I. J. Computer Network and Information Security, 2013, 12, 35-44
Published Online October 2013 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2013.12.05

Performance Evaluation of AODV under Blackhole Attack

Tarunpreet Bhatia and A.K. Verma
Department of Computer Science Engineering, Thapar University, Patiala - 147004, India
tarunpreetbhatia@gmail.com, akverma@thapar.edu

***Abstract* —** Mobile Adhoc NETwork (MANET) consists of mobile nodes that can move freely and route packets without aid of centralized infrastructure. Dynamic changing topology, limited battery power and lack of centralized trusted authority make it vulnerable to several attacks and lot of research is being carried out in the field of security by discovering attacks, evaluating the damage caused to the network and developing solutions to combat such attacks. This paper simulates one of the most malicious behaviors known as blackhole attack. The blackhole node creates forged reply, advertising valid and fresh route to destination and thereafter drops data packets maliciously. The analysis guides us to the various performance parameters such as throughput, packet delivery fraction, normalized routing load and number of dropped packets evaluated over different scenarios.

***Index Terms* —** MANET, AODV, Blackhole Attack, Security

I. Introduction

Wireless arena has been experiencing an exponential growth in the past few years. Wireless networking refers to the use of electromagnetic signals such as infrared or radio frequency signals to share information and resources among mobile devices. Wireless networks offers convenience in terms of simplicity, mobility and flexibility. It does not have constraint of physical cables. Wireless communication is an ever-developing field and the future holds many possibilities in this area. Future devices can be developed to support communication with higher data rates and more security. Based on architecture, wireless networks are classified as:

- Infrastructured network: Mobile nodes are connected to base station and communication among nodes take place via base stations acting as bridges. Eg WLAN, cellular network
- Adhoc network: Mobile nodes join to form a temporary network without aid of any established infrastructure. Each node shared the responsibility of route discovery and maintenance. The nodes within transmission range of a particular node can directly communicate with each other and multiple hops are used to route packets to nodes outside its transmission range. Eg MANET.

Mobile ad-hoc routing protocols are divided into following three categories [1]

- Proactive protocols in which each node has to maintain up-to-date information about all other nodes within an ad hoc network in its routing table. Route is always available but overhead is more.
- Reactive protocols in which routes are created on demand. Whenever a node wants to send data, it initiates route discovery.
- Hybrid routing protocols which are combination of above two. Within a small domain proactive is used and among domains reactive is used.

The attacks targeting MANET routing protocols are classified as active and passive attacks [2] (refer Figure 1). Passive attack refers to eavesdropping attack in which attacker just snoops the network without disrupting it. Active attacks are the attacks in which normal functioning of the network is disrupted by fabricating and modifying messages, intentionally dropping selective or all the packets and replaying attacks. Active attacks can either be caused by an external advisory or an internal compromised node. Simulation and performance evaluation of such attacks is necessary in order to design defensive solution against these attacks. The objective of this paper is to simulate one of the most vulnerable blackhole attack in wireless ad-hoc networks and evaluate its damage in the network. AODV protocol is used for evaluation.

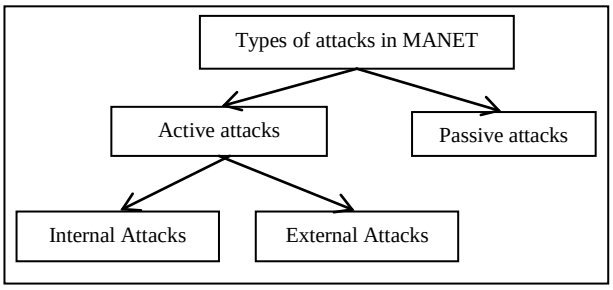

Figure 1: Classification of attacks

The rest of the paper is organized as follows: Section 2 introduces about the related work. Section 3 revisits AODV protocol. Section 3 focuses on blackhole attack on AODV. Section 4 deals with simulation environment. Section 5 presents simulation results and Section 6 summarizes the paper and discusses future scope.

II. Related Work

When MANET routing protocols were proposed, security issues were not given due consideration. Lately, researchers have highlighted the vulnerabilities and attacks that can be mounted against ad hoc protocols and solutions devised to combat them [3-5]. In [6], Ariadne, a symmetric key encryption scheme was proposed for DSR [7] that uses one way HMAC key chain immune to impersonation and fabrication attacks. In [8] ARAN for AODV based on asymmetric key cryptography was proposed. It required online trusted certification authority so computationally expensive scheme. Further, SEAD [9] for proactive protocols and SAODV [10] for AODV have been proposed. Both used one way hash functions for ensuring authentication and integrity of the message. Researchers in [11] surveyed strength and weakness of various secure routing protocols. But most of the above mentioned protocols guard against external attacks only.

However, internal selfish or malicious nodes could still have severe impact on network performance. Nguyen et. al. [12] has shown the impact of several attacks on the multicast MANET protocols. Blackhole attack is an insider attack in which selfish node fabricates protocol message fields so that all the traffic is redirected to it and it does not forward data packets afterwards [13]. Still a lot of work is required to analyze blackhole attack in MANET from all perspectives so that secure solution can be devised. In this paper, performance of AODV with and without blackhole attack is evaluated on the basis of various metrics like throughput, packet delivery ratio, normalized routing load and data packet loss with varying speed, number of nodes, number of malicious nodes etc.

III. Overview of AODV

AODV is an Adhoc On-demand Distance Vector routing protocol [14, 15] used for finding a path to a destination in an ad-hoc network. It is categorized as reactive protocol which is invoked when a node wants to transmit data. Each node maintains routing table and refers it to determine next hop to reach the destination. The protocol consists of two phases:

- Route Discovery: A node that wishes to transmit data to other node and is unable to find route in its routing table initiates route discovery phase.
- Route Maintenance: It can be initiated by source node if it moves to a new location or by an intermediate node or destination node if they move. After receiving messages, nodes update their routing tables and forward messages to source node.

It allows the mobile nodes to exchange messages with their neighbors in order to communicate with nodes that are not directly connected. The basic message set consists of – HELLO messages, Route Request (RREQ), Route Reply (RREP) and Route Error (RERR). HELLO messages are sent for link status monitoring to know whether other node is in the communication range of it or not. RERR messages are broadcasted for broken links.

A RREQ message is broadcasted by a node that wishes to send some data to a destination node to its neighbors. RREQ message contains several fields like source and destination IP addresses, lifetime, sequence number for the destination node to timestamp routing table entries and unique ID for rejecting duplicate RREQs. RREQs keep getting rebroadcasted until their lifespan is up. Each node maintains a routing table having entries keyed by destination nodes. In addition to destination node IP address, it contains next hop node, sequence number and hop count to reach that destination. As RREQs propagate through the network, intermediate nodes after updating their tables forward RREQs to their neighborhood. If any intermediate node receiving RREQ has a route to the destination, it compares sequence number to determine whether this route is fresh or not. Destination route with sequence number as great as contained in RREQ is considered valid.

A node can generate a reply if it is a destination node or an intermediate node having unexpired route to destination node. Intermediate nodes update their routing tables in the direction of source node while RREP propagates back to the source node. Destination node unicasts RREP along reverse path created by intermediate nodes while forwarding RREQ. In RREP destination node sets hop count to zero and enter its latest known sequence number. Intermediate node forwards RREP along reverse path after incrementing hop count by 1 and creating next-hop entry for destination in their routing table.

Consider Figure 2 in which node 1 being source node wishes to send data to destination node 3 so it broadcasts RREQ to node 4 and 2 setting RREQ id 10, its source IP to node 1 and sequence number to 100. Since it does not have prior information of destination sequence number it sets it to zero. Node 2 and 4 on receiving RREQ have two choices either to broadcast RREQ to their neighboring node 3 and 5 respectively after making a reverse path entry to node 1 in their routing table and incrementing hop count by 1 or to reply back if they already have route to destination in their table.

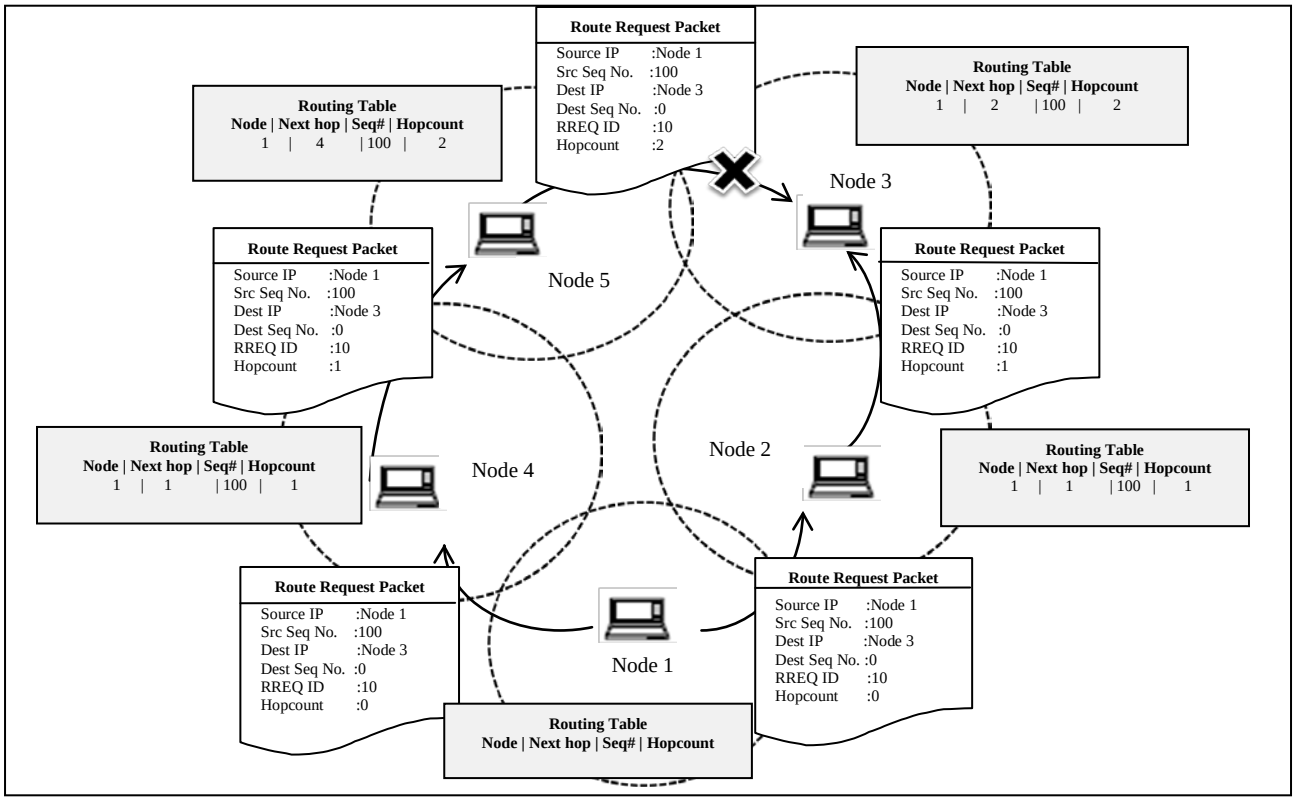

Figure 2: Propagation of RREQ in AODV

Node 3 being destination node formulates RREP and unicasts it to node 2 by setting hop count to zero, lifetime to 3 and destination sequence number to 140. This is illustrated in Figure 3. Meanwhile node 3 receives duplicated RREQ from node 5 and discards it. Node 2 propagates RREP incrementing hopcount by 1. It also makes reverse path entry to node 3 in its routing table. As RREP reaches source node, it will further send all the data packets through the established route. RREP messages also include destination sequence number field. Nodes update their routing table when they receive RREP having latest destination sequence number. In Figure 4 node 2 updates entry keyed by destination 3 on receiving RREP from node 3 and sets sequence number to 160. Similarly node 1 removes stale entry updating sequence number from 140 to 160.

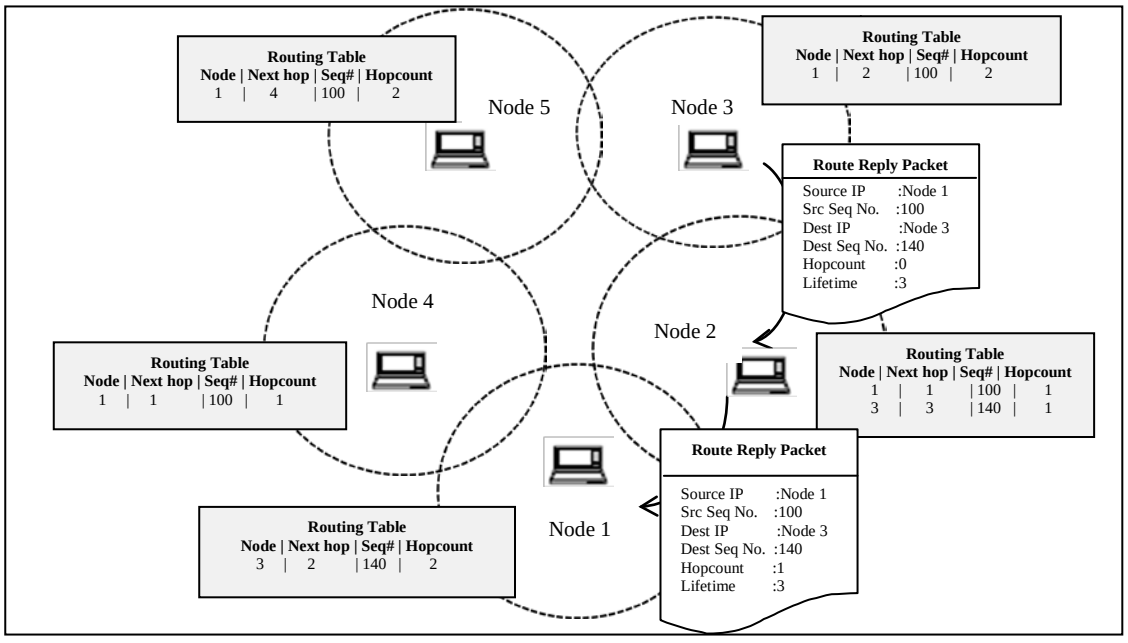

Figure 3: Propagation of RREP in AODV

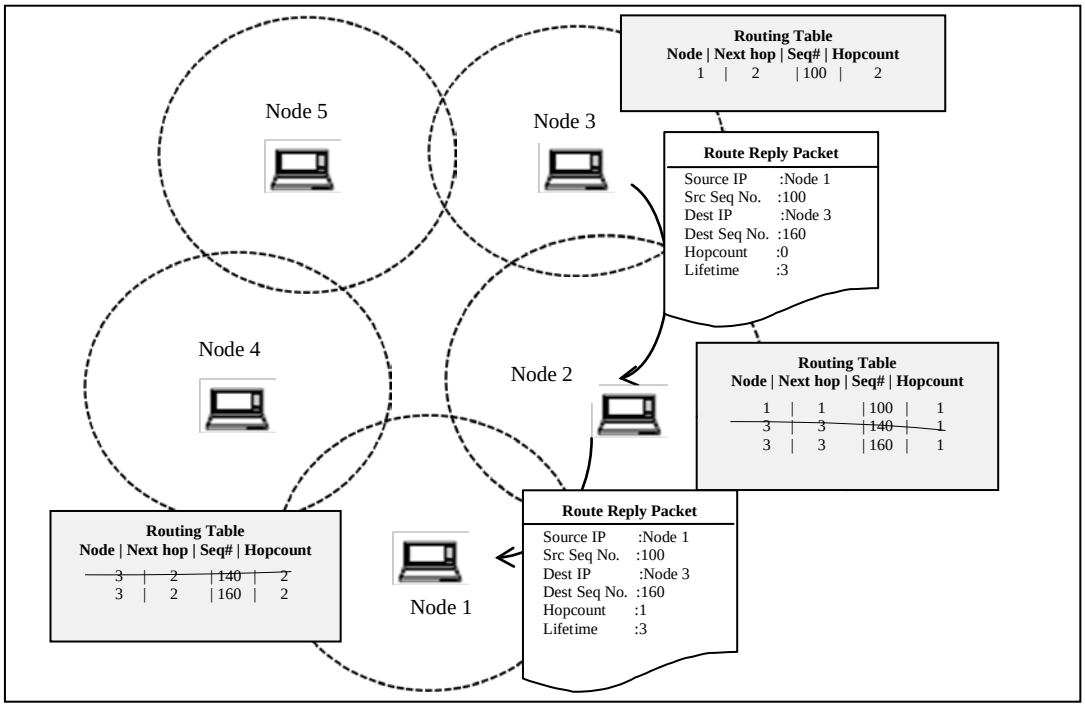

Figure 4: Sequence Number Updation

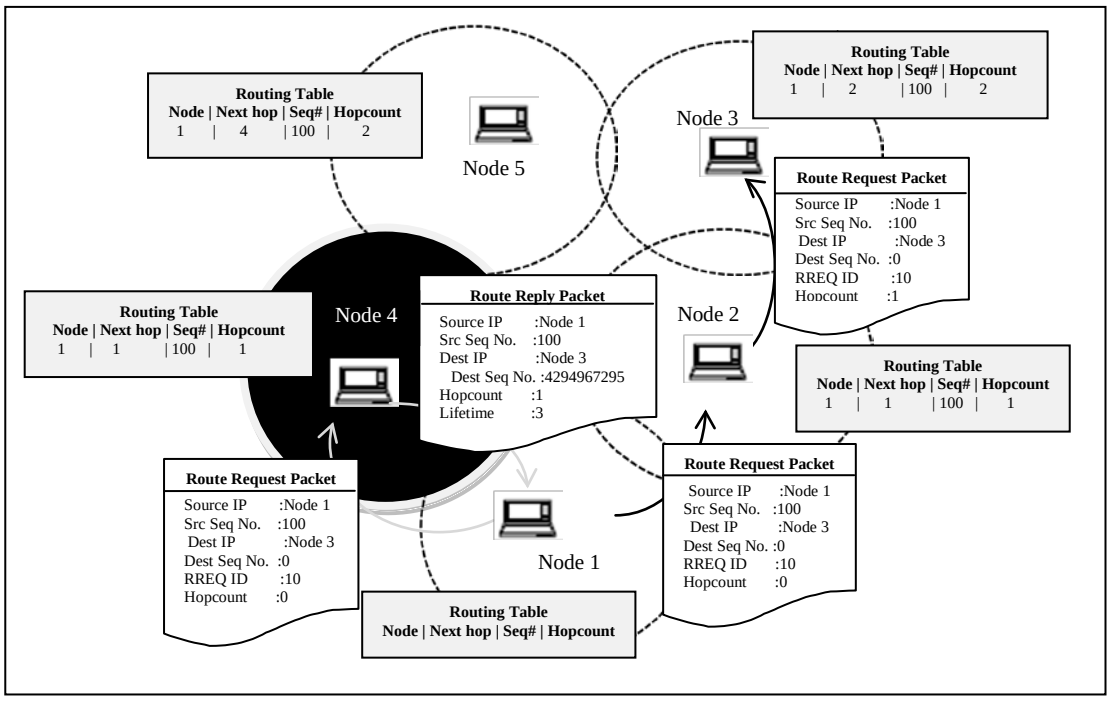

Figure 5: Blackhole Attack in AODV

IV. Blackhole Attack

It is one of the most vulnerable attacks against AODV routing protocol in which malicious node falsely replies for received route requests without having active or fresh route to specified destination and drops all the receiving data packets afterwards. In order to have shortest route, blackhole node creates forged packet by modifying either hop count or sequence number.

The malicious node overhears the communication of wireless channel of which it is a part and observes the sequence number of the nodes [13]. After that it creates RREP setting sequence number field to the highest observed sequence number till now, fooling the source node. It can also set hop count to 1 signifying that the route through blackhole node is the shortest. After introducing itself as an intermediate node in the route, it silently drops all the data packets. In Figure 5, node 4 being blackhole node replies immediately to node 1 setting hopcount 1 and destination sequence number to a

maximum value 4294967295. As this forged reply reaches source node it forwards data packets along this node which drops these packets instead of forwarding them.

V. Simulation Environment

NS-2 simulator [16, 17] is used for the performance evaluation of blackhole attack on AODV. Network traffic is generated by CBR (Constant Bit Rate) connections between wireless nodes [18]. Each CBR source sends packets at the rate of 0.25 i.e. 4 packets per second and each packet is of constant size 512 bytes. CBR is chosen since it is connectionless and unreliable connection. The source node continues to send UDP packets without waiting for acknowledgments and sent and received packets can be counted separately since UDP connection is not lost during the simulation. Each node maintains a FIFO queue of maximum size 50 based on drop-tail mechanism. Mobile nodes move inside a square area of 750m X 750m with Random Waypoint Model. The Random Waypoint Mobility Model is based on pause times between any change in direction and/or speed [19]. A mobile node stays in one location for a certain amount of time equal to pause time. After expiration of this time, the mobile node randomly chooses any destination within the simulation area and a speed uniformly distributed between minspeed and maxspeed. Simulation is done for 500 sec and maximum connections allowed are 30. Other parameters are listed in Table I.

TABLE I. Varying Simulation Parameters

Parameter	Scenario 1	Scenario 2	Scenario 3	Scenario 4
Pause Time (sec)	50, 100, 150, 200	2	2	5
Number of nodes	20	20, 40, 60, 80	20	25
Speed (m/s)	20	10	5, 10, 20, 30	20
Number of malicious nodes	1	1	1	1, 5, 10, 15, 20

A. Modified AODV Protocol in NS to Simulate Black Hole Behavior

In [20] implementation of a New Manet Unicast Routing Protocol in NS-2 is described. NS-2 is used as simulator in which AODV routing protocol is modified to implement Blackhole attack. When a packet is received by "recv" function of aodv.cc, it processes the packet based on its type. If it is AODV packet, it sends to "recv_AODV" function else it further checks if it is data packet originated by me then handle it in normal way otherwise it is forwarded packet so if blackhole attack has to be implemented node will maliciously drop it else sends it to destination address. Now "recv_AODV" will have AODV management packet. It checks based on its type RREQ, RREP or RERR and sends to appropriate function. RREQ packet is sent to "recv_Req" function which checks if this request is previously seen, it is dropped, otherwise if blachole attack then sends fake reply; if not then resolves the request and sends reply if it has route, otherwise forwards it. The other AODV packets are handled in normal way. In order to implement blackhole attack changes have to be made in RREQ function because blackhole behavior is carried out when the malicious node receives RREQ packet. It immediately sends forged RREP packet as if it has fresh enough path to the destination. Malicious node tries to deceive other nodes sending such RREP packet.

B. Performance Metrics

Performance Metrics are quantitative measures that can be used to evaluate any MANET routing protocol. The metrics that compare the performance of normal AODV and AODV under blackhole attack are as follows:

Throughput represents the amount of data received by the destination nodes in some period of time [21].

$$Average\ Throughput = \frac{Number\ of\ bytes\ received \times 8}{Simulation\ Time \times 1000} kbps$$

Packet delivery fraction (PDF) can be measured as the ratio of the data packets delivered to the destinations to those generated by the CBR sources. The PDF depicts how well a routing protocol can delivers packets from source to destination. The higher values give better results. This metric characterizes both the completeness and correctness of the routing protocol also reliability of routing protocol by giving its effectiveness [22].

$$PDF\ (\%) = \frac{Number\ of\ packets\ received}{Number\ of\ packets\ sent} \times 100$$

Normalize Routing Load (NRL) is the number of routing packets that are transmitted per delivery data packets [22].

$$NRL = \frac{Number\ of\ routing\ packets}{Number\ of\ packets\ received} \times 100$$

Dropped Packets refer to the number of packets sent by the source node that failed to reach the destination node. The routers might fail to deliver or drop some data packets after their arrival when their buffers are already full.

$$Dropped\ Packets = Sent\ Packets - \mathrm{Re}ceived\ Packets$$

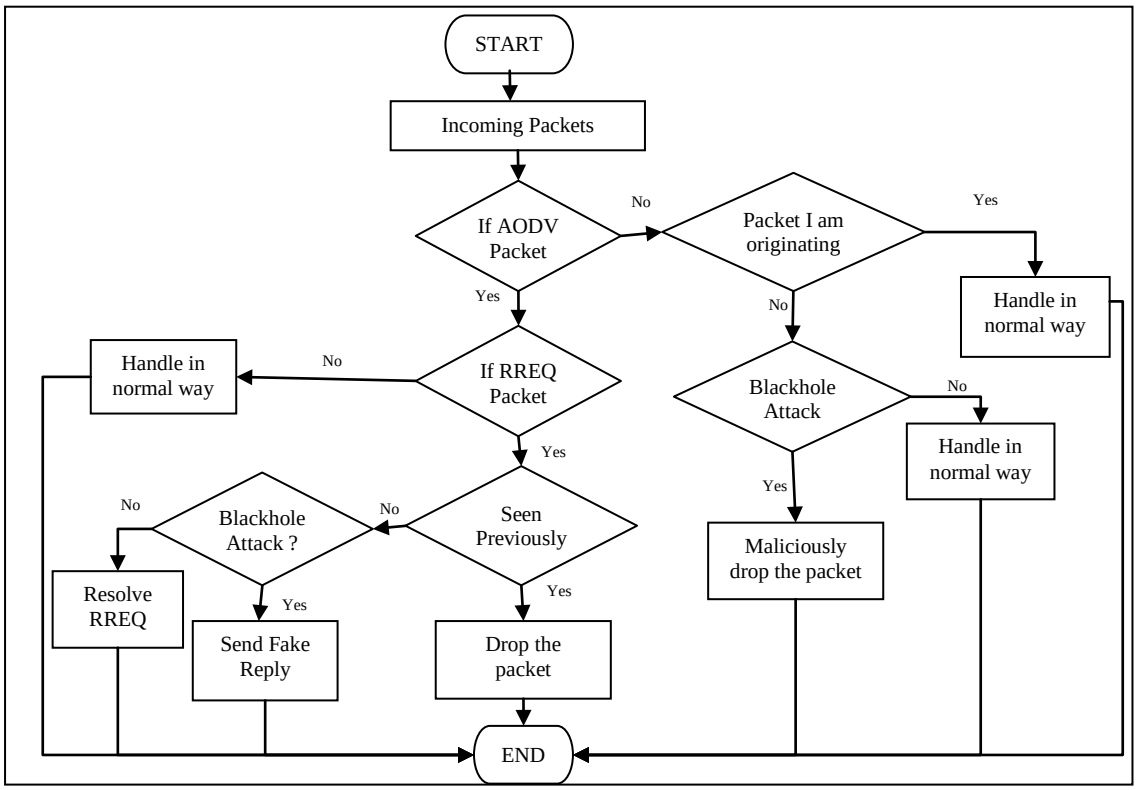

Figure 6: Simulation Overview

VI. Simulation Results And Analysis

The simulation is done for 4 different scenarios with varying number of nodes, speed, number of malicious nodes and pause time. For each set of parameters simulation is repeated 10 times and average results are taken. Packet delivery fraction, routing load, dropped packets, and throughput were calculated for AODV and AODV under blackhole attack. The results in the form of graph are as follows:

A. Varying the pause time

Pause time is the time for which mobile nodes wait at a destination before moving to other destination. Low pause time signifies high mobility as the node will have to wait for lesser time duration. Keeping all other parameters constant, pause time is varied in steps of 50 to observe the behavior of performance metrics. Figure 7 shows the effect of pause time on the throughput. There is huge difference between the throughput for AODV and Blackhole AODV. As pause time increases from 100 sec to 250 sec there is slight increase in throughput but after 200 sec it starts decreasing because pause time is related with mobility. High pause time means less mobility and more stable network but when pause time is equal to simulation time then the node will not move and throughput decreases. PDF also behaves in the same way as throughput as it is the ratio of packets received and packets sent. In blackhole attack malicious nodes absorb the data packets so number of packets actually delivered decreases so PDF drops from 80% to 25% with blackhole attack on AODV (refer Figure 8).

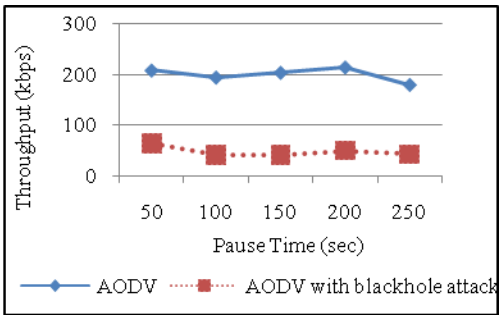

Figure 7: Throughput vs Pause Time

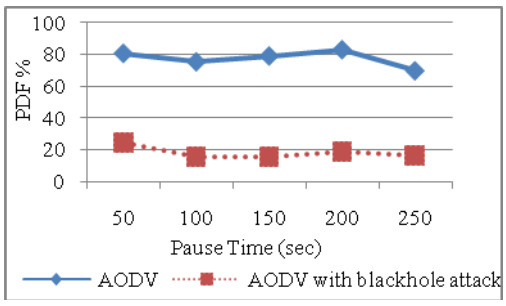

Figure 8: PDF vs Pause Time

NRL signifies routing overhead so it is more for AODV under blackhole attack as packets are dropped so re-route discovery messages are send and also retransmissions occur. As pause time increases network becomes stable so routing load decreases. Less pause time means more mobility. Whenever node changes its direction or speed, route maintenance occurs. For non malicious nodes in AODV, NRL is 0.87 and it increases

to thrice its value with AODV under blackhole attack (refer Figure 9). More number of packets is dropped in case of AODV under blackhole attack. There is little effect of pause time on number of dropped packets so it remains almost constant (refer Figure 10).

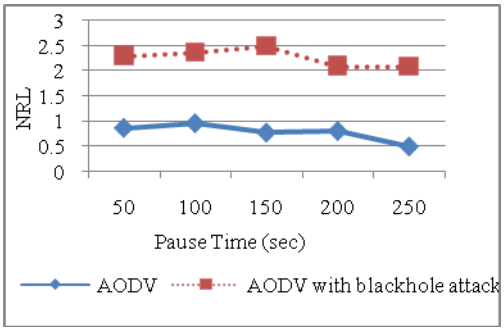

Figure 9: NRL vs Pause Time

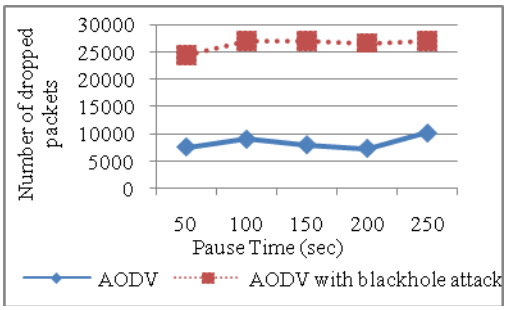

Figure 10: Dropped Packets vs Pause Time

B. *Varying the number of nodes*

Number of nodes can be another varying parameter that plays an important role in evaluating network performance. Our simulations show various performance parameters versus number of nodes to account for system scalability. There is huge difference between the throughput for AODV and Blackhole AODV. Throughput of AODV is not affected much by the change in number of nodes (refer Figure 11). PDF drops from 88% to 22% as compared to AODV without attack. Both the curves behave in the same way that is with increase in number of nodes in the network congestion in the network increases so packets are dropped due to the collisions (refer Figure 12).

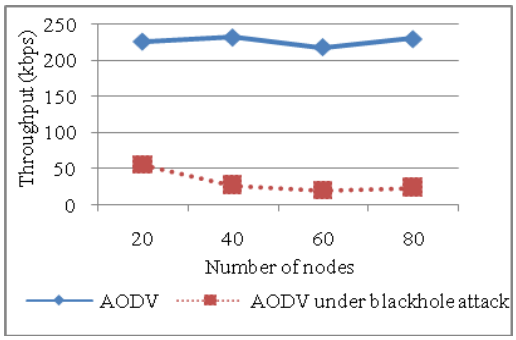

Figure 11: Throughput vs Number of nodes

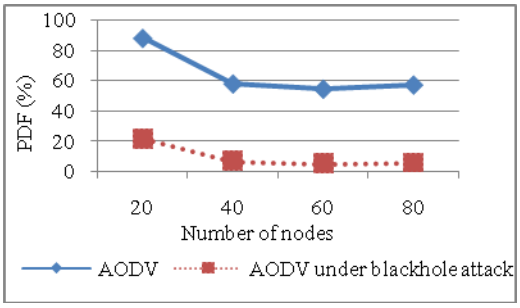

Figure 12: PDF vs Number of nodes

NRL for AODV under blackhole attack is more than normal AODV as more packets are dropped so more retransmissions occur. Further in Figure 13, both curves behave same that is NRL increases with increase in number of nodes as more routing information is exchanged but curve for AODV under attack is always above the normal AODV. It depicts number of dropped packets increased by 377.9% with malicious nodes in the network as compared to AODV without attack in Figure 14. With increase in number of nodes in the network, congestion increases so more packets are dropped due to the collisions.

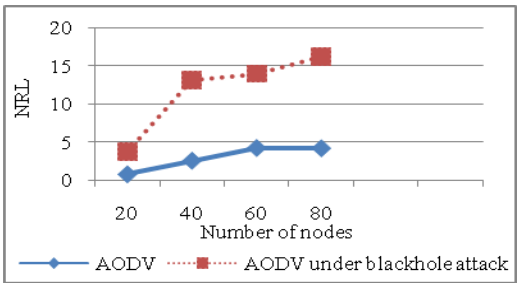

Figure 13: NRL vs Number of nodes

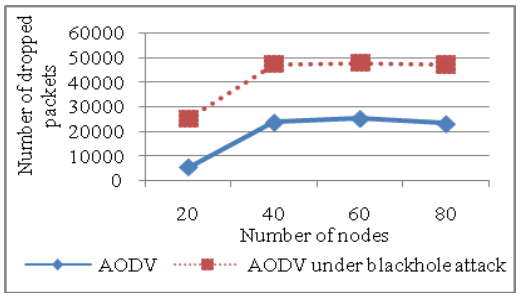

Figure 14: Dropped Packets vs Number of nodes

C. *Varying the speed of nodes*

The effect of speed variations for throughput for normal AODV and AODV under blackhole attack has been analyzed. It is clear from the below graphs that the blackhole attack deteriorates the network throughput from 220 kbps to 77 kbps with attack (refer Figure 15). It depicts that initially there is slight increase in throughput as speed increases because mobile nodes while moving enter into the transmission range of other nodes so packets may be delivered fast but increasing node speed beyond 20 m/s results in decreased throughput. The

reason is that as speed increases more re-route discovery messages are exchanged among nodes and collision in the network increases. PDF for AODV with attack reduces by 65% as compared to AODV without attack (refer Figure 16). PDF increases initially with increase in speed but after 20 m/s it started decreasing due to congestion in the network.

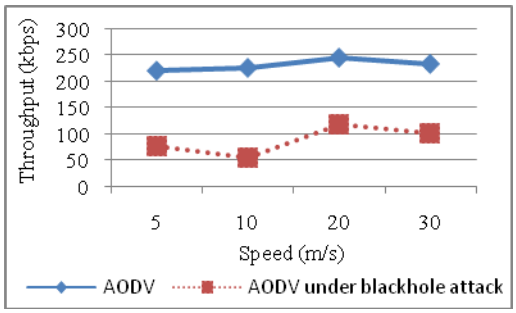

Figure 15: Throughput vs Speed Graph

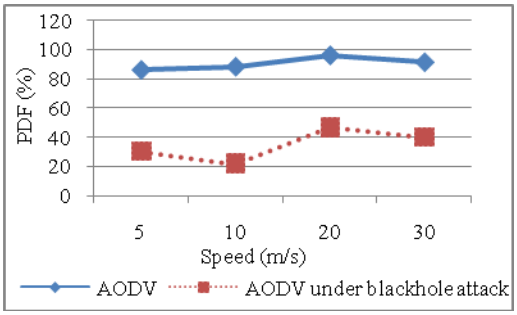

Figure 16: PDF vs Speed

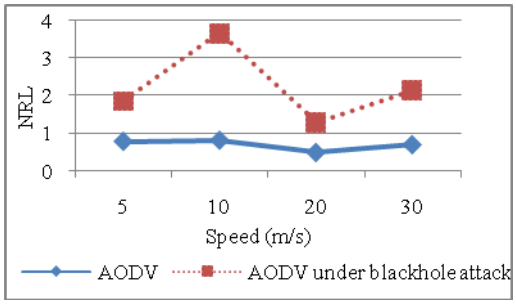

Figure 17: NRL vs Speed

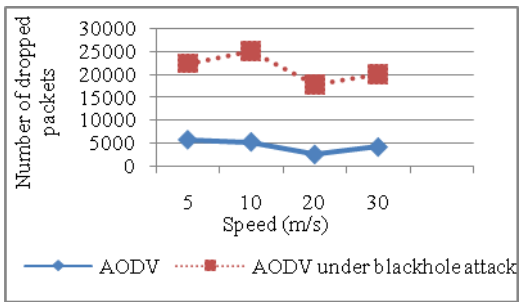

Figure 18: Dropped Packets vs Speed

As depicted in Figure 17, NRL for AODV under blackhole attack is more as packets are dropped so more retransmissions occur. Further it is clear from the Figure 18 that packets dropped are 291.4 % more for AODV under attack than AODV without attack. Increasing speed beyond 20 m/s causes more packets to drop because of collisions in the network.

D. Varying the number of malicious nodes

The effect of varying number of malicious nodes on the throughput for normal AODV and AODV under blackhole attack is analyzed. There is huge difference in throughput of AODV without attack and with blackhole attack (refer Figure 19). While evaluating throughput for normal AODV malicious nodes are not considered so throughput remains constant 237.22 kbps. In case of blackhole AODV as number of malicious nodes increase throughput decreases. It depicts throughput with presence of 4% to 80% malicious nodes in the network. Packet delivery fraction decreases by 77% when blackhole attack is simulated in AODV in Figure 20. As number of malicious nodes increases PDF should decrease but when malicious node increases beyond 50% PDF starts increasing as network contains more malicious nodes than normal nodes and all the malicious nodes receives the packet.

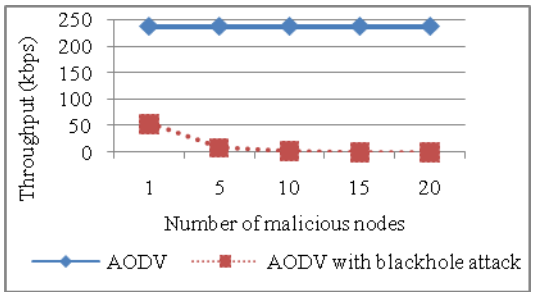

Figure 19: Throughput vs Number of malicious nodes

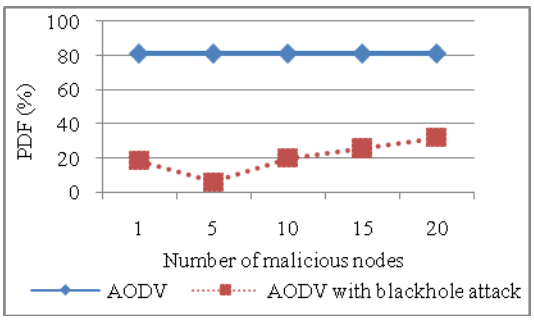

Figure 20: PDF vs Number of malicious nodes

NRL for AODV under blackhole attack is more because when packets are dropped more retransmissions occur so routing overhead increases. In case of AODV without attack NRL remains constant. When number of malicious node increases by 50% then these nodes act as source as well as destination and can easily receive packets so less overhead in routing (refer Figure 21). There is significant difference in number of packets dropped by AODV and AODV under attack as shown in Figure 22. Nearly dropped packets increased by 250% by introducing just one malicious node in the network. As percentage of malicious nodes increases from dropped packets decreases because malicious nodes are the actual destination and they receive the data packets successfully.

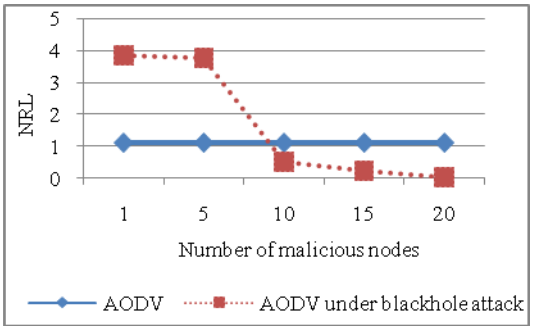

Figure 21: NRL vs Number of malicious nodes

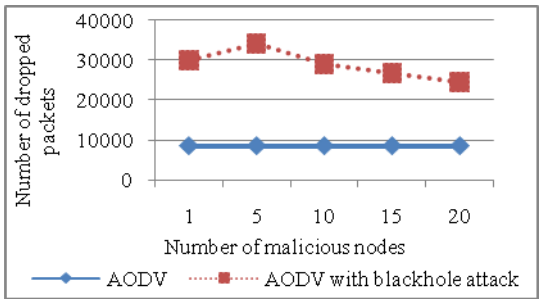

Figure 22: Dropped Packets vs Number of malicious nodes

VII. Conclusion

In this paper, security issues of routing in MANETs are highlighted and the work analyzes the performance of AODV with and without the mounting of blackhole attack under different parameters. The simulation results show that presence of blackhole nodes will have an adverse effect on the AODV performance. Having simulated the blackhole attack, it was observed that packet loss, normalized routing load is increased in the ad-hoc network. Average throughput with blackhole attack reduces to 75% approximately with the presence of single malicious node and further decreases with the presence of more malicious nodes, therefore, it is vital to have an efficient security functions in the protocol in order to avoid such attacks.

VIII. Future Scope

The solution for the blackhole attack is to be developed in the future that will secure routing from source to destination by avoiding multiple blackhole nodes. There is always a trade-off between security and network performance. The need of the hour is to develop optimized security solutions incurring low overhead on limited MANET resources to combat against blackhole attack. The other routing protocols could be simulated as well as they are expected to present different results. Therefore, the best routing protocol for minimizing the blackhole attack can be determined.

References

[1] M. Bouhorma, H. Bentaouit and A. Boudhir, "Performance Comparison of Ad-hoc Routing Protocols AODV and DSR," Proc. IEEE, International Conference on Multimedia Computing and Systems (ICMCS'09), April 2009, pp. 511-514.

[2] S. Gupte and M. Singhal, "Secure routing in mobile wireless ad hoc networks," Ad hoc networks, Elsevier, vol. 1, no. 1, pp.152-174, 2003.

[3] I. Aad, J.-P. Hubaux and E. W. Knightly, "Impact of Denial of Service Attacks on Ad Hoc Networks," IEEE/ACM Transactions on Networking, vol. 16, no. 4, pp. 791-802, 2008.

[4] O. Adaobi, E. Igbesoko and M. Ghassemian, "Evaluation of Security Problems and Intrusion Detection Systems for Routing Attacks in Wireless Self-Organized Networks," IEEE conference On New Technologies, Mobility and Security (NTMS), May 2012, pp. 1- 5.

[5] V. Daza, J. Herranz, P. Morillo and C. Rafols, "Cryptographic techniques for mobile ad-hoc networks," Computer Networks, Elseveir, vol. 51, no. 18, pp. 4938-4950, 2007.

[6] Y. C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," In Eighth Annual International Conference on Mobile Computing and Networking (Mobi-Com 2002), Atlanta, GA, USA, September 2002, pp. 12-23.

[7] D. B. Johnson, D. A. Maltz, and Y. C. Hu, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)," IETF Internet Draft, draft-ietf-manet-dsr-10, accessed on 20 Jan 2013.

[8] K. Sanzgiri, D. LaFlamme, B. Dahill, B. N. Levine, C. Shields and E. M. B. Royer, "Authenticated routing for ad hoc networks," IEEE Journal on Selected Areas in Communications, vol. 23, no. 3, pp. 598-610, 2005.

[9] Y. C. Hu, D. B. Johnson and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks" In the 4th IEEE Workshop on Mobile Computing Systems & Applications, 2002, pp. 3-13.

[10] M. G. Zapata, "Secure Ad Hoc on-demand Distance Vector (SAODV) Routing," IETF Internet Draft,draft-guerrero-manet-saodv-03, 2005, accessed on 20 Jan 2013.

[11] D. Djenouri, L. Khelladi and N. Badache, "A Survey of Security Issues in Mobile Ad Hoc and Sensor Networks," IEEE Commun. Surveys and Tutorials, vol. 7, no. 4, pp. 2-28, 2005.

[12] H. L. Nguyen, "A study of different types of attacks on multicast in mobile ad hoc networks," Ad Hoc Networks, Elsevier, vol. 6, no. 1, pp. 32-46, 2006.

[13] Usha and Bose, "Understanding Black Hole Attack in Manet," European Journal of Scientific Research, vol. 83, no. 3, pp. 383-396, 2012.

[14] C. Perkins, E. Royer, and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing," IETF, RFC 3561, 2003, accessed on 10 Jan 2013.

[15] D. Chakeres, E.M. Belding-Royer, "AODV routing protocol implementation design," Proc. Of 24th International Conference on Distributed Computing

Systems Workshops- W7: EC (ICDCSW'04), March 2004, vol. 7, pp. 698-703.
[16] K. Fall and K. Varadhan (Eds.), ns notes and documentation, 1999 accessed on 24 Dec, 2012.
[17] T. Issariyakul, E. Hossain, "Introduction to Network Simulator NS2," Springer, US, 2009.
[18] P. Bakalis and B. Lawal, "Performance Evaluation of CBR and TCP Traffic Models on MANET Using DSR Routing Protocol," International Conference on Communications and Mobile Computing (CMC), April 2010, vol. 3, pp. 318-322.
[19] W. Navidi and T. Camp, "Stationary distributions for the random waypoint mobility model," IEEE Transaction. Mobile Computing, vol.3, no.1, pp. 99-108, Jan-Feb 2004.
[20] F. J. Ros and P. M. Ruiz, "Implementing a New Manet Unicast Routing Protocol in NS2," December, 2004, [Online] Available: http://masimum.dif.um.es/nsrt-howto/pdf/nsrthowto.pdf accessed on Dec 29, 2012.
[21] A.U. Salleh, Z. Ishak, N. M. Din, and M. Z. Jamaludin, "Trace Analyzer for NS-2," IEEE, Student Conference on Research and Development (SCOReD), Malaysia, June 2006, pp. 29-32.
[22] I. K. Tabash, N. Ahmad and S. Beg, "Performance Evaluation of TCP Reno and Vegas over different routing protocols for MANETs," IEEE 4th International Symposium on Advanced Networks and Telecommunication Systems (ANTS), Dec. 2010, pp. 82-84.

Tarunpreet Bhatia is currently pursuing M.E. in Computer Science and Engineering from Thapar University, Patiala. She received her B. Tech in Computer Science and Engineering from ACE, Kurukshetra University. Her research interests include wireless networks, network security, MANETs and wireless sensor networks.

Dr. A. K. Verma is currently an Associate Professor in the department of Computer Science and Engineering at Thapar University, Patiala. He received his B.S., M.S. and Doctorate in 1991, 2001 and 2008, respectively, majoring in Computer science and engineering. He has worked as Lecturer at M.M.M. Engineering College, Gorakhpur from 1991 to 1996. He joined Thapar University in 1996. He has published over 120 papers in referred journals and conferences (India and Abroad). He has chaired various sessions in the International and National Conferences. He is a MIEEE, MACM, MISCI, LMCSI, MIETE, GMAIMA. He is a certified software quality auditor by MoCIT, Govt. of India. His research interests include wireless networks, routing algorithms and cloud computing.

