www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 4 Issue 8 Aug 2015, Page No. 13892-13899

Comparison of AOMDV With and Without Black Hole Attack

Ritika Sharma[1] , Bhawna Singla[2]
Computer Science and Engineering, N.C. College of Engineering, Israna
Panipat, India
[1]ritika.sharma268@gmail.com
[2]bhawna_singla@gmail.com

***Abstract*- The popularity of MANETS is increasing day-by-day as users choose to connect to a network irrespective of their geographical position. Because of this exceptional feature of MANETs, they are open to a huge amount of malicious activity. Black Hole attack is one kind of threat in MANETs in which the data of the network is routed towards a node which drops all the packets entirely. In this paper we propose a feasible solution to find and prevent black hole attack that can be implemented using AMODV protocol. Also, to develop simulations to analyze the performance of proposed solution based on various security parameters like Packet Delivery Ratio with and without black hole.**

Keywords: Mobile Ad-hoc Network (MANET), Routing Protocols,
Black Hole Attack, Ad hoc On-demand Multipath Distance Vector (AOMDV), Packet Delivery Ratio(PDR).

1. INTRODUCTION

One of the most critical problems in MANETs is the security vulnerabilities of the routing protocols. A set of nodes in a MANET may be compromised in such a way that it may not be possible to detect their malicious behavior easily. Such nodes can generate new routing messages to advertise non-existent links, provide incorrect link state information, and flood other nodes with routing traffic, thus inflicting Byzantine failure in the network. A new category of on-demand routing protocols for mobile ad-hoc network has been developed having the objective of minimizing the routing overhead. The key attribute of an on-demand protocol is the source initiated route discovery process. The on-demand protocols, multipath protocols have comparatively greater ability of reducing the route discovery frequency as compared to single path protocols. On-demand multipath protocols find out multiple paths between the source and the destination in a single route discovery. Therefore, a new route discovery is required only when all these paths fail. Routing is done by means of using the AOMDV routing protocol. AOMDV is based on a famous and well-studied on-demand single path protocol identified as ad hoc on-demand distance vector (AODV). AOMDV is an extension of the AODV protocol which discovers multiple paths between the source and the destination in all route discoveries. Multiple paths so computed are assured to be loop free as well as link disjoints. AOMDV also finds routes on-demand with a route discovery procedure. AOMDV depends in a great amount on the routing information previously available in the underlying AODV protocol, thus limiting the overhead incurred in finding multiple paths. Any special control packets are not required. Extra RREPs and RERRs for discovery and maintenance of multipath along with a few extra fields in routing control packets (i.e. RREQs, RREPs and RERRs) form the only added overhead in AOMDV relative to AODV.

2. BLACK HOLE ATTACK

The attacks could be of two types at the network layer- first is which does not forward any data or denies the service like black hole DOS attacks whereas the second can be the ones which selectively forwards the data but by modifies them like grey hole, worm hole or replay attacks. Black hole attack falls under the first type as it does not forward any data packet which is planned for the destination. The attacker interleaves itself into the direction from source to destination by conveying a false RREP containing higher Sequence number which gives an impression that it contains the freshest route towards destination. Thereafter the source will be captured into constructing a path via malicious node and rejecting all the other available paths. Later than, when the data packets are to be forwarded towards destination, the attacker just drops all of them and consequently destination will not receive yet a single piece of information.

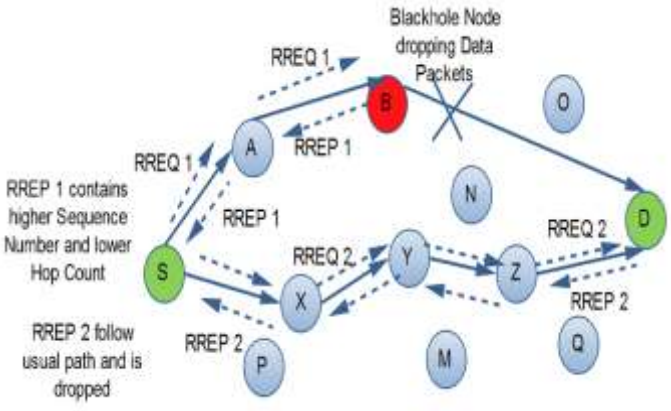


Figure.1 Black hole attack

3. Related work

DOI: 10.18535/ijecs/v4i8.50

DPRAODV Scheme

In this proposal, the authors had set up a threshold value for the sequence number. If the sequence number received is higher than the threshold value, then the sender node is considered as black hole node and then a blacklist is constructed with the attacker node. The scheme used a control packet called "ALARM" message to inform the neighboring nodes about this malicious node.

Discussion

DPRAODV increased the packet delivery ratio with supposed increase in routing overhead. This method was not able to detect the cooperative black hole attacks. The false detection ratio of this scheme was also high. The control packet overhead was also present due to extra "ALARM" messages and the transmission of these messages took considerable amount of time therefore taking longer before other nodes would get to know about the blacklist.

Distributed Cooperative Mechanism

In DCM method, the authors detected and alleviated the black hole nodes via a four step procedure. In the first phase, each node maintained an added table called estimation table which consisted of the assessment of credibility of each node based on the overhearing of packets. If a suspicion was found then the node entered the second phase of local detection in which it checked the partner cooperative node. If the inspection value was found to be negative then the node entered the third phase in which all one-hop neighbors were concerned in broadcasting about the credibility of that suspicious node. Finally, in the global reaction phase, the information was shared with all the nodes of the network and thus the black hole node was detached.

Discussion

The distributed and cooperative mechanism provided higher values of packet delivery ratio. However the routing control overhead was very high because multiple control packets were shared among nodes during second and third phase. In addition to phase three, the DCM involved a broadcasting procedure which accounted for a significant overhead. The complete four step process was time consuming thus resulted in high end-to-end delay.

Neighborhood Based Method

This proposal included the use of two additional control packets RQNS and RPNS. On receiving the RREP from more than one node the source will send RQNS to each of them and receive RPNS from them. The basic approach depends upon the difference between the neighbor sets. The source compared the received neighbor sets and if the difference between them was found to be greater than the threshold value the corresponding node was assumed to be black hole node .

Discussion

This scheme was highly efficient as it improved the throughput by 15% but it added to the routing control overhead by the introduction of two additional control packets. In addition after comparing the neighbor set, the actual detection of black hole node was done using a cryptographic method so that scheme was very costly and not feasible for the mobile ad hoc networks. The scheme was not able to detect the cooperative black hole attacks. This method failed in the scenario where the malicious node can forge fake RREPs.

Time-Based Threshold Detection Scheme

In this scheme, the basic idea was to check the time of receiving first route request with the timer threshold value. Every node after receiving first request sets the timer in "Timer Expired Table" and the subsequent requests was received until the timer expired. It stored the sequence number and the time at which route request arrived in "Collect Route Reply Table". After the timeout, it first checked its CRRT whether there was any same next hop node. If the next hop was repeated then it assumed that the path is safe i.e. does not contain any malicious node .

Discussion

Time-based mechanism delivered high packet delivery ratio with nominal routing overhead. The scheme was limited in use because if there were no repetition of next hop node then it would select random route from CRTT and there could be chances of black hole node being present over there. Also end-to-end delay would be raised when malicious node is away from source.

4. Ad-hoc On-demand Multipath Distance Vector (AOMDV)

***Protocol Overview*:**

A new group of on-demand routing protocol for mobile ad hoc network has been developed having the goal of minimizing the routing overhead. AOMDV has three fresh aspects in relation to other on-demand multipath protocols. Firstly, it does not have high inter-nodal coordination overheads. Secondly, it guarantees disjointness of alternate routes by means of distributed computation without using source routing. Thirdly, AOMDV computes alternate paths with minimal extra overhead over AODV, it does so by exploiting previously available alternate path routing information to the extent that is possible. AOMDV shares some features with AODV. It is based on the distance vector concept and makes use of hop-by-hop routing approach. In AOMDV, RREQ propagation from the source to the destination sets up multiple reverse paths at both intermediate nodes and the destination. Multiple RREPs pass through these reverse paths back to form multiple forward paths to the destination at the source and intermediate nodes. AOMDV also provides intermediate nodes with alternate paths because they are found to be useful in reducing route discovery frequency. The fundamental part of the AOMDV protocol lies in ensuring that multiple paths revealed are loop-free and disjoint, and also efficiently finding such paths via a flood-based route discovery. AOMDV route updating rules applied locally at each node plays an important role in maintaining loop-freedom and disjointness properties.

Based on the discussion above, we are formulating below a set of sufficient conditions for loop-freedom. These conditions permit multiple paths to be sustained at a node for a destination.

For maintaining multiple paths for the same sequence number, AOMDV uses the concept of an 'advertised hop count.' Each node preserves a variable called advertised hop count for every destination. The length of this variable is set to the 'longest' available path for the destination during the time of first advertisement for a particular destination sequence number. The advertised hop count is unchanged until the sequence number is changed. Advertising the longest path length allows more number of alternate paths to be maintained at a node for destination.

DOI: 10.18535/ijecs/v4i8.50

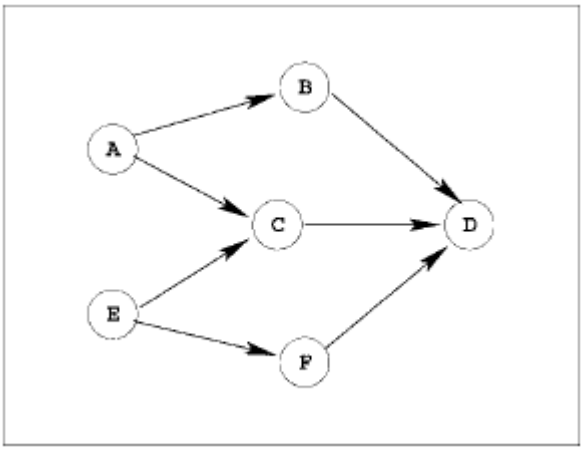
Sufficient Conditions

1. *Sequence number rule*: It maintains routes for the highest known destination sequence number only. For each destination, we limit that multiple paths maintained by a node have the same destination sequence number. This restriction maintains a loop freedom invariant like AODV. Once a route advertisement containing a higher destination sequence number is received, all routes corresponding to the older sequence number are discarded.
2. For the same destination sequence number,
   a. *Route advertisement rule:* Never advertise a route shorter than one already advertised.
   b. *Route acceptance rule:* Never accept a route longer than one already advertised.

To preserve multiple paths for the same sequence number, AOMDV uses the concept of an 'advertised hop count'. Each node maintains a variable called advertised hop count for every destination. The length of this variable is set to the 'longest' available path for the destination during the time of first advertisement for a particular destination sequence number. The advertised hop count remains unchanged till the sequence number is changed.

Disjoint Paths

AOMDV is used to discover node-disjoint or link-disjoint routes. To discover node-disjoint routes, each node does not reject duplicate RREQs instantaneously. Each RREQs arrive in by a different neighbour of the source defining a node –disjoint path. This is due to the reason that the nodes cannot broadcast duplicate RREQs, hence any two RREQs arriving at an intermediate node through different neighbour of source cannot traversed the same node. With an attempt to get multiple link-disjoint routes, the destination replies to duplicate RREQs, the destination only replies to RREQs arriving through unique neighbours. After the first hop, the RREPs pursue the reverse paths, which are node-disjoint and hence link-disjoint. The trajectories of each RREP might intersect at an intermediate node, although each takes a different reverse path to the source to guarantee link disjointness.



Paths maintained at different nodes to a destination might not be mutually disjoint. At this juncture *D* represents the destination. Node *A* has two disjoint paths to *D*: *A – C – D and A – B – D*. Correspondingly, node *E* has two disjoint paths to *D*: *E – F – D and E – C – D*. But the paths *A – C – D* and *E – C – D* are not disjoint since they share a common link *C – D*.

PROTOCOL DESCRIPTION

AOMDV protocol is expressed in four components: routing table, route discovery, route maintenance and data packet forwarding.

Routing Table

AOMDV route table entry maintains a new field for the advertised hop count. Also a route list is used in AOMDV for storing extra on formation for every alternate path including: hop count , next hop, last hop, and expiration timeout. Last hop information is useful in checking the disjointness of alternate paths.

Consider a destination d and a node i. Every time the destination sequence number for d at i is updated, the corresponding advertised hop count is initialized. Assume for a given destination sequence number, let hop count$^{d}{}_{ik}$ represent the hop count of k th path (for some k) in the routing table entry for d at i, i.e. (next hop$^{d}_{ik}$, last hop$^{d}_{ik}$, hop count$^{d}_{ik}$) $\in$ route list$^{d}_{i}$.

Rout Discovery

Like AODV, every time a traffic source wants a route discovery process it generates RREQs. Since the RREQs are flooded network-wide, a node may receive some copies of the same RREQ. All duplicate copies are examined in AOMDV for possible alternate reverse paths, yet reverse paths are created by means of only those copies that preserve loop-freedom and disjointness amongst the resulting set of paths to the source. Whenever an intermediate node obtains a reverse path using a RREQ copy, it checks if there are one or more valid forward paths to the destination. If so, node generates a RREP and sends it back to the source along the reverse path; the RREP includes a forward path that was not used in any previous RREPs for this route discovery. The intermediate node does not propagate the RREQ further. Or else, the node re-broadcasts the RREQ copy if it has not earlier forwarded any other copy of this RREQ and this copy results in the formation/updation of a reverse path. When destination receives RREQ copies, it also forms reverse paths in the same manner as intermediate nodes. The destination generates a RREP in response to every RREQ copy that arrives through a loop-free path to the source although it forms reverse paths by means of only RREQ copies that arrive through loop-free and disjoint alternate paths to the source. The RREQ flooding mechanism, where all node locally broadcasts a RREQ once, suppresses a few RREQ copies at intermediate nodes

Route Maintenance

Route maintenance in AOMDV makes use of RERR (Route Error) packets. Whenever a link breaks it then displays a RERR message, where it lists each of those lost destinations. The node sends the RERR upstream in the direction of the source node. If there are several previous hops that were using this link, the node broadcasts the RERR; otherwise, it uncast. Whenever a node receives a RERR, it initially checks whether the node that sent the RERR is its next hop to any of the destination listed in the RERR. If the sending node is the next hop to any of these destinations, the node invalidates these route tables and then propagates the RERR back towards the

DOI: 10.18535/ijecs/v4i8.50

source. The RERR continues to be forwarded in this manner until it is received by the source. Once the source receives the RERR, it can re-initiate route discovery if it still requires the route.

3.4. Data Packet Forwarding

For data packet forwarding at a node having multiple paths to a destination, we adopt a simple approach of using a path until it fails and then switch to an alternate path; we use paths in order of their creation. In other alternative, alternate paths are used simultaneously for load balancing where data packets are distributed over the available paths, thereby improving the network utilization and end-to-end delay.

5. Proposed Algorithm (BAOMDV)

In this, section the proposed mechanism for defending against a black hole attack is presented. The mechanism introduces two concepts,

(i) data routing information (DRI) table and

(ii) cross checking.

A. Data Routing Information

In the proposed scheme, two bits of additional information are sent by the nodes which respond to the RREQ message of a source node during route discovery process. Each node maintains an extra data routing information (DRI) table. In the DRI table, the bit 1 represents 'true' and the bit 0 represents 'false'. The first bit 'From' represents the information on routing data packet *from* the node (in the *Node* filed), while the second bit 'Through' represents information on routing data packet through the node (in the *Node* field).

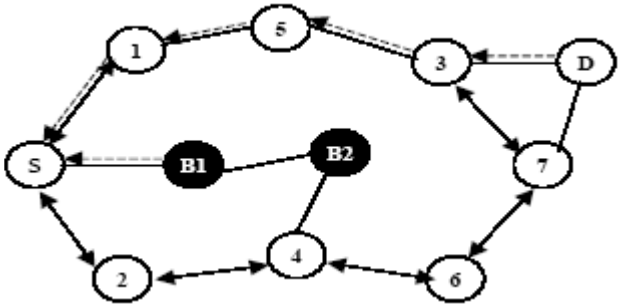


Figure.2 Propagation of RREP messages

A sample database preserved by node *4* is shown in Table1. The entry 1 0 for node *3* means that node *4* has routed data packets from *3*, however has not routed any data packets through *3* (before node *3* moved away from *4*). The entry 1 1 for node *6* means that, node *4* has successfully routed data packets from and through node *6*. The entry 0 0 for node *B2* means that, node *4* has not routed any data packets from or through *B2*.

Node #	Data Routing Information	
	From	Through
3	1	0
6	1	1
B2	0	0
2	1	1

Table1. DRI table maintained in node 4

B. Cross Checking

The proposed method depends on reliable nodes (nodes through which source has routed data before and knows them to be trustworthy) to transfer data packets. The BAOMDV protocol and the algorithm for the proposed mechanism are depicted in Fig. 3. In the customized protocol, the source node (SN) broadcasts a RREQ message to find out a secure route to the destination node. The intermediate node (IN) that generates the RREP has to provide information concerning its next hop node (NHN) and its DRI entry for that NHN. Upon receiving the RREP message from IN, SN will check its own DRI table to see whether IN is its reliable node. If SN has used IN previously for routing data packets, then IN is said to be reliable node for SN and SN starts to route data through IN. If not, IN is unreliable and hence SN sends FRq message to NHN to verify the identity of the IN, and asks NHN about the subsequent information:

(i) whether IN has routed data packets through NHN,

(ii) who is the next hop of current NHN to destination, and

(iii) whether the current NHN routed data through its own next hop.

The NHN, in return, responds with FRp message together with the subsequent responses:

(i) DRI entry for IN,

(ii) the information about its (NHN's) next hop node, and the DRI entry for its (NHN's) next hop.

On the basis of the FRp message from NHN, SN verifies if NHN is reliable or not. If SN has routed data through NHN previously, NHN is reliable; Or else, NHN is unreliable for SN. If NHN is reliable, then SN checks whether IN is black hole node or not. If the second bit of the DRI entry from the IN is equal to 1,which means IN has routed data *through* NHN, and the first bit of the DRI entry from the NHN is equal to 0 which means NHN has not routed data from IN, then IN is said to be a blackhole. If IN is not a blackhole node and NHN is a reliable node, then the route is secure, and SN will update its DRI entry for IN with 0 1, and starts routing data via IN. If IN is a blackhole, then SN identifies all the nodes along the reverse path from IN to the node that generated the RREP as blackhole nodes. Subsequently SN ignores any other RREP from the blackholes and broadcasts the list of cooperative blackholes in the network. If NHN is an unreliable node, SN treats current NHN as IN and sends FRq to the updated IN's next hop node and goes on in a loop from steps 7 through 24 in the algorithm.

DOI: 10.18535/ijecs/v4i8.50

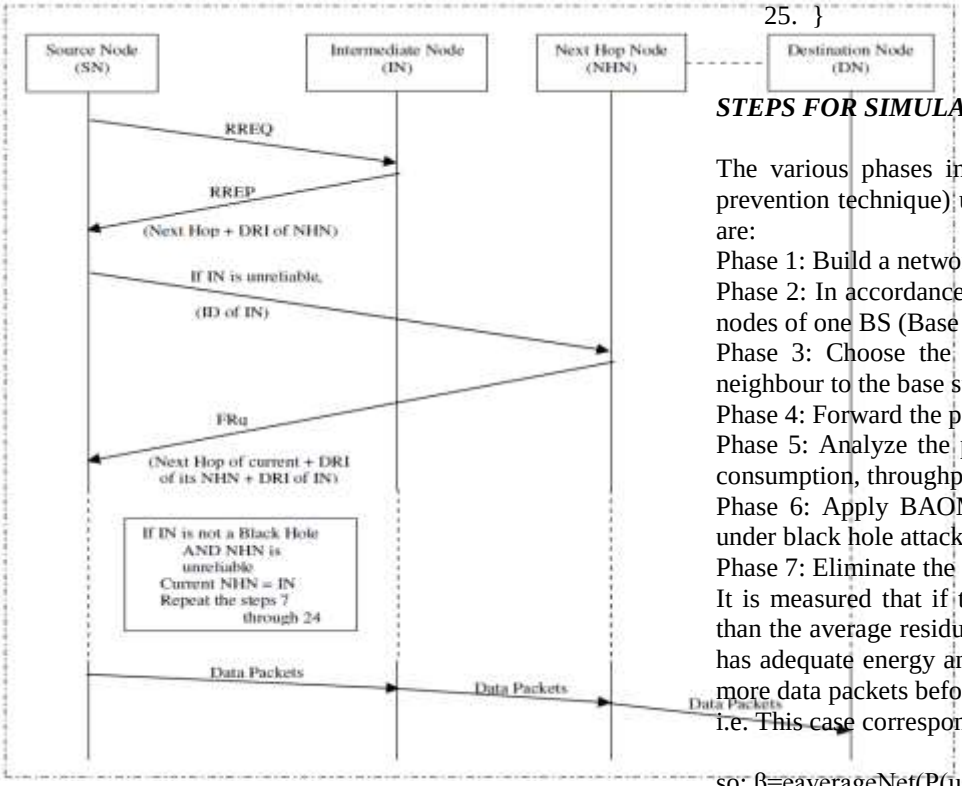


Figure.3 BAOMDV protocol to prevent Black hole

Algorithm:

Notations:
SN: Source Node IN: Intermediate Node
DN: Destination Node NHH: Next Hop Node
FRq: Further Request FRp: Further Reply
Reliable Node: The node through which the SN has routed data
DRI: Data Routing Information
ID: Identity of the node

1. SN Broadcasts RREQ
2. SN receives RREP
3. IF (RREP id from DN or a reliable node){
4. Route data packets(Source Route)
5. }
6. ELSE{
7. Do{
8. Send FRq and ID of IN to NHH
9. Receive FRq. NHH of current NHH. DRI entry for
10. NHN's next hop. DRI entry for current IN.
11. If (NHN is a reliable node){
12. Check IN for black hole using DRI entry
13. If (IN is not a black hole node)
14. Route Data Packets(Secure Route)
15. ELSE(
16. Insecure routes
17. IN is a Black hole
18. All the nodes along the reverse path from IN to the node
19. that generated RREP are black hole
20. }
21. }
22. ELSE
23. Current IN = NHN
24. } While (IN is NOT a reliable node)
25. }

STEPS FOR SIMULATION

The various phases in the BHDPT (black hole detection & prevention technique) using AOMDV & BAOMDV algorithm are:
Phase 1: Build a network of N nodes.
Phase 2: In accordance with given range, describe the member nodes of one BS (Base station).
Phase 3: Choose the neighbour member of nodes which is neighbour to the base station.
Phase 4: Forward the packets from one node to another node.
Phase 5: Analyze the parameters such as routing total energy consumption, throughput for all nearest node.
Phase 6: Apply BAOMDV to detect whether the network is under black hole attack or not.
Phase 7: Eliminate the attack
It is measured that if the residual energy of a node is greater than the average residual energy of the network, then this node has adequate energy and has a high probability of transmitting more data packets before being exhausted.
i.e. This case corresponds to $(w(uj) \geq \beta)$,

so: β=eaverageNet(P(u0,un))……1

As a result, TNet=∏j=1Kα*w(uj)β≤ak, and we achieve the following:

α≥(TNet)1/K
……..2

Following Equation 1, we achieve
α<βw(uj) ……3

Steady-state probabilities could be solved. To solve the value of steady-state probabilities, transition probability values are set as follows: pa = 0.4; pm = 0.3; pe = 0.5; pi = 0.6.'

Simulation Validation

For the validation of the setup of the system under test in MATLAB 2013Ra, a segment of the experiment is conducted with the implemented Black Hole simulation models. Cai's experimentation concerned simulating a Black Hole attack for AOMDV of 50 nodes with 100 iteration in a 100m2 area. The number of Black Holes in the network was a factor with selected levels as powers of 5.

Design Validate

The validation is conducted using simulation for each Black Hole simulation model and for all Black Hole levels. Each factor level arrangement is replicated 100 times to obtain the average packet loss percent for the given levels. The results are revealed in comparison to Cai's original. The data shows that the AOMDV Black Hole models display similar growth in packet loss as the number of Black Hole nodes is increased. Yet, there is an observable performance of the AOMDV Black Hole attacks.

DOI: 10.18535/ijecs/v4i8.50

Given r replications, *Packet Loss Percentage is*

$$\text{Packet Loss Percentage} = \frac{\sum_{i=1}^{r} \frac{\mu_{D,i}}{\mu_{S,i}}}{r}$$

Determining Number of Reproductions (RREP)

To account for random variation, the experiment is repeated a number of times using different random seeds to calculate approximately the mean of each response variable. Conversely, if the experiment is not repeated enough times, considerable sampling bias is inserted into the data, making it complex to justify conclusions on the data collected.
A familiar approach to determine a reasonable number of replications:
1. Approximate a good number of replications.
2. Run the experiment with the intention that multiple groups of replications can be generated.
3. Find out the confidence intervals of response variables for each replication group.
4. Convert the root of black hole node from single network area.

6. SIMULATION SCENARIO

In the beginning a network is created with a blank scenario with the help of startup wizard. Initial topology is chosen by creating the empty scenario and network scale is preferred by selecting the network scale. In our case campus is selected as our network scale. Size of the network scale is particular by selecting the X span and Y span in known units. We have preferred 100 * 100 meters as our network size. Additional technologies are specified which are used in the simulation. We have preferred MANET model in the technologies. Hereafter the manual configuration, different topologies can be generated by dragging objects from the palette of the project editor workspace. After the design of network, nodes are properly configured manually.

SIMULATION PARAMETERS	
Examined Protocol	ADOMDV, BAOMDV
Simulation Time	1000 seconds
Simulation area(m*m)	100*100
Number of Nodes	14,25
Traffic Type	TCP
Performance Parameter	Packet Delivery Ratio
Pause time	100 seconds
Mobility(m/s)	100 meter/second
Packet Inter-Arrival time(s)	Exponential(1)
Packet Size(bits)	Exponential(124)
Transmit Power(W)	0.008
Data Rate(Mbps)	15Mbps
Mobility Model	Random waypoint

7. RESULT

The AOMDV protocols are implemented using MATLAB2013a software to stimulate the network. The performance of using AOMDV protocols are related with and deprived of multiple based stations on numerous network parameters.

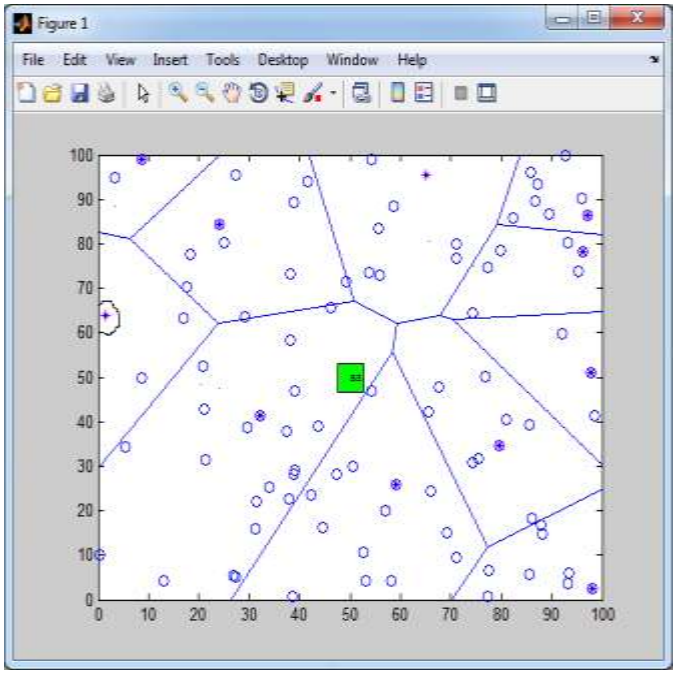


Figure 1: Black hole detection at unbound distance from one zone to another zone

Figure 2 shows the exact positions of the black holes in the MANET network. The first malicious node frontwards the packet by the essential communicate power to mislead two nodes backward. The second malicious node drops the packet; despite the fact that the attack is detected by the last node prior than the black holes. The omitted transmission is represented by a circle in Figure1.

DOI: 10.18535/ijecs/v4i8.50

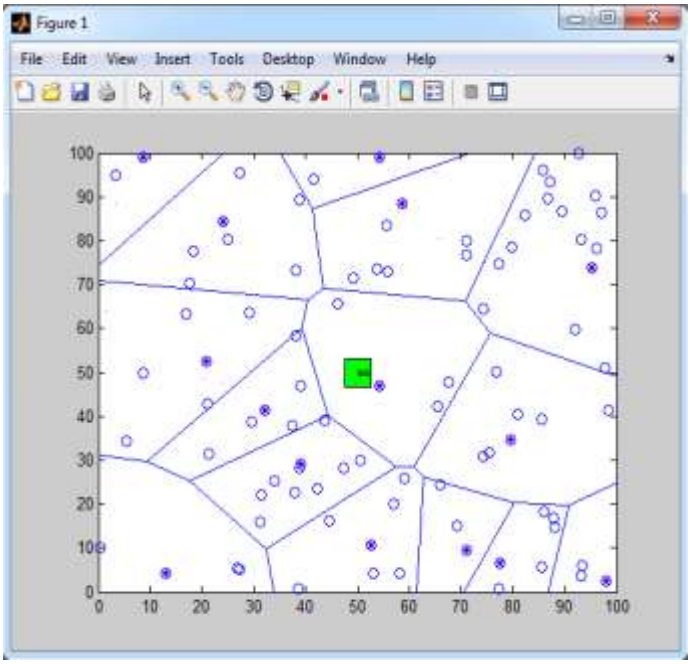


Figure 2. Black hole prevention by AOMDV

In a MANET, successful packet delivery to the BS is on the whole more compulsory than the prevention of data to be taken by an attacker.

Node 1 sends RREQ Secure Multipath to node 3
Node 1 sends RREQ Secure Multipath to node 4
Node 1 sends RREQ Secure Multipath to node 5
Node 1 sends RREQ Secure Multipath to node 7
Node 1 sends RREQ Secure Multipath to node 8
Node 1 sends RREQ Secure Multipath to node 9
Node 1 sends RREQ Secure Multipath to node 14
Node 1 sends RREQ Secure Multipath to node 15
Node 1 sends RREQ Secure Multipath to node 16
Node 1 sends RREQ Secure Multipath to node 17
Node 1 sends RREQ Secure Multipath to node 20
Flag= 1
Node 20sends RREP to node 1
Node 1
Sends message to node 20

Our objective was to determine the protocol which has low vulnerability for black hole attack taking AOMDV and BAOMDV routing protocols. The three performance parameter network load, delay and throughput is taken into consideration. Our objective was to study the effect of black hole on AOMDV and BAOMDV through analyzing how much performance of the network has been compromised.

Taking into account the delay of the network in mind the performance in the existence of a single black hole node is analyzed. Likewise the performance parameters that is throughput and network load shows the amount of network performance that has been affected by the presence of black hole node.

For throughput taking into consideration low traffic (low load) of BAOMDV, the performance in the presence of a malicious node is comparatively low with comparison to AOMDV due to its less routing forwarding and routing traffic.

Black hole node discards the data which is routed to it. Or we can say that the outcome of black hole attack is packet loss of almost all the data sent from source to destination.

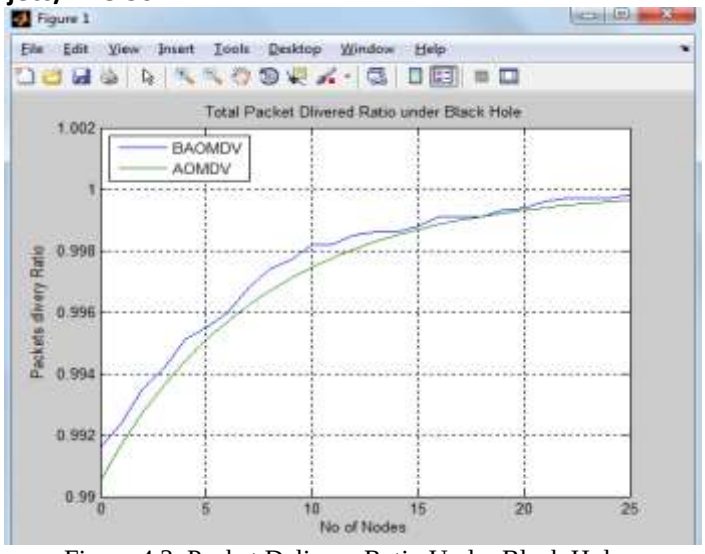


Figure 4.3. Packet Delivery Ratio Under Black Hole

It can be seen that without black hole the packet delivery ratio of AOMDV and BOMDV are comparable.

In figure 3, it can be seen that AOMDV is more affected by black holes. AOMDV produces less of Packet delivery ratio than BAOMDV. As the number of black hole node increases, there is a decrease in packet delivery ratio in both the protocols. But, BAOMDV produces more amount of packet delivery ratio than AOMDV.

After analyzing the vulnerability of both protocols i.e. AOMDV and BAOMDV in terms of low network traffic and high network traffic, results shows that AOMDV is more affected by the black hole node.

On the basis of our research and analysis of simulation results, it can be observed that AOMDV is more open to Black Hole attack than BAOMDV.

8. CONCLUSION AND FUTURE WORK

MANET is one of main feature for its extension. In this thesis, we have analyzed the behavior and challenges of security threats in Mobile Ad Hoc Networks with a solution finding technique. The results obtained from simulation are analyzed in great depth so as to draw the final conclusion. Different mitigation plans are studied in detail and we come up with mitigation plan that suits best to eliminate Black Hole attack. The performance of routing protocols in MANET on a large scale depends on type of attacks. One of such attacks is a black hole attack. The results of simulation have shown that the attack has huge effect on AOMDV protocol. In this case, on the basis of the number of attacker, the Packet Delivery Ratio is either high or low. If the number of attacker increases, the Packet Delivery Ratio is low due to black hole attack.

A lot of research work is still required in this area. We tried to find out and analyze the impact of Black Hole attack in MANETs using AOMDV and BAOMDV protocols. They can be categorized on the basis of how much they affect the performance of the network. We wish to introduce one model that can detect this kind of attack. In case, because of dynamic topology for this network, we must use a dynamic model.

DOI: 10.18535/ijecs/v4i8.50

REFERENCES

[1]. C.E.Perkins and E.M.Royer, "Ad-Hoc on Demand Distance Vector Routing", Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, pp.90-100, Feb, 1999.

[2]. C.Jiwen, Y.Ping, C.Jialin, W.Zhiyang, L.Ning, " An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network",24th IEEE International Conference on Advance Information Networking and Application (AINA 2010), pp. 775-780, April,2010.

[3]. Z.J.Hass, M.R.Pearlman, P.Samar, "The Zone Routing Protocol (ZRP) for Ad Hoc Networks", 55th Proceeding of International task force, July, 2002.

[4]. S. Kurosawa, H.Nakayama, N.Kato, A.Jamalipour, Y.Nemoto, "Detecting Blackhole Attack on AODV- Wireless sensor Networks by Dynamic Learning Method", International Journal of Network Security, Vol. 5, No.3, pp. 338-346, Nov, 2007.

[5]. K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, E.M. Belding Royer, "Secure routing protocol for Ad-Hoc networks", In Proc. of 10th IEEE International Conference on Network Protocols, Dept. of Computer Science, California Univ., Santa Barbara, CA, USA. Pp.78- 87, ISSN: 1092-1648, Nov. 2002.

[6]. H. Deng, W. Li, Agrawal, D.P., "Routing security in wireless Ad-Hoc networks", Cincinnati Univ.,OH, USA; IEEE Communications Magazine, , Vol.40, pp.70- 75, ISSN: 0163-6804, Oct. 2002.

[7]. M.T.Refaei, V.Srivastava, L.Dasilva, M.Eltoweissy, "A Reputation-Based Mechanism for Isolating Selfish nodes in Ad-Hoc Networks", Second Annual International Conference on Mobile and Ubiquitous Systems, Networking and Services, pp.3-11, July, 2005.

[8]. Zhu, C. Lee, M.J.Saadawi, T., "RTT-Based Optimal Waiting time for Best Route Selection in Ad-Hoc Routing Protocols", IEEE Military Communications Conference, Vol. 2, pp. 1054-1059, Oct, 2003.

[9]. H.L.Nguyen, U.T.Nguyen, "Study of Different Types of Attacks on Multicast in Mobile Ad Hoc Networks", International Conference on System and Networks and International Conference on Mobile Communications and Learning Technologies (ICN/ICONS/MCL 2006), pp.149-149, April, 2006.

[10]. West off, D., Paul K, "Context Aware Detection of Selfish Nodes in DSR based Ad Hoc Networks", IEEE GLOBECOM.Taipei, Taiwan, pp. 178-182, 2002.

[11]. Y.F.Alem, Z.C.Xuan, "*Preventing Wormhole Attack in Mobile Ad-hoc Networks Using Anomaly Detection",* 2ndInternational Conference on Future Computer and Communication (ICFCC 2010), Vol. 3, pp. 672-676, May,2010.

[12]. M.Parsons, P.Ebinger, "*Performance Evaluation of the Impact of Attacks on mobile Ad-Hoc Networks*" April. 10, 2010.

[13]. Rashid Hafeez Khokhar, Md Asri Ngadi and Satira Mandala, "*A Review of Current Routing Attacks in Mobile Ad Hoc Networks",* International Journal of Computer Science and Security, pp. 18-29, Volume-2 Issue-3, 2009

[14]. Mr. L Raja, Capt. Dr. S SanthoshBaboo "Comparative study of reactive routing protocol AODV, DSR, ABR and TORA" in International Journal Of Engineering And Computer Science Vol 2 Issue 3 March 2013 Page No. 707-718

[15]. C.Sivaram murthy, B.S. Manoj, *Adhoc wireless networks: Architectures, and protocols*, Pearson Education, 2004.

[16]. Aarti and Dr. S.S Tyagi, *"Study of MANET: Characteristics, Challenges, Application and Security Attacks",* IJARCSSE International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, May 2013

[17]. Mohit Kumar and Rashmi Mishra ―*An Overview of MANET: History, Challenges and Applications*‖, Indian Journal of Computer Science and Engineering (IJCSE), Vol. 3 No. 1 Feb-Mar 2012.

[18]. Dr. Kamaljit I. Lakhtaria, *Analyzing Reactive Routing Protocols in Mobile Ad Hoc Networks, Int. J. Advanced Networking and Applications* Volume:03 Issue:06 Pages:1416-1421 (2012) ISSN : 0975-029

[19]. Sunil Taneja and Ashwani Kush, ―A *Survey of Routing Protocols in Mobile Ad-Hoc Networks*‖, International Journal of Innovation Management and Technology, Volume 1, No3, 279-285, August 2010.

[20]. Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao " *A survey of black hole attacks in wireless mobile ad hoc networks"* Human-centric Computing and Information Sciences 2011.