Impact of Black hole Attack on Performance of AODV Routing Protocol

Parminder Kaur, Monika Sachdeva, Gagandeep

Abstract- MANET includes number of wireless nodes. The network topology varies frequently. During the communication nodes act as sender, receiver and router. There is various attacks in MANET routing protocols. In this paper, we discuss about the black hole attack under AODV. Black hole attack accesses the packets and then drops packets. In this paper, we evaluate and stimulate the effect of black hole in AODV. We evaluate the performance of AODV under black hole attack using different performance metrics i.e. Energy consumption, Average Jitter, End-to end Delay and throughput. Simulation is carried out using widely used simulator Qualnet.

Keywords- MANET, AODV, Black hole, Performance metrics.

I. INTRODUCTION

MANET is consist of wireless nodes which are linked with each other to communicate .It is infrastructure less network i.e. there is no central access point. It is self-configured network in which the nodes communicate or send message from source to network and also nodes are independent to network i.e. node can join or leave a network[1]. Topology change accordingly the route is modernized. The nodes in network proceed as a sender, receiver and router [2]. Whenever nodes start communication, nodes start moving toward the destination.

II. ROUTING PROTOCOLS

There is the classification of routing protocols:

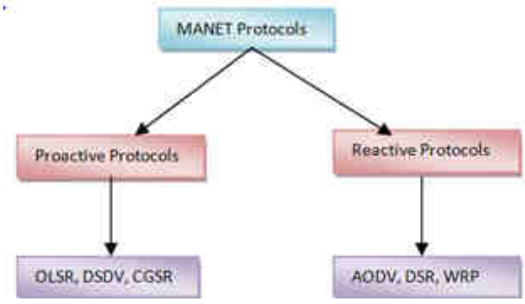

Fig.1 Classification of routing Protocols

Proactive Protocols: Proactive protocols are recognized as table driven protocols in which nodes store the information in tables [3]. All the nodes maintain the information about their neighbor nodes. Nodes maintain an accurate and consistent update of network topology [4]. There is no need to discover the route for communication. Examples of Proactive Protocols are OLSR, DSDV and CGSR.

Revised Version Manuscript Received on April 28, 2016.

Parminder Kaur, Department of Computer Science and Engineering, Shaheed Bhagat Singh State Technical Campus, Ferozepur (Punjab). India.

Monika Sachdeva, Associate Professor, Shaheed Bhagat Singh State Technical Campus, Ferozepur (Punjab). India.

Gagandeep, Assistant Professor, Shaheed Bhagat Singh State Technical Campus, Ferozepur (Punjab). India.

Reactive Protocols: Reactive protocols are the on demand protocol in which the route is discovered and establish when required [5]. Route discovery process is used in reactive protocols. It consumes bandwidth only when the node communicates. Examples of Reactive protocols are: ADOV, DSR, SSA and WRP.

AODV: Adhoc On-Demand Distance Vector routing is on demand protocols in which the route establish when requiring [6]. AODV overcome the problem of counting-to-infinity problem by using sequence number than other protocols. AODV consist of unicast, broadcast and multicast routing. The source node broadcast the route request (RREQ) to their neighbor nodes and then further that nodes forward RREQ to their neighbor nodes.

Route Request: The network is established whenever source node need to communicate with its destination node [7]. If there is no route for the communication then source node generates RREQ (route request) and broadcast to all its neighbors. Route request has following fields:

Table1: Route Request field

Source Address	Route Request ID	Sequence no.	Destination Address	Hop count

***Establishing Route*:** When source node doesn't have any path to transfer packets then source node broadcast Hello message to all its neighboring nodes and routing tables are updated simultaneously[8]. The nodes receive RREQ then all nodes check routing table. If there is route exist from the source to destination then that receiver node send back RREP (route reply) to the source node and if there is no path then receiver nodes rebroadcast the message to its neighboring nodes. This process is continued until route is not found [9]. Whenever path is found then intermediate nodes update its routing table. While receiving route reply, then source node send the information using established route.

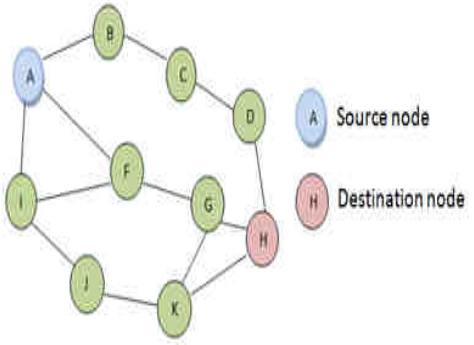

Fig.2 Route Discovery

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

Route Reply: After finding a path or route from source to destination for communication, receiver node send back route reply to source node. Packets have following information:

Table 2: Packet fields

Source Address	Destination Address	Destination sequence no.	Hop count	Life time

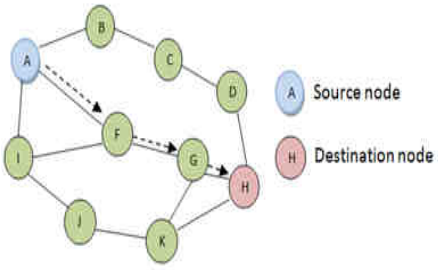

Fig.3 Path selected

Route Error: All nodes store the information about neighboring node in the route table. When the node gets lost in route or any type of error occurs, the route error (RERR) message is generated to notify the others node [10].

Route Deletion: The route will be activated till the packets are transferred. If the route is not in use or route is idle then the route will be deleted. The life time of route is user defined and timeout of route's life time then route will be deleted or inactive [11]. After that the communication is not possible by this route. Whenever route fails to transfer packets then route will be deleted. If there is any link breakage then RERR (route error) message is generated to notify the error in route [12]. When RERR message is received by nodes then each node deletes that invalid route from its routing table. If this route is required then the node can reinitiate for communication [13]. Whenever the path is discovered then shortest path is selected for the communication between the source and destination [14]. There is less overhead than DSDV. With the increasing of mobility, then overhead packets also increased and the line failure and route discovery are also rises [15]. Latency is also less in AODV than DSR and DSDV.

Black hole Attack: Black hole attack is an active attack that is defined as a malicious node. A malicious node accesses the packets and drops all the packets. When the black hole node receives the route request then it sends back immediate route reply without checking its routing table. Malicious node sends a high sequence number to make entry as a fresh and valid route [16]. Then the source node supposes that this is valid and short route for the communication and ignores the other route replies.

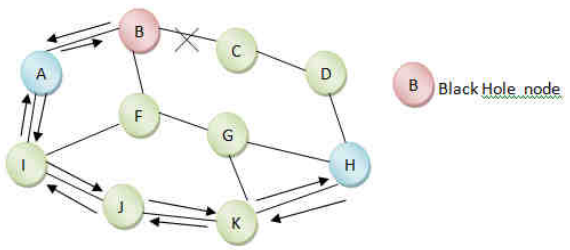

Fig.4 Black hole Attack

After receive a RREP from malicious node, source node send the packets to malicious node [17].So the malicious nodes access all the packets from source and drop all the packets. Behavior of black hole is determined by that it advertise itself a fresh and latest route and showing its high sequence number to defined that route is valid for transferring the packets. From this way malicious nodes attacks on route and then access and drop the packets [18].

Algorithm:

Step 1: Searching phase
Generate discovery process from the source node by generating (new hash value).Assigned current time and time required to receive reply.
Step 2: Storing phase
Store all the route replies from neighboring nodes then check the speed of the nodes and compute the threshold which decide whether to put the node into blacklist or not.
Step 3: Identification Phase
Repeat the step 1 and 2 until reach the destination in effective way. Once the node identified as a black hole , the route node update table by adding blackhole node address.
//Initialize blacklisted neighbors
AodvBlacklistNode*current=BlacklistTable->head
AodvBlacklistNode*previous=NULL
Step 4: Continue default process of AODV.

III. SIMULATION ENVIRONMENT

Goal of this simulation study is to calculate and analyze the performance of black hole under AODV protocol using different performance metrics. The simulations have been performed using Qualnet version 6.1, software that provides scalable simulations of Wireless Networks. We simulate the network using the various source nodes like 10, 20, 30 and 40 over a terrain of 500m*1500m area. Source and destination are same in each model are locating at same place. Simulation time is 30 sec. AS simulation start the nodes start moving towards their destination node in network.

Table3: Simulation Parameters

Parameters	Values
Routing Protocol	AODV
Terrain size	1500*1500
Mobility Model	Random waypoint model
No. of Sources	10,20,30,40
Simulation Duration	30sec
Data Traffic Rate	CBR
MAC Layer	802.11

***Energy consumption*:** Total amount of energy consumed by the nodes in the network. Four possible energy consumption states are identified: transmit mode, receive mode, idle mode and sleep mode

Average Jitter: Jitter is defined as the variation in packet arrival time. It signifies the packets from the source will reach the destination with dissimilar delays. A packet's wait varies with location in the queues of the routers along the path between source and destination and this position varies unpredictably.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

***End-to-end delay*:** The delays is calculated from and in which all the packets transmitted from sender to receiver and including the average time, data received at latency and retransmission delay.

***Throughput*:** It is defined as number of packets received by the destination and measures the effectiveness of a routing protocol and is the number of packets delivered successfully.

IV. RESULTS AND DISCUSSIONS:

In this, we evaluate the performance of black hole under Ad hoc Demand Distance vector (AODV), for wireless ad hoc networks based on performance. We are simulating the AODV routing Protocol with variations in nodes i.e. 10, 20, 30 and 40 and analyzing the performance of AODV in the light of energy consumption, Average Jitter, end to end delay and Throughput in MANET. End-to-end delay: Fig.5: Shows that AODV under black hole attack, have more delay than without black hole. With the variation of nodes, delay increases with black hole AODV.

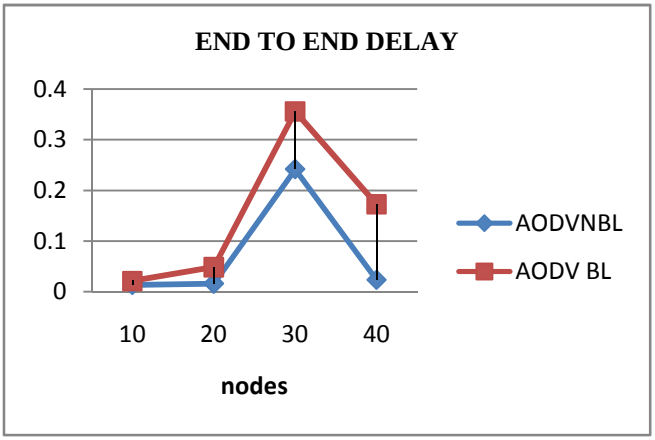

Fig.5 End-to-end delay

Throughput: Fig.6: Shows that the throughput of AODV is greater than the AODV with blackhole attack and AODV perform better.

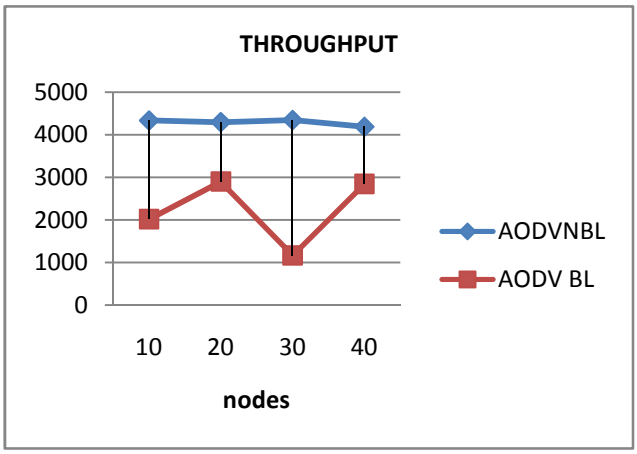

Fig.6 Throughput

Energy consumption: Fig.7. Shows that black hole node in AODV consumes more energy in transmission mode but AODV consume less energy.

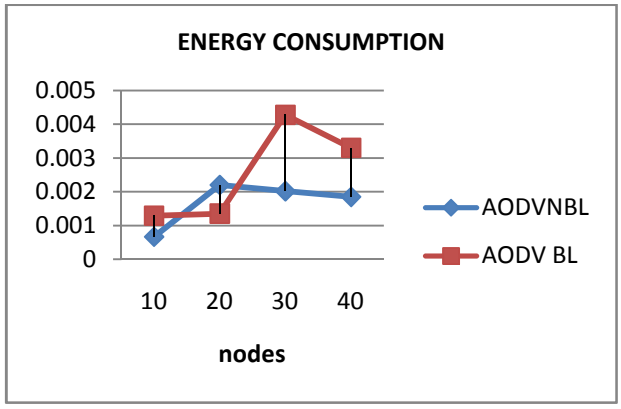

Fig.7 Energy Consumption

A. *Average Jitter*:

As shown in fig 8. . Jitter is increased with black hole due to delays. There is more delay in blackhole than AODV without blackhole

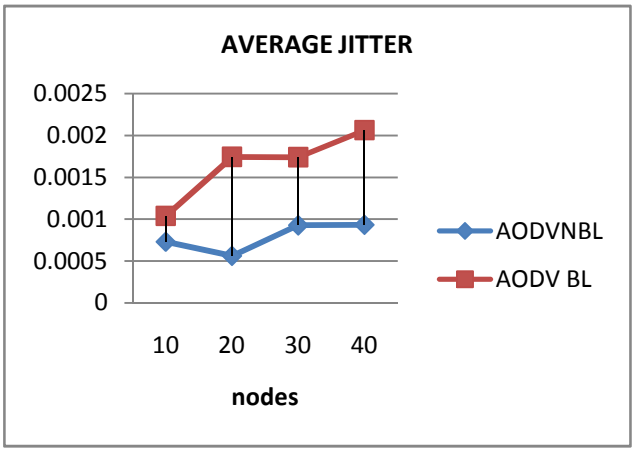

Fig.8 Average Jitter

V. CONCLUSION AND FUTURE WORK

In this paper, we evaluate the effect of black hole attack under the performance of AODV protocol. The performance metrics are energy consumption, average jitter, end to end delay and throughput. The simulation has been done using Qualnet simulator. The simulation result shows that when there is black hole node in network then it can be affected and degrade its performance. We use an algorithm for detection and prevention of black hole. In future, we plan for evaluate and stimulate the effect of black hole in other protocols.

REFERENCES

1. P.R.Jasmine jeni, A.Vimala Juliet, R.Parthasarathy, A.Messiah Bose "Performance Analysis of DOA and AODV Routing Protocols with Black Hole Attack in MANET" International Conference on Smart Structures & Systems,ISBN:978-1-4673-6240-5/32©2013 IEEE.
2. Avni Khatkar, Yudhvir Singh "Performance Evaluation of Hybrid Routing Protocols in Mobile Adhoc Networks " International Conference on Advanced Computing & Communication Technologies,ISBN:978-0-7695-4640-7/12©2012 IEEE.
3. Mona N.Alslaim, Haifaa A.Alaqel, Soba S.Zaghloul "A Comparative Study of MANET Routing Protocols" ISBN:978-1-4799-3166-8©2014 IEEE.
4. Harjeet Kaur, Varsha Sahni, Dr. Manju Bala " A Survey of Reactive,Proactive and Hybrid Routing Protocols in MANET:A Review" IJCSIT,ISSN:0975-9646,2013.
5. Latif Ullah Khan, Faheem Khan, Naeem Khan "Effect of Network

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

Density on the Performance of MANET Routing Protocols" International Conference on Circuits, Power and Computing Technologies,ISBN:978-1-4673-4922-2/13©2013 IEEE.
6. Mr.B.Karthikeyan,Mrs. N.Kanimozhi, Dr.S.Hari Ganesh "Analysis of Reactive AODV Routing Protocol for MANET" ISBN:978-1-4799-2877-4/14© 2014 IEEE.
7. Gagandeep, Aashima " Study on Sinkhole Attacks in Wireless Adhoc Networks" IJCSE,ISSN:0975-3397,2012.
8. Gagandeep, Aashima ,Pawan kumar " Analysis of Different Security Attacks in MANETs on Protocols Stack. A-Review " IJEAT,ISSN:2249-8958,2012
9. Abu Hasnat Md. Riadul Alam, Md. Atiqur Rahaman Khan,Jia Uddin "Network Design and Performance Analysis of Geographical Routing Protocol in Mobile Ad-Hoc Network" ISBN:978-1-4799-0400-6/13© 2013 IEEE.
10. Pragya Gupta ,Sudha Gupta "Routing Protocols " International Conference on Advanced Computing& communicationTechnologies"ISBN:9780-0-7695-49415/13©2013 IEEE.
11. Ajinkya. D.Kadam, Prof. Sharad.S.Wagh "Evaluating MANET Routing Protocols Under Multimedia Traffic" ICCCNT-2013,IEEE-31661.
12. Mazhar H malik*,Qasim Always#, Mohsin Jamil** and Dhyani# "Performance Analysis of Proactive and Reactive Protocols in Mobile Ad-Hoc Networking:A Simulation based Analysis" ICREATE ,ISBN:978-1-4799-5132-1/14©2014 IEEE.
13. Changling Liu.Jorg Kaiser " A Survey of Mobile Ad Hoc Routing Protocols.
14. Shabana Habib, Somaila Saleem, Khawaja Muhammad Saqib " Review on MANET Routing Protocols and Challenges " Student Conference on Research and Development,ISBN:978-1-4799-2656-5/13 ©2013 IEEE.
15. Beigh Bilal Maqbool,Prof.M.A.Peer "Classification on Current Routing Protocols for AdHoc Networks-A Review" International Journal of Computer Application,ISSN:0975- 8887,2010.
16. Neeraj Arora and Dr. N.C.Barwar "Evaluation of AODV,OLSR and ZRP RoutingProtocols under Black hole attack" IJAIEM,ISSN:2319-4847,2014.
17. Harjeet Kaur, Manju Bala, Varsha Sahul " Performance Evaluation of AODV,OLSR and ZRP Routing Protocols under the Black hole Attacks in MANET" IJAREEIE,ISSN:2278-8875,2013.
18. P. Sankareswary, R. Suganthi and G. Sumathi "Impact of Selfish Nodes in Multicast Ad Hoc On demand Distance Vector Protocol" ICWCSC, IEEE, 2010.

Parminder Kaur has completed her B.Tech in Computer Science and Engineering in 2013 from Baba Farid group of institutions, Bathinda, Punjab. She is currently pursuing her M.Tech in Computer Science and Engineering at Shaheed Bhagat Singh State Technical Campus Ferozepur.Her area of interest is Networking.

Monika Sachdeva has completed her PhD in Network security at GNDU Amritsar. She has done her M.S in Software System at BITS Pilani .She has completed B.Tech in Computer Science and Engineering at GNDU Amritsar. Her area of interest is Networking.

Gagandeep has done his M.Tech in Computer Science and Engineering at Shaheed Bhagat Singh State Technical Campus Ferozepur. He is done his BTech in Computer Science and Engineering at Shaheed Bhagat Singh State Technical Campus Ferozepur. His area of interest is networking.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.