Algorithm to Detect and Overcome the Black Hole Attack in MANETs

Heta Changela
PG Scholar, Computer Engineering,
RK University
Rajkot, Gujarat, India

Amit Lathigara
HOD – Department of Computer Engineering,
RK University
Rajkot, Gujarat, India

ABSTRACT
In Mobile ad-hoc network to resolve security or any other issue, broadcasting is the common factor in networking. MANETs is very new concept and gives us to very different direction to the internet and when we use it, it will become reduce the cost of both the network i.e. with infrastructure and infrastructure less networks. Mobile Ad-hoc network not need backbone infrastructure support and easy to detect in wireless ad-hoc network is very reliable and also contains the routable networking environment in MANETs. In our paper, the effect of black hole attack in AODV based network is studied. The network parameters like Throughput, Packet Delivery Fraction (PDF) and Average End to End Delay are calculated with normal network (without black hole) and a network with one black hole. The performance of network parameters are compared in all the three scenarios. We proposed some scheme is able to finding string of single malicious nodes which drops all the packets.

Keywords
MANET, Black hole Attack, AODV

1. INTRODUCTION
A mobile ad hoc network (MANET) is a continuously self-construct, infrastructure-less network in which mobile devices connected without wires. It is collection of devices with wireless communication. [2] MANET is very popular in few years and wireless network is become very famous topic and it become very popular from past few decades, if we talk about when it be- come popular then it is within the 1990s. When they are just go through the mobility. As some fresh topic in the MANETs the mobile devices are become more interesting and well liked, in communication wireless network is most active field for researching. Mobile ad-hoc network has bright future there are still many issues regarding security or any other factor. [3]

There are many routing protocols are available for the MANETs some of them categorized into proactive routing protocol and reactive routing protocols. In proactive approach to the MANETs routing has to maintain all the information regarding routing continuously. The full network should be acknowledged to all nodes. Each and every node knows the path which is having pre-established path. There is no initial delay in communication but the results should be in terms of overhead of routing traffic. In reactive protocols routes are initiated when it is needed. It has to follow the appointed routes when it needed. If a node in the network wants to communication with a nodes which are in the network to which has no route to destination, the routing protocol will try to establish such a route which will reach to the destination. [1] It is called on demand routing protocol. Black hole attack is replies to each and every node that it has shortest path. This is the way to redirect all the network traffic to the malicious node and this the way for discarding the packet. [2]

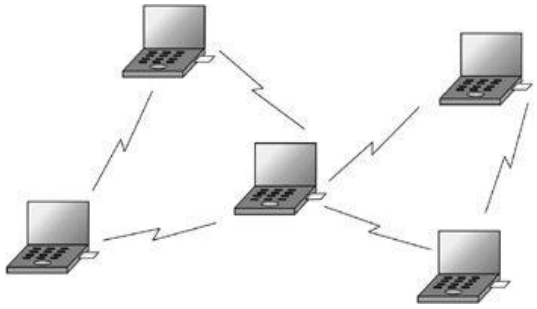

Fig. 1 Mobile Ad-hoc Network

There are many type of protocol which is categorized into proactive routing protocol, reactive routing protocol and hybrid routing protocol. In routing a mechanism like topology is updated constantly and will maintain the routing information constantly. In network every node knows the path to reach the other nodes. In network if a node wants to communicate with node but in actual the node does not have the path to destination, and protocol initiate the path when it needed called reactive routing protocol. [6]

2. BLACK HOLE ATTACK
In a Black hole attack, a node which is called malicious node will absorb all the network traffic towards them and discard all the packet. If we want to catch the black hole attack, when malicious node checking its routing table it directly send a fake RREP with largest sequence number and smallest hop count to prove that it has the minimum path to reach the destination. By this way we can catch the black hole node in the network. Source node gets the more than one RREP from the different node but it is choose the RREP from the malicious node because that has a largest sequence number. The source node ignores the RREP which are not coming from the malicious node and then malicious node drops all the packets rather better to forward further to the destination node. [4]

The malicious node takes all the route towards them and attack all the RREQ packet. Malicious node generates the fake RREP and that will be delivered to the source node that it does know the path for destination. By this way source node assumes that it is the next node to reach the destination so it will send the packet to the malicious node and malicious node will be remove all the packets which are comes from the source node. [11]

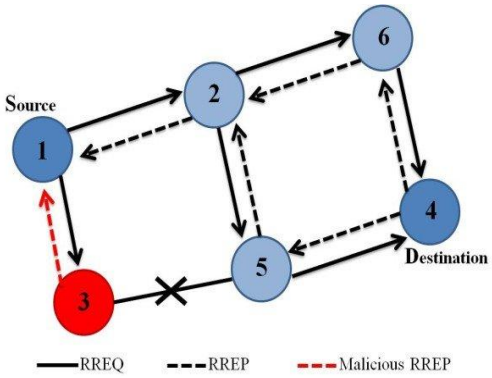

Fig. 2 Black Hole attack

Single black hole attack and Collaborative black hole attack are two types for the black hole attack. [8] In the network if all the network traffic is switched to single node, it is called single black hole attack which is malicious node and it will drops all the packets. In collaborative black hole attack, there are many malicious nodes which are work together to switch normal routing information towards the malicious node and assemble that route according to them. Some researchers had work on black hole attack and provide methods to detect malicious nodes but that is not sufficient to solve the black hole problem and the more detection method should be initiated to solve the black hole attack. [5]

3. AD-HOC ON DEMAND ROUTING PROTOCOL

Ad hoc On-Demand Distance Vector (AODV) Routing is a protocol which is working with mobile ad-hoc networks (MANETs) and every other network including wireless also. The AODV (Ad-hoc On Demand Distance Vector) routing protocol is a example for reactive routing protocol also called on demand. Routes are established as per the demand so it is called on demand routing vector. However, once established a route is maintained as well as they need to maintain the each entry in the routing table. Reactive routing protocols establish a path between the one to other node only when data to be exchanged and path will be established. In AODV, the network is not doing any work until a connection is needed. [9]

There are some control message specify for the AODV routing protocol, RouteRequest, RouteReply and RouteError. A source node is receiving multiple RREPs then the source node will choose the RREP with having minimum hop count. If HELLO packet was not received by any node consecutive three times, it concludes that the specific node will be down. If link is break and it detected then a Route Error (RERR) is sent. A route request is consider the parameters like source id, destination id, expiry date and broadcast id.

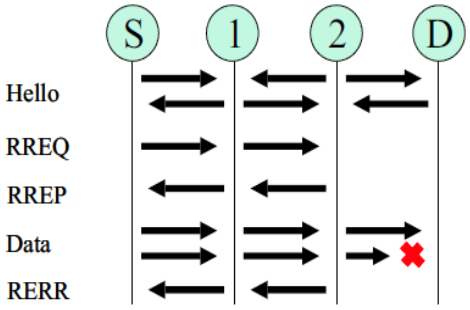

Fig. 3 AODV Routing Protocol

For detecting and counseling it's neighbor node Hello message is used. Hello messages are used then it is broadcast by some active node and it's all neighbor node are receiving the Hello message. From the neighbor node if a node is not able to receive the Hello messages., in result nodes sends continuously Hello message if a link break is detected. Here in AODV source node broadcast the RREQ to every node in the network. Source node will broadcast the RREQ, destination node will send return RREP to source node via neighbour node and source node receive RREP and path will complete.

4. RELATED WORK

Watchara Saetang and Sakuna Charoenpanyasak [9] in his work has proposed to used credit. Credit Acknowledgment (CACK) is used to reduce n increase the credit. A node can not receive CACK than credit will be decrease. The node will be untrusted and mark as a blacklist, when a credit reaches zero.

Kozma W,Lazos L [14] in his work has proposed this scheme has three parameters (i) Audit phase (ii) Search phase and (iii) Identification phase. This all phase work in different way first phase called audit phase in this phase it has to power to verify the node whether it has the audit for the node or not if node is audited then it will forwards the data packet to the destination node. If node is audited then it identify or it proves that packets are forwarded by itself. Audit phase also mainly contain some other parameter like First send an audit request second is to build the proof for packet forwarded by it and the last one is to be analysis the process how it built the proof for forwarded packet. Main second phase is verify that from which link packets are to be dropped by the node. After verifying the node mark node as misbehaving node and compare with others and it records only information about the transmission packets. It is purely for the single black hole attack it is not compatible with collaborative black hole attack.

Watchdog Mechanism [15] is used ,it keep track record of two table pending packet table and node rating table. Both the table contain the information about the source node, destination node, next hop count unique packet id etc. In packet pending table it name suggest that the packet is still in queue then what are the parameter it should contains , it has it's own unique packet id or address for the very next node also records the when packet to be forwarded and where packet should go. In node rating table it contains the information about the dropped packet. If we calculate the ratio between forwarded packets and dropped packet and if it is more then threshold value then mark the node as malicious node and his misbehave value is 1 else node is not malicious node and mark value as 0.

Payal N. Raj, Prashant B. Swadas [17] in thier work have proposed In normal AODV work based on sequence number. If RREP packet has RREP_Seq_No greater than the present value in the routing table. One control packet is used called ALARM packet and it has already a black list node so it avoids the RREP which is coming from the node which are in black list node. ALARM packet has already the list so it is easy to compare RREP and discard the RREP from that particular node. Update the threshold value after any node receiving the RREP packet. Node receive the RREP then it has the simplified value of threshold. Packet delivery ratio is higher in this method tan the original AODV but routing overhead is higher.

Tamilselven L and Sankaranarayanan [12] in his proposed work the sequence number of source node and the sequence number of the node from which RREP is initiated in Route Reply and Request Reply table in which the malicious node has highest sequence number. If difference is too high, then consider that node as malicious one, and it will discarded from the network.

Sonal,Kiran Narang [16] in their proposed work, IDS is used based on two factors packet loss rate and data rate. Fuzzy logic is use to solve this problem. The algorithm is based on priority, first we define the N number of nodes. Priority define by following step 1) packet loss is very low and data rate is very high set high priority 2) packet loss is medium and data rate is high set medium priority 3) Packet loss and data rate both low set low priority.

Al-Shurman M, Yoo S, Park S[18] in their proposed work they have two approach, First approach is Sender node will utilize the authenticity of the RREP packet. If sender find safe path to reach the destination after that buffered packet will be transmitted. Another approach is called unique sequence number in this keep record from last sequence number for last packet to be sent. Tables are updated constantly when any transmission has begun or end. Intermediate node has route to destination then it will sent the RREP to source node along with last packet sequence number.

Nital Mistry et al. [19] in his proposed work he added a new table called new timer is used MOS_WAIT_TIME and a new table called RREP table is initiated and a variable called malicious node in original AODV routing protocol. A source node send first RREP Packet after receiving the RREP control message is apply in given time period called RREP_WAIT_TIME. MOS_WAIT_TIME is half the value of RREP_WAIT_TIME. Parameters like PDR, End-to-End delay to be affected by applying this mechanism and it will better then the black hole attack.

5. PROPOSED SCHEME

In our proposed work we use two way handshaking mechanism. After receiving the RREQ from the source node to destination node first sends the RREQ_ACK to the source node to check whether it has valid route or not and AODV discovers route using reserve route discovery procedure. This proposed method is based two-way handshaking. We assume the network in which normal and malicious node both are presented. When process is initiated from source to destination node and it is looking for route to the destination node.

Communication begin with source node, it will broadcast the RREQ message to its neighbour nodes which are in the range and has valid the route to the destination because the route in the routing table is absence. All the address recorded the source node and check whether it has routing table for an active route to destination node. In absence of an active route to destination node the IN forwards RREQ to its neighbour node. A black hole node send RREP message after receiving the RREQ , It does not send RREQ-ACK.

If black hole node send RREP directly to source node without sending the RREP-ACK but in our work source node waiting for the RREP-ACK from the node who receives the RREQ. Hence the RREP message is terminated from the network. An intermediate node may receive the RREQ multiple times with the same broadcast id and same source address, RREQ message was broadcasted throughout the network.

When destination node receive the first RREQ instead of Uni-casting RREP back to source node it first generate the RREP-ACK and send it to its neighbour nodes which are in range towards the source node. This whole mechanism is similar to the unicast process of RREP. In network black hole node is not aware about this mechanism and it directly send RREP without verify router to destination. Routing table of source node will cached the RREP from black hole. We assume that if black hole node knows the router mechanism and it will start to send the RREP-ACK. The source node accept the RREP-ACK from the black hole node it does not send RREP to the node first it verify the DSN (destination sequence number) with Source Sequence number. f it is too high then simply discard RREP and assuming the first reply are from Black hole Node else accept the RREP and send the packets. This is how our mechanism is work in which detect the black hole node and remove from the network.

Table 1 Simulation Parameter

Simulator	Ns-2 (ver.2.35)
Simulation Time	100(s)
Number of Mobile Nodes	25, 50, 75, 100
Number of Black hole Nodes	1
Topology	1000m * 1000m
Routing protocol	AODV
Traffic	CBR
Pause Time	2(s)
Maximum Connection	5, 12,30,45
Packet Size	512 bytes
Maximum Speed	5m/s
Mobility Model	Random Waypoint

A. Performance Metrics

1) Throughput : The number of packets (bits) from sources that a destination receives in given time slots.

2) End-to-End Delay : A data will requires some time to transmit the data from source to destination node, it is called End-to-end delay.

3) Packet Delivery Fraction : PDF calculated in terms of ratio like it has ratio in between the no. of date packets delivered to the destination node and no. of data packets sent by the source node.

4) Normalize Routing Load : Total load of network route for transmitting data is required to find the total number of routing packet is delivered in the network to setup the path between source and destination.

B. Graph for Throughput

Throughput is very high in case of normal AODV routing protocol with our solution mode. In our proposed solution it does not allow the any malicious activity by the malicious

node. In black hole attack protocol It is suffer from the attacker node and the value of throughput is very low because malicious node is free do any activity and there is no any mechanism to prevent the black hole. So, in result throughput is very low in terms of black hole node and very high in normal AODV. We are successfully implemented our solution and increase the value of throughput in our solution.

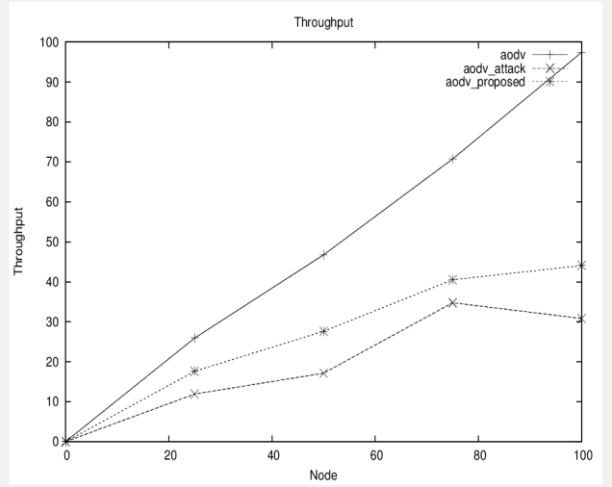

Fig 3 Throughput

C. Graph for Packet Delivery Fraction

Here in figure Packet Delivery fraction is analysis with black hole attack, without attack and in case of prevention scheme. The first observation is that in AODV protocol has a high packet delivery ratio as compared to black hole attack and with our prevention scheme. So, it is best route for data delivery. In black hole attack performance is very low it indicates the attacker behaviour. There is no any mechanism in attack to recover the data loss. In our proposed mechanism performance is increase as compare to black hole attack. Here apply the mechanism and try to decrease the data loss rate.

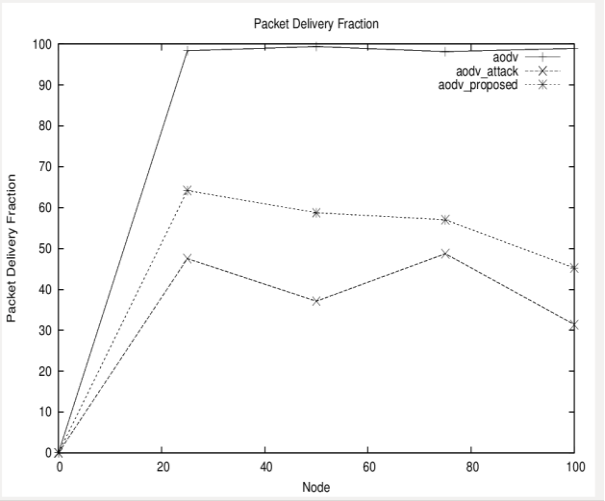

Fig. 5 Packet Delivery Fraction

D. Graph for End-to-End Delay

In graph it is display the effect of End-to-End delay in all three ways. In black hole attack node has find the safe path and it is affected by the attacker node. S, it is difficult to find the safe and attack free route. In our proposed solution it slightly differ from the normal AODV as the number of nodes increases. In AODV at one point it is become very high.

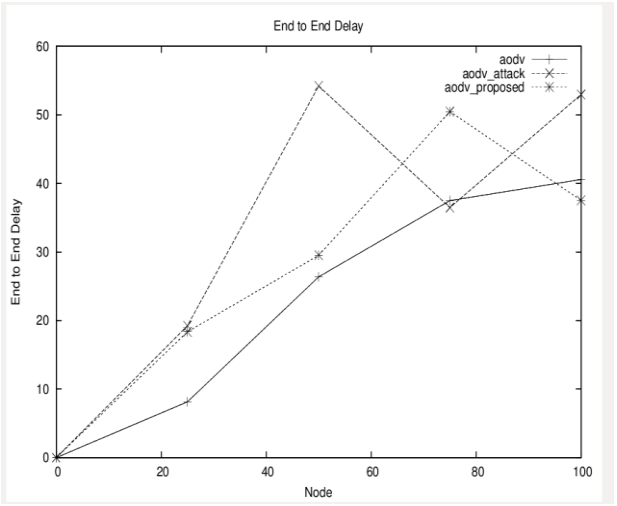

Fig. 4 End-to-End Delay

E. Graph for Normalize Routing Load

Normalized routing load is defines as the total number of routing packets are to be delivered in the network to set the path in between source to destination. In our prevention scheme Normalize routing load is very high as compare to others because it identify the path from source to destination node. In attack load is decrease as compare to without attack and our proposed scheme because it delivers minimum routing packet. In simple AODV it find the path between source to destination and after it delivered routing packets on that path.

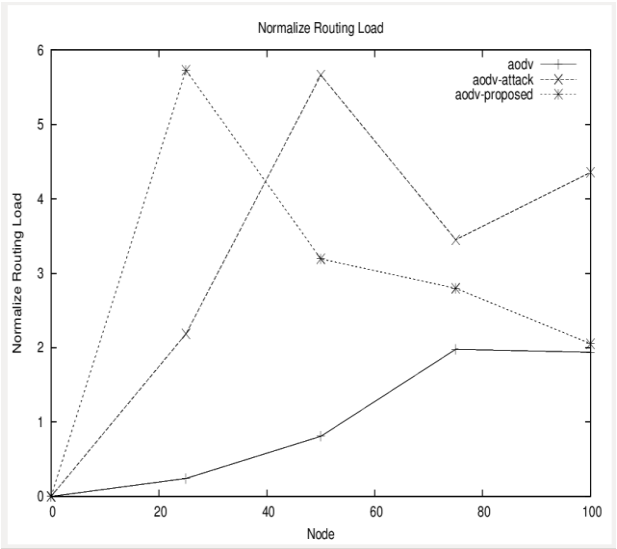

Fig. 5 Normalize Routing Load

6. CONCLUSIONS

Security for MANETs is major issue. In our work we have proposed a technique for black hole attack by using RREQ_ACK. If source node receive the RREQ_ACK then compare DSN and SSN value, if DSN greater than the SSN then discard that node from the quarantine list. With this scheme we compare some parameter like throughput, End-to-End delay and Packet delivery ratio. Throughput is increase as compare to attacker node and PDF will also increase. We can apply this proposed solution to identify and remove any number of black hole in a MANET and discover a safe path from source to destination by diverting the malicious nodes. In future we can study for the false feedback also go through

some other parameters and check the results with and without black hole attack. Performance of other protocols like GRP, TORA, DSR under these attacks in MANET can be taken as future work.

7. ACKNOWLEDGMENT

I would like to thank everyone who helped me in my research work. I would like to thank my supervisor Prof. Amit Lathigara. I am very happy that you gave me the opportunity to continue my research during last two years.

8. REFERENCES

[1] Ming-Yang Su, Kun-Lin Chiang, Wei-Cheng Liao " Mitigation of Black-Hole Nodes in Mobile Ad Hoc Networks" in *International Symposium on Parallel and Distributed Processing with Applications* 2010 *IEEE.*

[2] Gundeep Singh Bindra , Ashish Kapoor , Ashish Narang , Arjun Agrawal "Detection and Removal of Co-operative Blackhole and Grayhole Attacks in MANETs" *International Conference on System Engineering and Technology* september 11-12 2012.

[3] Mohamed A. Abdelshafy, Peter J. B. King "Analysis of Security Attacks on AODV Routing" 2013 *IEEE.*

[4] Monika Roopak , Dr. Bvr Reddy "Performance Analysis of Aodv Protocol under Black Hole Attack" *International Journal of Scientific & Engineering Research V*olume 2, Issue 8,August-2011.

[5] Sonia, Padmavati "Performance analysis of Black Hole Attack on Vanet's Reactive Routing Protcols" *International Journal of Computer Applications* Volume 73– No.9, July 2013.

[6] Ankur mishra , Ranjeet Jaiswal , Sanjay Sharma " A Novel Approach for Detecting and Eliminating Cooperative Black Hole Attack using Advanced DRI Table in Ad hoc Network" 2012 *IEEE.*

[7] Vishnu K, Amos J Paul "Detection and Removal of Cooperative Black/Gray hole attack in Mobile ADHOC Networks" *International Journal of Computer Applications* Volume 1 – No. 22 2012.

[8] Ravinder Kaur, Jyoti Kalra "A Review Paper on Detection and Prevention of Black hole in MANET" *International Journal of Advanced Research in Computer Science and Software Engineering* Volume 4, Issue 6, June 2014.

[9] Watchara Saetang and Sakuna Charoenpanyasak, "CAODV Free Blackhole Attack in Ad Hoc Networks" 2012 *International Conferenceon Computer Networks and Communication Systems* (CNCS 2012).

[10] Abhilasha Sharma, Rajdeep Singh, Ghanshyam Pandey "Detection and Prevention from Black Hole attack in AODV protocol for MANET" *International Journal of Computer Applications* Volume 50 – No.5, July 2012.

[11] Mangesh Ghonge , Prof. S. U. Nimbhorkar " Simulation of AODV under Blackhole Attack in MANET" *International Journal of Advanced Research in* Computer Science and Software Engineering Volume 2, Issue 2, February 2012.

[12] Tamilselven L and Sankaranarayanan, "Prevention of Black hole Attack in MANET" *International Conference on wireless Broadband and Ultra Wideband Communications*, 27-30 August 2007.

[13] Sushil Kumar Chamoli, Santosh Kumar, Deepak Singh Rana "Performance of AODV against Black Hole Attacks in Mobile ad-hoc Networks" *Computer Technology & Applications*,Vol 3 (4), 1395-1399. IJCTA July-August 2012.

[14] Kozma W,Lazos L,"REAct: Resource-Efficient Accountability for Node Misbehavior in Ad Hoc Networks based on Random Audits".Second *ACM* Conference on Wireless Network Security, Zurich, Switzerland, 16-18 March 2009.

[15] Amol A. Bhosle, Tushar P. Thosar and Snehal Mehatre, "Black- Holeand Wormhole Attack in Routing Protocol AODV in MAN *International Journal of Computer Science, Engineering and Applications (IJCSEA)* Vol.2, No.1, February 2012.

[16] Sonal,Kiran Narang "Black Hole Attack Detection using Fuzzy Logic" 2013 *International Journal Of Science and Research(IJSR)*,ISSN:2319-7064.

[17] Payal N. Raj, Prashant B. Swadas. "DPRAODV : A Dyanamic Learning System Against Blackhole Attack In Bodv Based Manet." *International Journal of Computer Science* Issues, Vol.2, 2009, pp 54-59.

[18] Al-Shurman M, Yoo S-M, Park S (2004) "Black Hole Attack in MobileAd Hoc Networks", Paper presented at the 42 nd Annual *ACM* Southeast Regional Conference (ACM-SE'42), Huntsville, Alabama, 2-3 April 2004.

[19] Mistry N, Jinwala DC, IAENG, Zaveri M (2010) "Improving AODV Protocol Against Blackhole Attacks". Paper presented at the *International MultiConference of Engineers & Computer Scientists*,Hong Kong, 17-19 March, 2010.