Performance Evaluation of AODV with and without Black hole Attack in MANETs

Devottam Gaurav, CharuWahi

Abstract-A Wireless ad-hoc network is a temporary network where several mobileindependent nodes can move freely in any direction. With the help of routing protocols source node locates a path to the target node and forward data packets through intermediate nodes.However, due to mobility and ad-hoc nature, security becomes an important issue in MANET because once malicious nodes are in the range of networks; they can join the network freely and degrades the performance by attacking it. The vulnerability of MANET is very high towards routing attacks such as blackhole, which drops all the packets instead of forwarding it to the targeted node andresults in data loss. This research paper focuses on analyzing the performance of AODV with various parameters such as throughput, packet delivery ratio, normalized routing load and average end-to-end delay using different scenariosof network configuration with and without blackhole attack in MANET.

Keywords-*AODV, Blackhole, MANET, Ns2.34, Routing Protocols.*

*****

1. INTRODUCTION

MANET itself stands for Mobile Ad Hoc Network which is an automated network consisting of several mobile nodes communicating with each other via transmission links through wireless medium. "**Ad Hoc**"in Latin itself stands "**for this purpose**" where devices change its links frequently in any direction. They also forward their traffic to other devices unrelated to its own use and therefore can be named as a router. Hence, MANET is a temporary network of several mobile routers (and associated hosts) which are interlinked by asymmetrical links dynamically without any pre-existing network infrastructure[1]. Mobile nodes are able to move randomly in any direction at any given point of time or can be arbitrary located [2]. Moreover, these are often regarded as autonomous network because of absence of centralized administration. In other words, the topology is dynamic and routing of traffic through a multi-hop path is necessary so that all nodes can communicate easily[3].

A key point in MANETs is that amount of traffic generated by the routing protocols is kept at a least due to limited bandwidth availability through mobile nodes. These issues have been addressed in several routing protocols.

1.1. Classification of Routing Protocols

S. Gupta et. al. [4] have classified routing protocols on the basis of type of necessity and type of resources (Figure 1):

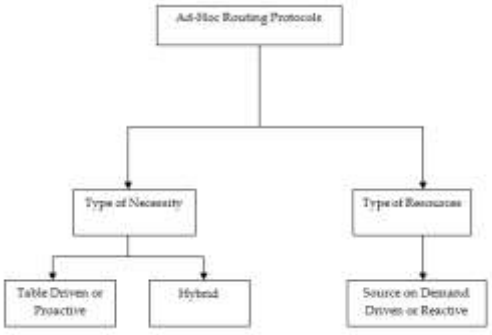

Figure 1:Classification of Routing Protocols [2]

1.1.1. Depending upon the type of necessity

- **Proactive or Table driven Routing Protocols**

The table driven approach is similar to the connectionless approach of forwarding data packets, with no regard to when and how frequently such routes are desired. It relies on an underlying routing table update mechanism that involves regular propagation of routing information [5]. Here, a route to every other node in ad-hoc network is always available, regardless of whether or not it is needed. Examples of such approach are DSDV (Destination Sequence Distance Vector Routing Protocol), OLSR (Optimized Link State Routing Protocol), etc.

- **Hybrid Routing Protocols**

These protocols combine the best features of proactive and reactive routing protocols. In other words, it is used to find a balance between both protocols. Example of such approach is Dynamic MANETs On-demand Routing Protocols (DYMO).

1.1.2. Depending upon the type of resources

- **Source on demand or Reactive Routing Protocols**

These protocols try to eliminate the conventional routing tables and consequently reduce the need for updating these tables to track changes in the network topology. In an On-demand approach, when a node desires a route to the destination, it will have to wait until such route can be discovered, i.e.,routes are discovered whenever a source node have packets to send[5] and maintain it until either the route is no longer desired or it becomes inaccessible and finally remove it by route deletion procedure. Examples of such protocols are Ad-Hoc on Demand Distance Vector Routing Protocol (AODV), Dynamic Source Routing (DSR).

The attacks targeting MANET routing protocols are classified as active and passive attacks [6]. Passive attacks 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. However, one of the most popularized security threats which change the behavior of routing problem is black hole attack. Blackhole attack is deliberated under the AODV routing protocol and its effects are studied by stating how this attack interrupt the performance of MANET. Very little awareness has been given to the fact to study the impact of Blackhole attack in MANET using Reactive protocols and to find out why this protocol is more vulnerable against the attack. There is a need to address this type of protocol as well as the impacts of the attacks on the MANETs.

The remaining part of the paper is summarized as follows: Section 2 provided an overview of AODV routing protocol. In section 3, we describe the effects of blackhole attackon AODV. In section 4, we present experimental configuration of the network used in different scenarios. In section 5, analysis of results is done to visualize the effect of blackhole attack on AODV in MANETs.Finally, we conclude in Section 6.

2. AODV

Ad-Hoc Distance Vector Routing Protocol (AODV) [7] offers quick alterations to dynamic link conditions, low dispensation, low memory overhead, low network consumption and unicast route purpose to destinations within the ad-hoc network[8]. It uses destination sequence numbers (DSN) to ensure loop freedom at all times (even in face of inconsistent delivery of routing control messages), avoiding troubles (like continuing to infinity) linked with standard distance vector protocols[9].
The primary objective of AODV routing protocol are [10]:

- To transmit discovery packet only when it is necessary.
- To differentiate between local connectivity management (neighborhood discovery) and general topology protection.
- To publicize about changes in local connectivity to those adjacent mobile nodes which are in needs of such information.
- AODV diminish the control overhead by decreasing the number of transmits using a pure on-demand route acquisition method. AODV uses only symmetric link between adjacent nodes.

3. BLACKHOLE ATTACK

An intermediate node works alone or a collection of intermediate nodes works in collusion to carry out blackhole attack.The performance of the routing services are degraded due to the formation of routing loops, forwarding ofpackets through non optimal paths or selectively sinking of packets by the malicious node. This intermediate node is called as Blackhole[11] (Figure 2).

A Blackhole nodehas two properties:

- The node makes use of ad-hoc routing protocol, for instance AODV, to publicize itself as a valid route to a target node, even if, the route is fake with the aim of interrupting packets.
- The node guzzles the intercepted packets.

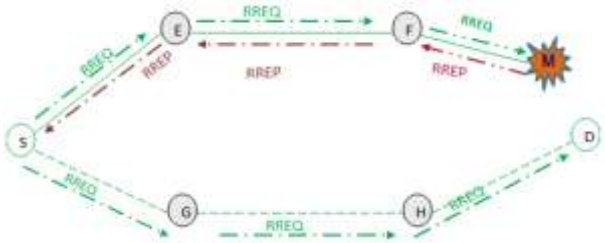

Figure 2 : Blackhole Attack Problem

4. EXPERIMENTAL CONFIGURATION

All the simulation work is performed in Ns2 wireless network simulator version 2.34.Scenarios have been designed within a terrain area of 750m*750m. The channel is wireless channel on Two Ray Ground Propagation Model. Mobility model used is Random Way Point (RWP) [12]. In this model, a mobile node is placed randomly at any location in the simulation arena. This model is based on pause times between any change in direction and/or speed [13]. For simulation, the speed of node changes from 10m/s to 60m/s with and without blackhole attack. Packet size of each datagram is 1000 bytes and maximum queue length is set to 50 packets. Each CBR source sends packets at the rate of 0.01Mb. Network traffic load is provided by constant Bit Rate (CBR) application[14].

A CBR traffic source presents a constant stream of packets during the entire simulation, thus further pressurizing the routing task. MAC_802.11 is used as medium access control protocol. Multiple runs are conducted for each scenario by varying the simulation parameters and average of collected data is obtained.The overall simulation parameters are depicted in Table 1.

Table 1: Simulation Parameters

Parameters	Value
Simulator	Ns-2.34
Area	750m * 750m
Routing Protocol	AODV
Simulation Time	200s
Application Traffic	CBR

Number of nodes	10, 20, 30 , 40, 50
Number of malicious nodes	1, 2, 3, 4, 5
Packet Size	1000 bytes
Maximum Speed	10m/s to 60m/s
Number of Connections	5
Movement Model	Random Way Point

The performance metrics describes the outcome of the simulation or set of simulations. They also indicate about what really happened during the simulation and provide valuable information about the proposed system.The performance metrics chosen for the evaluation of blackhole attack are packet delivery ratio, throughput, normalized routing load and average end-to-end delay:

- **Packet Delivery Ratio (PDR):** It is defined as the ratio of number of data packets sent to all the receivers to the number of data packets thought to be delivered to the receivers. The ratio represents the effectiveness of the routing protocol [15]:

  PDR (%) = Number of Packets Received *100
  Number of Packets Sent

- **Throughput:** It refers to how much data can be moved from source to the receivers in a given period of time. It is measured in Kbps (kilo Bits per Second) [16].

Average Throughput = Number of bytes received *8 (kbps)
Simulation Time * 1000

- **Normalized Routing Load (NRL):** It is defined as the ratio of number of routing packets transmitted per data packets received[15].

  NRL = Number of routing packets
  Number of packets received

- **Average End to End Delay (EED):** It is average time taken for a data packet to move from source to the receivers. It is measured in milliseconds (ms).

EED = Total EED ms
Number of packets sent

5. SIMULATION RESULTS

Our simulation results illustrate three different scenarios, i.e., by varying number of nodes, by varying number of malicious nodes and by varying speed of nodes against throughput, packet delivery ratio, average end-to-end delay and normalized routing load.

5.1. By varying the number of nodes

The Scenario 1 (Figure 3) shows the movement of 30 mobile nodes without the presence of blackhole attack where the source and destination nodes are 0 and 8 respectively. The same scenario is taken for 10, 20, 40 and 50 mobile nodes without blackhole attack under simulation time as 200s.

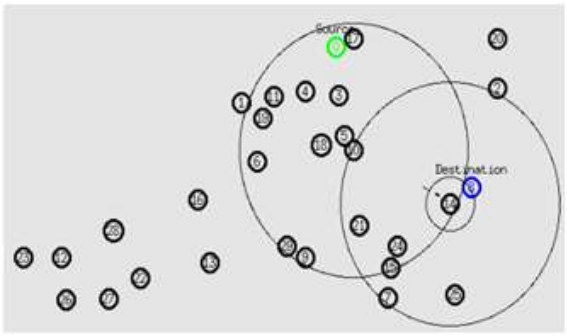

Figure 3: By varying number of nodes

The simulation results in Figure 4 depict that throughput of AODV increases more with increase in number of nodes as compared to throughput of AODV under blackhole attack.The reason behind this is that malicious node abandons all the data packets rather than sending it to the destinations, thus effecting throughput under attack.

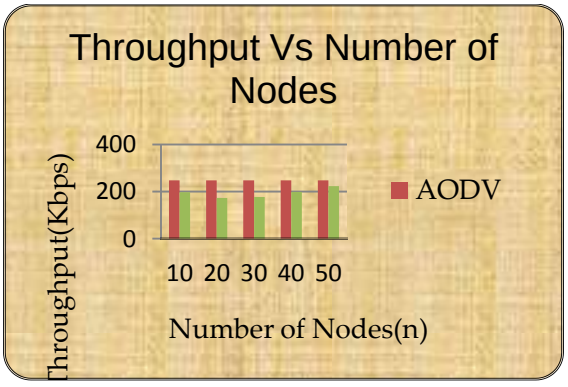

Figure4:Throughput Vs Number of nodes

PDR drops from 99.96% to 59.871 in presence of blackhole. The curve of PDR under blackhole attack first decreases with increase in number of nodes, then, increases linearly in the network as compared to AODV without attack which has very little effect upon it (Figure 5). This is because a blackhole node drops the maximum amount of packet of those nodes which are closest to it and hence hampers the performance of the network.

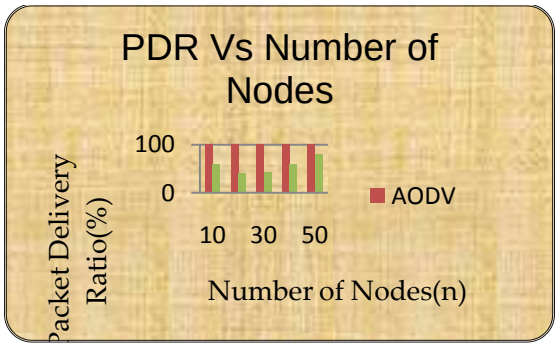

Figure5:PDR Vs Number of nodes

NRL for AODV under blackhole attack is more than as compared to AODV as more packets are dropped so more retransmission takes place. Furthermore, from Figure 6, we observe that both curves behave in the same way, i.e., NRL increases with increase in number of nodes as more routing information is swapped but the curve of AODV under attack is always above the AODV.

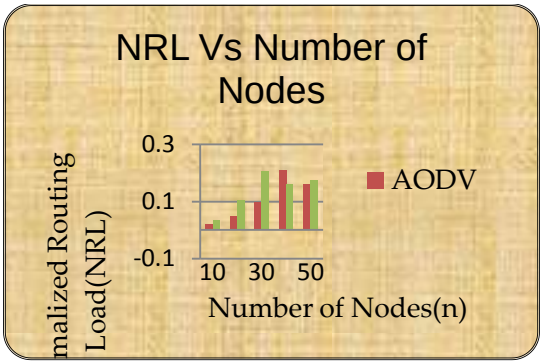

Figure6:NRL Vs Number of nodes

It can be shown(from Figure 7) that Avg. End-to-End Delay Vs number of nodes without blackhole attack increases up to 30 nodes but henceforth starts decreasing. In case ofblackhole attack it increases up to 30 nodes followed by. The reason for this is that higher node density increases the number of neighboring nodes and that causes more route reply messages to the source node and thus causes increase in delay.

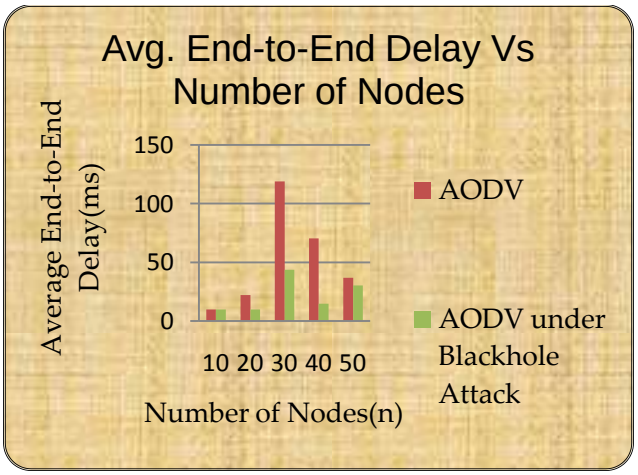

Figure 7:Avg. End-to-End Delay Vs Number of Nodes

5.2. **By varying number of malicious nodes**

The Scenario 2 (Figure 8) shows the movement of 30 mobile nodes with the presence of blackhole attack where the source node, destination node and blackhole node are 0, 8 and 21 respectively. The same scenario is taken for 2, 3, 4 and 5 blackhole nodes under simulation time as 200s.

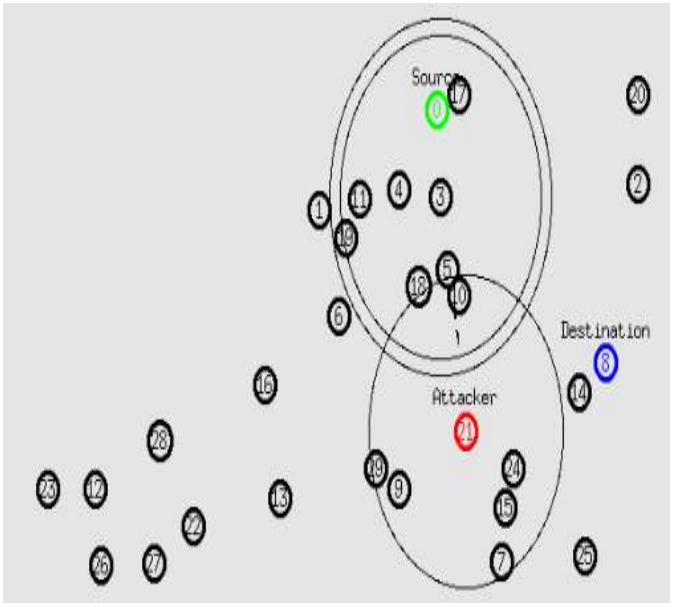

Figure 8: By varying number of malicious nodes

The next scenario incorporates variation in number of malicious nodes in a MANET of 30 nodes.In case of original AODV protocol, the throughput is 247.75kbps but it drops to 177.14kbps under blackhole attack. It is quite obvious that throughput linearly decreases and increases with increase in number of malicious nodes in the network (Figure 9).

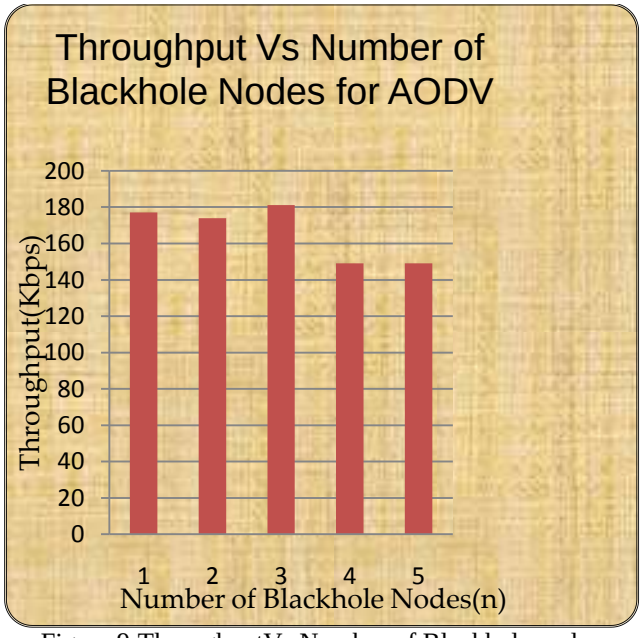

Figure 9:ThroughputVs Number of Blackhole nodes

When PDR of AODV protocol is 99.759%, then it is observed that the PDR of the network with one blackhole node drops to 42.811%. It can be seen that PDR of AODV linearly decreases and increases when there is increase in number of malicious nodes in the network (Figure 10).

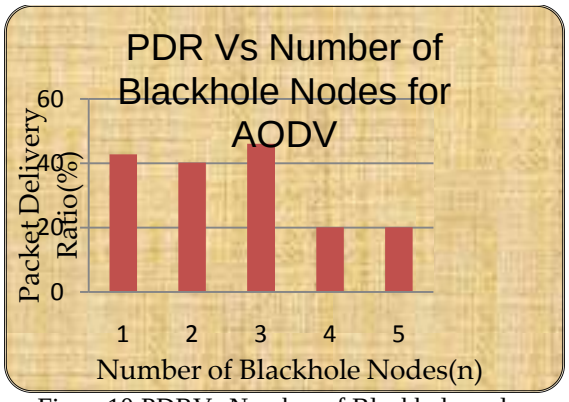

Figure10:PDRVs Number of Blackhole nodes

The impact of malicious node on NRL and average end-to-end delay are depicted in (Figure 11) and (Figure 12) respectively. It can be observed that NRL increases with increase in number of malicious node but average end-to-end delay decreases with increase in number of malicious nodes.

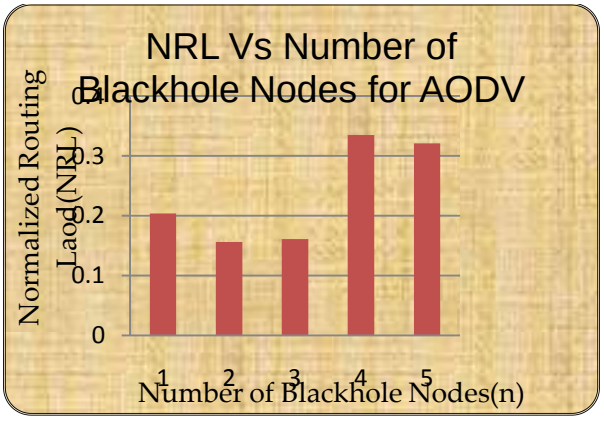

Figure 11:NRLVs Number of Blackhole nodes

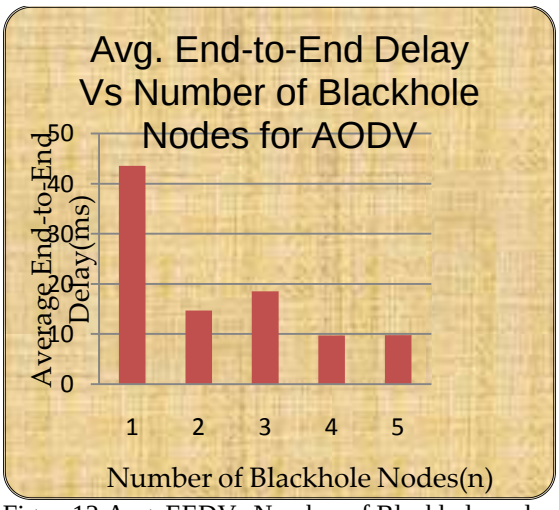

Figure12:Avg. EEDVs Number of Blackhole nodes

5.3. **By varying speed of nodes**

The Scenario 3 (Figure 13) shows the movement of 30 mobile nodes with the presence of blackhole attack where the source and destination nodes are 0 and 8 respectively.

The same scenario is taken for 10, 20, 40 and 50 mobile nodes with blackhole attack under simulation time as 200s and speed of nodes vary from 10m/s to 60m/s . The performance of the network Vs speed of nodes are calculated in the light of average throughput, packet delivery ratio, average end-to-end delay and normalized routing load.

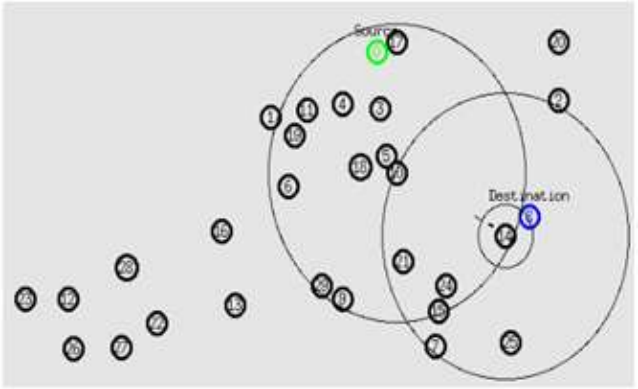

Figure 13:By varying speed of nodes

The effect of speed variations for AODV and AODV under blackhole attack has been examined. It is obvious from the graph that the blackhole attack worsened the network throughput. It depicts that there is slight increase in throughput from 247.75kbps to 247.95kbps as speed raises up to 30m/s because mobile nodes while moving enter into the transmission range of other nodes so packets may be distributedrapidly but escalating node speed ahead of 30m/s outcomes in lessen throughput (Figure 14).The reason behind this is that as speed rises, more re-route discovery messages are swapped among nodes and thereby increasing collision in the network.

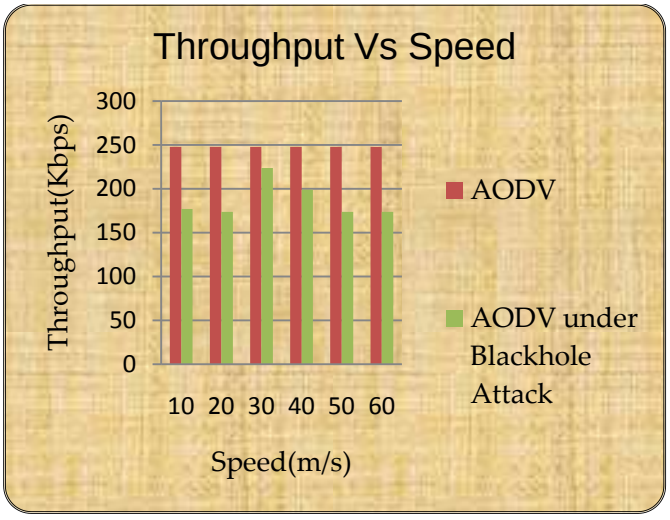

Figure 14:Throughput Vs Speed of Nodes

PDR for AODV with attack reduces by 49% as compared to PDR without attack (Figure 15). PDR increases in the

beginning with increase in speed but beyond 30m/s it started declining due to congestion in the network.

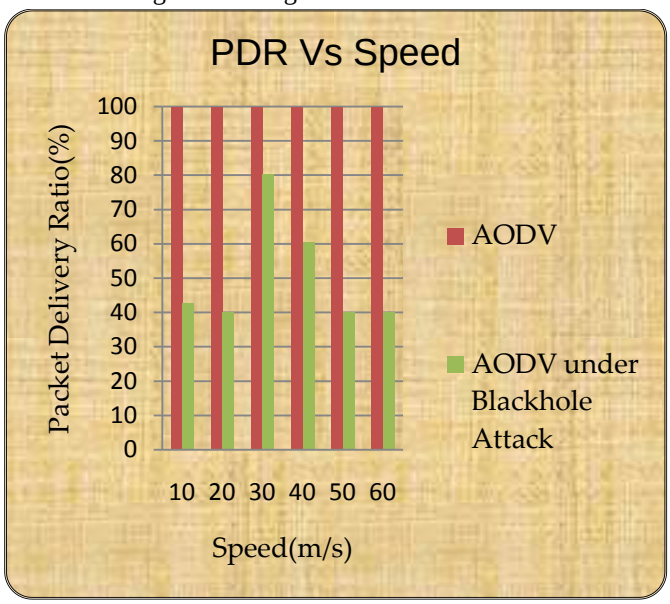

Figure 15:PDR Vs Speed of Nodes

From (Figure 16), we observe that NRL for AODV under blackhole attack is more as packets are dropped so more retransmissions occur.

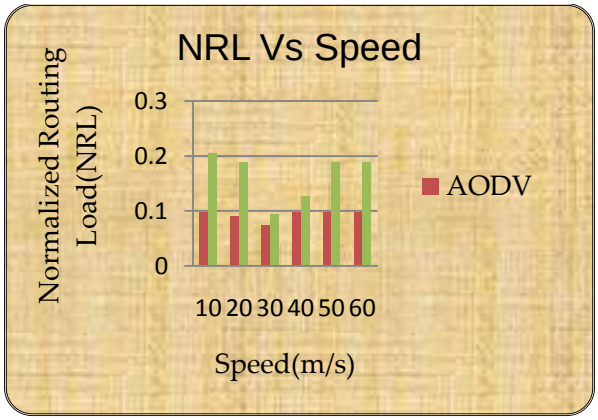

Figure 16:NRL Vs Speed of Nodes

6. Conclusion

In this paper, we analyzed the performance of an AODV Network with and without blackhole attack using different simulation parameters. Thereafter, the fact is that AODV protocol is susceptible to the Blackhole attacks.The simulation results showed that presence of blackhole nodes will have an unfavorable effect on the AODV performance. During simulation of blackhole attack, it was observed that normalized routing load and packet loss are increased in the ad-hoc network. Due to increase in packet loss in the network, the blackhole attack affects the overall network connectivity and causes the data loss in the network. Average throughput with blackhole attack lessen to 72% approximately with the presence of single malicious node and further declines with the presence of more malicious nodes, therefore, it is essential to have security functions in the routing protocol in order to evade such attacks.

7. Future Work

We simulated the Black Hole Attack in the Ad-hoc Networks and investigated its affects. In our study, we used the AODV routing protocol. But the other routing protocols could be simulated as well. All routing protocols are expected to present different results. Therefore, the best routing protocol for minimizing the Black Hole Attack may be determined.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.

References

[1] Burbank JL, Chimento PF, Haberman BK, Kasch WT (2009) Key Challenges of Military Tactical Networking and the Elusive Promise of MANET Technology. IEEE Communication Magazine 44(11):39–45.

[2] M. Frodigh, P. Johansson, P. Larsson, 2000, “Wireless Ad-Hoc Networking: the art of networking without a networking”, Ericsson Review, No.-4, pp.248-263.

[3] Abolhasan, M., Wysocki, T., Dutkiewicz, E (2004): A review of routing protocols for mobile ad hoc networks. Elsevier, Amsterdam.

[4] Sachin Kumar Gupta, R.K. Saket, June 2011, “Performance Metric Comparison of AODV and DSDV Routing Protocols Using Ns-2”, Volume 7, Issue 3,

[5] C. Siva Ram Murthy, B.S. Manoj, 2004, “Mobile Ad-Hoc Networks-Architectures & Protocols”, Pearson Education, New Delhi.

[6] PriyankaGoyal, SahilBatra, Ajit Singh, November 2010, “A Literature Review of Security Attack in Mobile Ad-hoc Networks,” International Journal of Computer Applications (0975 – 8887), Volume 9, No.12.

[7] Charles E Perkins,E M Royer,Sameer R. Das, 2001, “Ad hoc On-Demand Distance Vector (AODV) Routing,” Internet Draft, draft-ietf-manetaodv- 09.txt.

[8] Shurman, M.A., Yoo, S.M., Park, S(ACMSE 2004).: Black hole attack in wireless ad hoc networks. In: ACM 42nd Southeast Conference.

[9] Hu Y-C, Perrig A (2004) Survey of Secure Wireless Ad Hoc Routing. IEEE Security & Privacy 2(3):28–39. doi: 10.1109/ MSP.2004.

[10] Layuan, Li Chunlin, YaunPeiyan, February 2007, “Performance Evaluation and simulation of Routing Protocols in Ad-Hoc Networks”, Computer Communication.

[11] CH.V. Raghavendran, G. Naga Satish and P. Suresh Varma, 2013, “Security Challenges and Attacks in Mobile Ad Hoc Networks,” Information Engineering and Electronic

Business, 3, 49-58 Published Online September 2013 in MECS.

[12] Kevin Fall, KannanVaradhan, 24 Dec.-2012,The Ns Manual and documentation, 1999 accessed, Available: http://www.isi.edu/nsnam/ns/doc/index.html.

[13] W. Navidi, T. Camp, Jan-Feb 2004, "Stationary distributions for random way point mobility model", IEEE Transaction. Mobile Computing, Vol.3, No. 1, pp.99-108.

[14] B. Bakawis, B. Lawal, April 2010, "Performance Evaluation of CBR and TCP Traffic Models on MANET Using DSR Routing Protocol", International Conference on Communications and Mobile Computing (CMC), Vol.3, pp.318-322.

[15] I.K. Tabash, N. Ahmad, S. Beg, Dec.-2010, "Performance Evaluation of TCP Reno and Vegas over different routing protocols for MANETs", IEEE 4th Symposium on Advanced and Telecommunication Systems (ANTS), pp.82-84.

[16] A.U. Salleh, Z. Ishak, N.M. Din, M.Z. Jamaludin, June 2006, "Trace Analyzer for Ns-2", IEEE Student Conference on Research and Development (SCOReD), Malaysia, pp.29-32.

DECLARATION:

I and CharuWahi hereby declare that there is no conflict of interest regarding the publication of this manuscript.

Devottam Gaurav (M.Tech Scholar)

CharuWahi (Assistant Professor)

SUMMARY OF AUTHORS:

CharuWahi is currently a PH.D. candidate in the department of Computer Science & Engineering, Birla Institute of Technology, Ranchi. She received her B.E. degree in Electronics and M.Tech- Computer Science in 2008. She is currently working as Assistant Professor in the Department of Computer Science and Engineering, Birla Institute of Technology, Ranchi. Her research areas include routing, security, quality of service especially in mobile ad-hocnetworks and sensor networks.

Devottam Gaurav is currently working as Assistant Professor in the department of Computer Science & Engineering, Noida Institute of Engineering & Technology, Gr. Noida. He received his B.E. degree in Information Science & Engineering from Basaveshwar Engineering College, Karnataka in 2012 and M.Tech – Computer Science & Engineering from Birla Institute of Technology, Ranchi in 2015. His research areas include routing, security especially in mobile ad-hocnetworks and wireless sensor networks.