Achieving High Reliability in SAODV by Decreasing False Positive Blackhole Detection Rate in MANET

Yudhister Chawla[1], Dr. Hardayal Singh Shekhawat[2]

[1]Dept. of Computer Science, Govt. Engineering College, Karni Industrial Area, Pugal Raod Bikaner, Rajasthan, India
[2]Department of Information Technology, Govt. Engineering College, Karni Industrial Area, Pugal Raod Bikaner, Rajasthan, India

Abstract: ***A MANET is grouping of freely movable nodes or autonomous nodes which are free to join or leave the wireless network without any central control. due to this decentralised management there is security violence in wireless network due to various attacks like grayhole, blackhole, overflow routing table attack, DOS attacks. but here we discuss blackhole attack in MANET which occurs due to malicious nodes in network. to avoid this attack we implement AODV protocol which is less reliable again black hole attack. To overcome the reliability issues in MANET. In this work we achieve the high reliability in SAODV protocol. In this work to decrease false positive detection of blackhole node in SAODV we modified the SAODV protocol. After the modification we achieve the higher reliability in MANET***.

Keywords: AODV Ad hoc On-demand Distance Vector Protocol, CBR Constant Bit Rate, DSR Dynamic Source Routing Protocol, E-E delay End to End delay, MANET Mobile Ad hoc Network, PDR Packet Delivery Ratio, RREP Route Reply, RREQ Route Request, RRER Route Error, UDP/IP User Datagram Protocol / Internet Protocol

1. Introduction

Wireless ad-hoc networks are composed of autonomous nodes that are self- managed without any infrastructure. In this way, ad-hoc networks have a dynamic topology such that nodes can easily join or leave the network at any time. They have many potential applications, especially, in military and rescue areas such as connecting soldiers on the battlefield or establishing a new network in place of a network, which collapsed after a disaster like an earthquake. To support this connectivity, nodes use some routing protocols such as AODV (Ad-hoc On-Demand Distance Vector), DSR (Dynamic Source Routing) and DSDV (Destination-Sequenced Distance-Vector). As wireless ad-hoc network slack an infrastructure, they are exposed to a lot of attacks. One of these attacks is the Black Hole attack. In the Black Hole attack, a malicious node absorbs all data packets in itself, similar to a hole which sucks in everything in. In this way, all packets in the network are dropped.

Security is the cry of the day. In order to provide secure communication and transmission, the engineers must understand different types of attacks and their effects on the MANETs. Wormhole attack, Black hole attack, Sybil attack, flooding attack, routing table overflow attack, Denial of Service (DoS), selfish node misbehaving, impersonation attack are kind of attacks that a MANET can suffer from.

In the last few years, security of computer networks has been of serious concern which has widely been discussed and formulized. Most of the discussions involved only static and networking based on wired systems. However, mobile Ad-Hoc networking is still in need of further discussions and development in terms of security .With the emergence of ongoing and new approaches for networking, new problems and issues arises for the basics of routing. With the comparison of wired network Mobile Ad-Hoc network is different. The routing protocols designed majorly for internet is different from the mobile Ad-Hoc networks (MANET). Traditional routing table was basically made for the hosts which are connected wired to a non dynamic backbone. Due to which it is not possible to support Ad-Hoc networks mainly due to the movement and dynamic topology of networks.

To analyze the behaviour of wireless network we have implemented the AODV protocol but due to less secure channel between source and destination of the packets this protocol is less effective against blackhole attacks further studying the nature of blackhole attack we have implemented the Secure AODV prtocol which provide more reliability and enhanced communication with the nearst node to source node by using the ‘from’ and ‘through’ entry in the routing table.all the analysis is taken on the network simulator(NS2) which provide graphical representation of black hole nodes in wireless movable network.

2. Related Work

Deng et.al.[10] have proposed a solution against black hole attack by modifying the AODV protocol. This approach avoids malicious nodes advertising the route that is not existed. In order to check whether the route advertised is existed and free of malicious nodes, each intermediate node has to include the address of the next hop node in RREP packets. Once the source node received the RREP packet, it extracts the details of the next hop node and sends a further request to the next hop node. This is to verify the existence of the next hope node and the routing metric value (i.e. the hop count) with the next hop node.

According to proposed solution [12] by Tamilselvan et.al, the source node has to wait for other replies with next hop information without sending the data packets to the destination. Once it receives the first RREP it sets timer in the TimerExpiredTable‟, to collect the further RREP from different nodes are stored in “Collect Route Reply Table‟ (CRRT) with the „sequence number‟, and the time at which the packet arrives. In order to calculate the „timeout‟ value, uses arrived time of the first RREP It first checks in CRRT whether there is any repeated next hop node. If any repeated next hop node is present, in route reply paths it assumes the paths are correct or the chance of malicious paths is limited. The disadvantages of the proposed solution are time delay, since source node has to wait for other route replies and it cannot detect cooperative black hole attack.

In [13] this paper authors Satoshi Kurosawa et.al. have introduced an anomaly detection scheme to detect black hole attack using dynamic training method in which the training data is updated at regular time intervals. They use the features to express the state of the network. In this scheme, the average of the difference between the Dst_Seq in RREQ packet and the one held in the list are calculated and this operation is executed for every received RREP packet.

Latha Tamilselvan, Dr. V Sankaranarayanan [14] proposed a better solution with the modification of the AODV protocol, which avoids multiple black holes in the group. It uses Fidelity table where every node that is participating is given a fidelity level that will provide reliability to that node. Any node having 0 value is considered as malicious node and is eliminated from the network. The fidelity levels of nodes are updated based on their trusted participation in the network.

In paper [16] authors K. Lakshmi et.al. have proposed and discussed a feasible solution for the black hole attacks that can be implemented on the AODV protocol. In this solution, compare the first destination sequence number with the source node sequence number, if there exists much more differences between them, surely that node is the malicious node, immediately remove that entry from the RR-Table. Final process is selecting the next node id that have the higher destination sequence number, is obtained by sorting the RR-Table according to the DSEQ-NO column, whose packet is sent to Receive Reply method to continue the normal AODV process.

Herminder Singh et.al. [14] have discussed the AODV protocol suffering from black hole attack and proposed a feedback solution which comparatively decreases the amount of packet loss in the network. The black holes by examining the no of sent packets at that node which will always be equal to zero for most of the cases. After the malicious black nodes have been detected, we can adopt a feedback method to avoid the receptance of incoming packets at these black holes. The packets coming at the immediate previous nodes to black nodes are propagated back to the sender and the sender follows an alternative safer route to the destination. However, it cannot detect black hole nodes when they worked as a group.

Sen, J et.al. have proposed mechanism [9] for defending against a cooperative black hole attack. This proposed mechanism modifies the AODV protocol by introducing two concepts, such as (a) data routing information (DRI) table and (b) cross checking. In the proposed scheme, the nodes that respond to the RREQ message of a source node during route discovery process send two bits of additional information. Each node maintains an additional DRI table. In the DRI table, the bit 1 stands for “true” and the bit 0 stands for “false”. The first bit “From” stands for the information on routing data packet from the node (in the ode filed), while the second bit “Through” stands for information on routing data packet through the node. In this mechanism source node (SN) broadcasts a RREQ message to discover a secure route to the destination node. The intermediate node(IN) replies with Next Hop and the DRI of Next Hop Node (NHN).

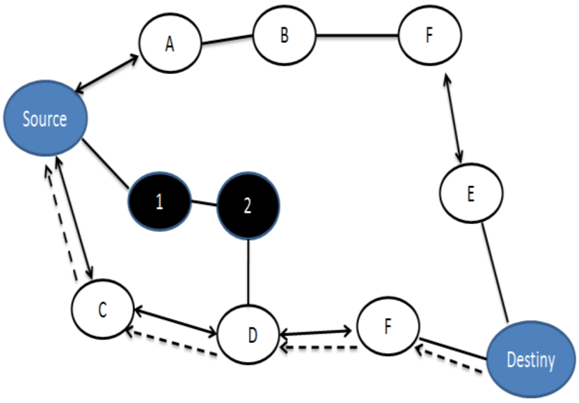

Figure 1: Solution to identify false black hole node

3. SAODV Protocol

Slightly changed AODV protocol which is known as SAODV (secure ad hoc on demand distance vector)[21] by introducing Data Routing Information (DRI) Table and route confirmation.

The solution to identify false black hole nodes acting in cooperation involves two bits of additional information from the nodes responding to the RREQ of source node S. Each intermediate node maintains an Data Routing Information (DRI) table. In the DRI table, 1 takes for ‘true’ and 0 for ‘false’. The first bit “From” stands for information on routing data packet from the node (in the Node field) and the second bit “Through” stands for information on routing data packet through the node (in the Node field). In reference to the example of Figure1, a sample of the database maintained by node D is shown in Table 1. The entry 1 1 for node C implies that node 4 has routed data packets from 3, and routed any data packets through 3 (before node 3 moved away from 4). The entry 1 0 for node B implies that, node D has successfully routed data packets from and through node B. The entry 0 0 for node 2 implies that, node D has NOT routed any data packets from or through node 2.

Table1: Data routing table for node D

Node #	*Data Routing Information*	
	From	*Through*
C	1	1
2	0	0
B	1	0
F	1	1

(Nodes through which the source node has routed data) to transfer data packets. In the protocol, the source node (SN) broadcasts a RREQ message to discover a secure route to the destination node. The Intermediate Node (IN) generating the RREP has to provide its Next Hop Node (NHN), and its DRI entry for the NHN. Upon receiving RREP message from IN, the source node will check its own DRI table to see whether IN is a reliable node.

If source node has used IN before to route data, then IN is a reliable node and source node starts routing data through IN. Otherwise, IN is unreliable and the source node sends FRq message to NHN to check the identity of the IN, and asks NHN: 1) if IN has routed data packets through NHN, 2) who is the current NHN's next hop to destination, and 3) has the current NHN routed data through its own next hop. The NHN in turn responds with FRp message including 1) DRI entry for IN, 2) the next hop node of current NHN, and 3) the DRI entry for the current NHN's next hop. Based on the FRp message from NHN, source node checks whether NHN is a reliable node or not. If source node has routed data through NHN before, NHN is reliable; otherwise, unreliable. If NHN is reliable, source node will check whether IN is a black hole or not.

If the second bit (ie. IN has routed data through NHN) of the DRI entry from the IN is equal to 1, and the first bit (ie. NHN has routed data from IN) of the DRI entry from the NHN is equal to 0, IN is a black hole. If IN is not a black hole and NHN is a reliable node, the route is secure, and source node will update its DRI entry for IN with 01, and starts routing data via IN. If IN is a black hole, the source node identifies all the nodes along the reverse path from IN to the node that generated the RREP as black hole nodes. Source node ignores any other RREP from the black holes and broadcasts the list of cooperative black holes.

When node B1 responds to source node S with RREP message, it provides its next hop node B2 and DRI for the next hop (i.e. if B1 has routed data packets through B2). Here the black hole node lies about using the path by replying with the DRI value equal to 0 1. Upon receiving RREP message from B1, the source node S will check its own DRI table to see whether B1 is a reliable node. Since S has never sent any data through B1 before, B1 is not a reliable node to S. Then S sends FRq to B2 via alternative path S-2-4-B2 and asks if B2 has routed any data from B1, who is B2's next hop, and if B2 has routed data packets through B2's next hop. Since B2 is collaborating with B1, it replies positively to all the three requests and gives node 6 (randomly) as its next hop. When the source node contacts node 6 via alternative path S-2-4-6 to cross check the claims of node B2, node 6 responds negatively. Since node 6 has neither a route to node B2 nor has received data packets from node 2, the DRI value corresponding to B2 is equal to 0 0 as shown in Figure 1. Based on this information, node S can infer that B2 is a black hole node. If node B1 was supposed to have routed data packets through node B2, it should have validated the node before sending it. Now, since node B2 is invalidated through node 6, node B1 must cooperate with node B2. Hence both nodes B1 and B2 are marked as black hole nodes and this information is propagated through the network leading to their listing as black holes, and revocation of their certificates. Further, S discards any further responses from B1 or B2 and looks for a valid alternative route to D. The process of cross checking the intermediate nodes is a one-time procedure which we believe is affordable to secure a network from multiple black hole nodes. The cost of cross checking the nodes can be minimized by letting nodes sharing their trusted nodes list (DRI table) with each other.

4. Relaibility Analysis of SAODV Over False Blackhole Detection

As we have seen the DRI table of the node D in above figure, the From and Through bit for node 2 is 0 so the source node is assuming that node 2 will be the black hole node. But sometimes this is not true. Assume that from and through bits for node 2 in routing table of node B will be 1 and 0 respectively and node B wants to send data to node D through node 2.then according to DRI table of node D as shown in above figure will have from and through bit is 0 and node B send data to node 2 but node D do not receive data from node 2 so it will drop the packets from node2. But in real the node 2 is not the malicious node. This is the known as false blackhole detection in SAODV protocol so that source node is not able to identify the malicious behavior. Further we will check reliability of SAODV protocol by measuring the no. of packets dropped from the total packets with the help of reliability formula

Reliabilty(R) = 1- Failure rate

Where
Failure rate = no. of packet drop/total no of packet sent

By applying this formula we analyse the result as shown in table 2

5. SAODV for False Positive Detection of Blackhole node

In this experiment we implement the SAODV for three categories of nodes. In first categories those node included which are working nodes in the network. In second category those nodes which are present in the network but are in idle state called normal nodes. In third category, the blackhole nodes included. We apply this simulation set up for different numbers of the nodes and we study the behavior of the SAODV. In this four type of behavior considered. These are the case TRUE Positive means the actual blackhole node detected. In the Second Case TRUE Negative means the blackhole node not detected. In third case FALSE Positive means the normal idle node detected as blackhole negative. In fourth case FALSE Negative means nothing has been detected. The simulation result is given in the table below.

Table 2: Results of detection of nodes in SAODV

Total Nodes	Normal Nodes	Idle Normal Nodes	Blackhole nodes	True Positive	True Negative	False Positive	False negative
30	25	3	2	1	0	2	0
40	30	5	5	4	1	3	0
50	35	8	7	5	2	6	1
60	40	10	10	9	1	8	0
80	45	12	13	12	1	11	0

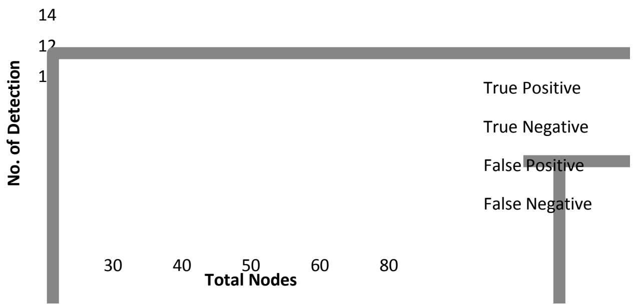

Figure 2: Behaviour of SAODV in blakhole node detection

As we can see clearly that in case of True Positive SAODV works efficiently. But from table and graph we can see the as the number of node increases the False Positive detection rate also increase in SAODV. In this case the reliability of the SAODV is decrease as the number of idle normal nodes increase.

6. Proposed Modification in SAODV

```
1.      Analyze DRI entry to identify the black node
2.      If (BlackHole(IN))
{
Ack= send(Sample Packet, IN)
If(Ack !== NULL)
{
Set Route=secure
Set IN.Blackhole=False
}
Else
{
3.      Set Route=Insecure
4.      Set IN.Blackhole=True
5.      Black all node the communication with IN
 } }
```

To decrease the false positive detection rate in SAODV we don some minor change in the blackhole detection technique. As above we see that in SAODV blackhole detection is base on The DRI table. In the process of detection every node checks own DRI table entry for the next node on the path. Also from the above discussion we have see that the DRI entry for any blackhole node and normal idle node is same on the every node. This is caused for the false positive rate in SAODV. To decrease the false positive rate of the blackhole detection, we did some changes in algorithm. In this when the any node analyze the DRI table entry for the next node in the path, if it found the symptoms of blackhole detection then it should confirm the node by sending e sample packet to it. If packet dropped and acknowledge doesn't come then it is confirmed the node is blackhole but if node is normal idle node then it will send acknowledge. If the sender node gets acknowledgement then confirm it as a normal node. After the modification in the SAODV algorithm we measure the behavior of the modified SAODV for the same setup given above in the table. we have seen the large decrement in the false positive rate of blackhole detection. The resuls are shown in the table .The modification in SAODV algorithm given in section above.

7. Experiments Results for Improved SAODV

For the same parameters and setup used in simulation of AODV we simulate modified SAODV against the blackhole detection. And the results are given in table below.

Table 3: Results of detection of nodes in Modified SAODV

Total Node	*Nornal Nodes*	*Idle Normal Nodes*	*Black hole nodes*	*True (+)*	*True (-)*	*False (+)*	*False (-)*
30	25	3	2	1	2	1	0
40	30	5	5	5	0	1	1
50	35	8	7	6	1	2	0
60	40	10	10	10	0	2	1
80	45	12	13	11	1	3	2

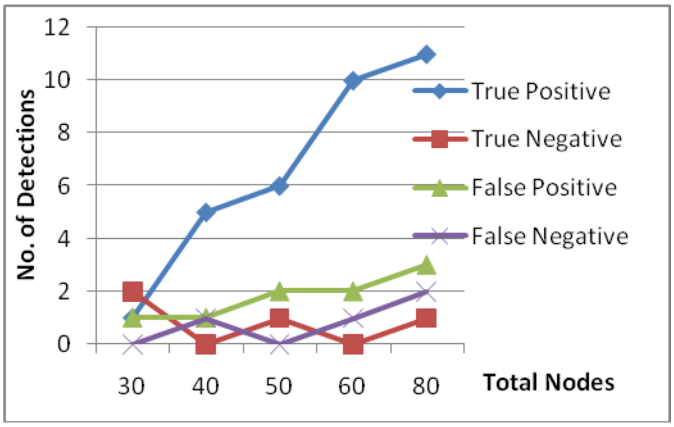

Figure 4: Behavior of Modified SAODV in blakhole node detection

8. Comparison of SAODV and Modified SAODV

As the tables 2 and 3 shows that the false detection rate in SAODV is decreases as the number of nodes increase. From fig.2 and fig 3 we can see the rates for detections against the blackhole node. In this modification our objective was to decrease the false positive detection of the blackhole node. from fig. 4 we can see the comparative graph for False positive in SAODV and Modified SAODV.

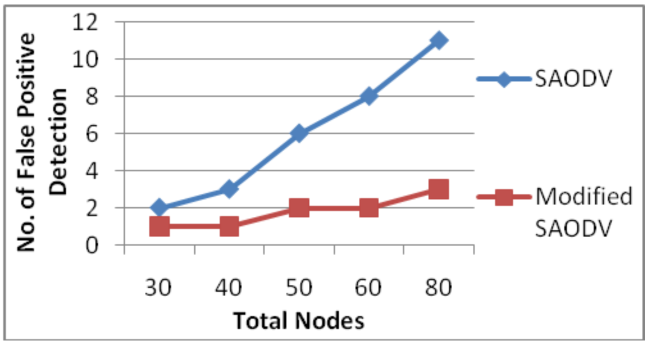

Figure 5: Comparision of SAODV and Modified SAODV against false positive detection

9. Conclusion

The presented work is defined as the improvement over the existing AODV protocol to provide the reliable and safe communication. The presented work has provided the solution to problem of false positive detection of blackhole nodes in SAODV. This improved SAODV protocol is called Modified SAODV protocol used the concept of DRI table based mapping to identify black hole nodes and provide the reliable and safe route over the network. The presented work has observed the network nods under reliability parameters and generate the effective communication route. In this work, at the first level, the reliable node identification is done by proving the node identity.

Reference

[1] Yudhister Chawla, Hardayal Singh Shekhawat, ”Reliability Analysis of AODV Protocol and simulation of SAODV Protocol, ” International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 4, Issue 3, March 2014.

[2] Sen, J.; Koilakonda, S.; Ukil, A.; , "A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Ad Hoc Networks”, Intelligent Systems, Modelling and Simulation (ISMS), 2011 Second International Conference on , vol., no., pp.338-343, 25-27 Jan. 2011.

[3] Osathanunkul, K.; Ning Zhang; , "A countermeasure to black hole attacks in mobile ad hoc networks, " Networking Sensing and Control (ICNSC), 2011 IEEE InternationalConference on, vol., no., pp.508-513, 11-13 April 2011.

[4] N. Bhalaji, A. Shanmugam, “A Trust Based Model to Mitigate Black Hole Attacks n DSR Based MANET”, European Journal of Scientific Research, Vol.50 No.1, pp.6-15, 2011.

[5] C.H Perkins, S.R “Ad hoc on demand Distance Vector, AODV” RFC 561

[6] B. LanNgnyen and L.Treng “A study of different types of attacks on multicast mobile adhoc networks” , Adhoc network Vol

[7] Deng H., Li W. andAgrawal, D.P., "Routing security in wireless ad hoc networks, " ommunications Magazine, IEEE, vol.40, no.10, pp. 70- 75, October 2002.

[8] Al-Shurman, M., Yoo, S. and Park, S, "Black hole Attack in Mobile Ad Hoc Networks", ACM Southeast Regional Conference, pp. 96-97, 2004.

[9] Tamilselvan, L.; Sankaranarayanan, V., "Prevention of Blackhole Attack in MANET, " ireless Broadband and Ultra Wideband Communications, 2007. Aus Wireless 2007. The 2nd International Conference on, vol., no., pp.21, 27-30 Aug. 2007.

[10] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, YoshiakiNemoto, Detecting Black hole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method” International Journal of Network Security, Vo l.5, No .3, P P.338–346, Nov. 2007.

[11] Alem, Y.F.; Zhao Cheng Xuan; , "Preventing black hole attack in mobile ad-hoc networks using Anomaly Detection, " Future Computer and Communication (ICFCC), 2010 2nd International Conference on , vol.3, no., pp.V3-672-V3-676, 21-24 May 2010.

[12] Medadian, M.; Mebadi, A.; Shahri, E., "Combat with Black Hole attack in AODV routing protocol", Communications (MICC), 2009 IEEE 9th Malaysia International Conference on, vol., no., pp.530-535, 15-17, Dec.2009.

[13] XiaoYang Zhang; Sekiya, Y.; Wakahara, Y., "Proposal of a method to detect black hole attack in MANET, " Autonomous Decentralized Systems, 2009. ISADS '09. International Symposium on, vol., no., pp.1-6, 23-25 March 2009

[14] Songbai Lu; Longxuan Li; Kwok-Yan Lam; LingyanJia, "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack, " Computational Intelligence and Security, 2009. CIS '09. International Conference on, vol.2, no., pp.421-425, 11-14 Dec. 2009.

[15] NitalMistry, Devesh C Jinwala, MukeshZaveri, “Improving AODV Protocol against lackhole Attacks”, proceedings of the International Multi Conference of Engineers and Computer Scientists 2010 Vol II, IMECS 2010.

[16] Yaserkhamayseh, Abdulraheem Bader, Wail Mardini, and MuneerBaniYasein, “A New Protocol for Detecting Black Hole Nodes in Ad Hoc Networks”, International Journal of Communication Networks and Information Security (IJCNIS) Vol. 3, No. 1, April 2011.

[17] Payal N. Raj1 and Prashant B. Swadas2, “DPRAODV: A Dynamic Learning System against Blackhole Attack in AODV based MANET”, IJCSI International Journal of Computer Science Issues, Vol. 2, 2009