting.

With this configuration the network is almost stopped for transmitting packets having number of attackers more than 7.

In the second methodology we fixed the number of attackers as five and vary the number of legitimate nodes). From figure 4 and figure 5 it is clear that when the number of nodes is 100 then the network is almost stopped transmitting. The results are depicted using xgraph.

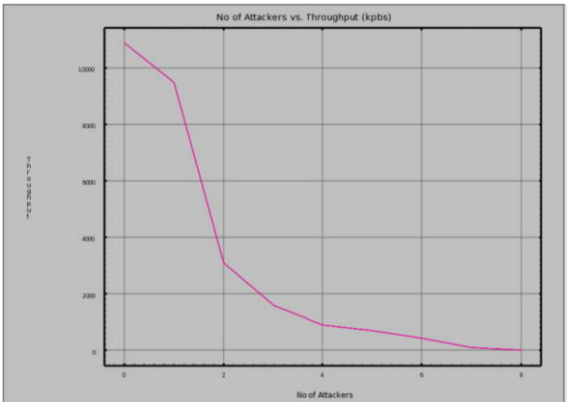

Figure 2: No. of attackers vs. Throughput (kbps)

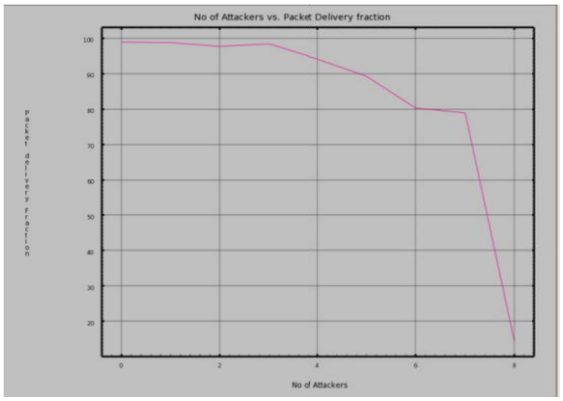

Figure 3: No. of attackers vs. Packet delivery fraction

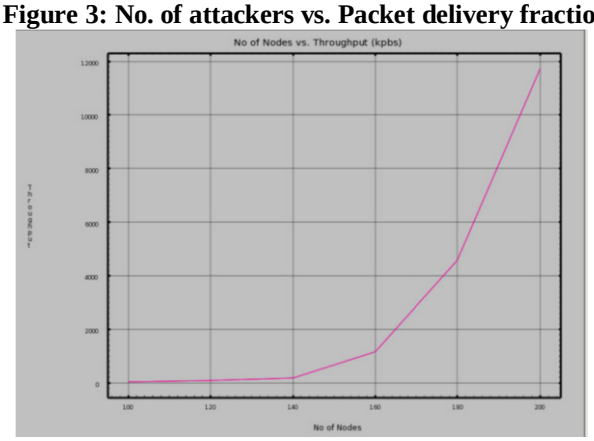

Figure 4: No. of nodes vs. Throughput (kbps)

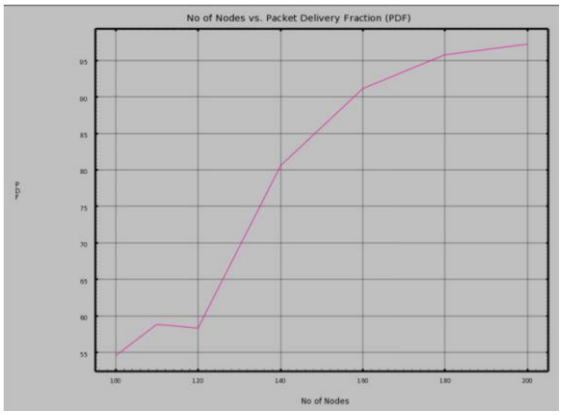

Figure 5: No. of nodes vs. Packet delivery fraction

V. PROPOSED METHOD

This paper proposes a two phase computation for detection and prevention of black hole attack. The black hole attack is based on relaying the higher sequence number to show the shortest path through the malicious nodes and subsequently dropping of packets. In this two phase computations a behavior trust based model is considered where any number of nodes having packet dropped more than average packet drop per node in the network suspected as malicious nodes. The nodes having packet drop more than a threshold value is completely taken as black hole. Every source node maintains a trusted list to identify the legitimate node. However trusted nodes can also be made on the basis of RREQ and RREP message passing. This trust based concept will reduce the computational activity to identify the attackers in the second phase we prefer the sequence comparison method as it is more efficient and easy to implement. During communication with the legitimate nodes every nodes judge the sequence number in the reply packet. If the variation between the source and destination sequence number is more than a threshold value the node is to be considered as attacker and source has to find out another route from communication.

VI. CONCLUSION

In the current study we have discussed the weakness of AODV routing protocol and the possible vulnerabilities of black hole attack. We illustrate some simple and efficient detection and prevention techniques which require low overhead but high true positive value. One important observation to be mentioned here is that all these techniques are well working under single black hole attack. For cooperative black hole attack more robust and complex detection schemes will require which are beyond the scope of the paper. We have shown through simulation the attack scenario and the effect of the attack on throughput and packet delivery fraction. Lastly we have proposed detection techniques for the single black hole attack using trust value of the nodes.

REFERENCES

1. Acharya A. A., K. M. Arpitha K.M., Santhosh Kumar B. J., " An intrusion detection system against UDP flood attack and ping of death attack (DDOS) in MANET", International Journal of Engineering and Technology (IJET), 2016, 8(2).
2. S. Anand, Akarsha, R. R., "A Protocol for the Effective Utilization of Energy in Wireless Sensor Network", International Journal of Engineering & Technology, 2018, 7(3.3), 93-98.
3. M. Y. Su, "Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems", Computer Communications, 2011, 34(1), 107-117.
4. P. N. Raj, P. B. Swadas, "Dpraodv: A dyanamic learning system against blackhole attack in aodv based manet", 2009, arXiv preprint, arXiv:0909.2371.
5. V. Khandelwal, D. Goyal, "Blackhole attack and detection method for AODV routing protocol in

MANETs", International Journal of Advanced Research in Computer Engineering & Technology, 2013, 2(4).

6. F. H. Tseng, L.D. Chou, H. C. Chao, "A survey of black hole attacks in wireless mobile ad hoc networks", Humancentric Computing and Information Sciences,2011, 1(1), 4.
7. B. Sun, Y. Guan, J. Chen, U.W. Pooch, "Detecting black-hole attack in mobile ad hoc networks", presented at 5th European Personal Mobile Communications Conference, Glasgow, United Kingdom, 22-25 April 2003.
8. N.H. Mistry, D.C. Jinwala, M.A. Zaveri, "MOSAODV: solution to secure AODV against blackhole attack", IJCNS) International Journal of Computer and Network Security, 2009, 1(3), 42-45.