ISSN 2277-3061

Fangled Protocol for Black Hole Detection in Ad Hoc Networks

Reeta Mishra

Department of computer Engineering and Information Technology
K J Institute of Technology, Savli, Vadodara, India
E-mail- reetatrpth@gmail.com

ABSTRACT

Now a day, security in Mobile Ad hoc Network is very important issue. Due to dynamic topology and mobility of nodes, Mobile Ad hoc Networks are more vulnerable to security attacks than conventional wired and wireless network. Nodes of Mobile Ad hoc Network communicate directly without any central base station. That means in ad hoc network, infrastructure is not required for establishing communication. Therefore attacks in this are very frequent than other networks. In this research paper we are describing black hole attacks which are easy to launch in wireless ad hoc network. Black hole attack is referred to as a node dropping all packets and sending forged routing packets to route packets over itself. Ad hoc networks are vulnerable to different kinds of attacks such as: denial of services, impersonation, and eavesdropping.This paper discusses one of the security problems in ad hoc networks called the black hole problem. It occurs when a malicious node referred as black hole joins the network. The black hole conducts its malicious behaviour during the process of route discovery. For any received REQ, the black hole claims having a route and propagates a faked REP. The source node responds to these faked REPs and sends its data through the received routes. Once the data is received by the black hole, it is dropped instead of being sent to the desired destination.

The proposed protocol is built on top of the original AODV. It extends the AODV to include the following functionalities: source node waits for a reliable route; each node has a table in which it adds the addresses of the reliable nodes; REP is overloaded with an extra field to indicate the reliability of the replying node.

Keywords

Black Hole; Routing; Ad Hoc Networks; Behavioural Analysis; Mobility.

SUBJECT CLASSIFICATION

Computer Science & Information Technology Classification

LITERARY ANALYSIS / RELATED WORK

Different ideas and studies discuss the black hole problem and its effects on the routing process. One of them proposes to solve the problem by preventing the intermediate nodes from replying to the received route requests. Such idea forces the intermediate nodes to broadcast the route request. In this solution, only the destination node holds the responsibility of sending the route reply. Such idea limits the cooperative behavior of the nodes, where it prevents the exchange of route information between the nodes, and hence increases the overhead of route discovery.

V Sankaranarayanan and Latha Tamilselvan [6] discuss the problem of black hole and its effects on the AODV routing protocol, and propose a solution that detects the route and ensures its reliability before sending the data packets through it. The proposed solution modifies the AODV protocol to handle the problem as follows: when the source node receives a route reply it does not send data through it immediately, instead it waits until receiving other routes from other neighboring nodes and checks the safe route to send data through. The source node runs a timer to collect the route replies from the neighboring nodes. The source node maintains the collected route replies in a table. After the timer reaches the timeout value, the source node chooses the most reliable route from the table of collected routes. Routes containing more repeated common nodes are considered more reliable by the source, if there are no repeated common nodes in the routes; the source node considers the route as reliable if the replying node provides information about its next hop in the route [6]. Figure 1 shows the proposed solution in [6].

Wei Li, and Agrawal [10] present a study to solve the black hole problem as follows: the source node sends a route request as usual, it receives route replies from neighboring nodes, and delays transmitting data until checking the reliability of the received routes (route is considered reliable if the source node has routed data through the replying node successfully).

Latha Tamilselvan and Dr. V Sankaranarayanan [9] present a study which considers the cooperative behavior of two black hole nodes working as a team. The study borrows the concept of path rater from [8] which computes the trust values of each participating node. Each node has a fidelity table in which it records the fidelity values of the participating nodes. The fidelity value of a given node is incremented or decremented proportional to its behavior in the network.

The protocol works as follows: the source node sends a REQ and waits for a predefined period of time to collect the REPs. Once the routes are collected, the source checks the fidelity values of both the replying node and its next hop in each received route. The source node chooses the route with the highest fidelity values and sends its data through. If there is more than one route with the same fidelity values, the source chooses the one with least number of hops. Once the destination node receives the data it sends an acknowledgement to the source informing it that it has

Successfully received the data. The source increments the fidelity values of the replying node and its next hop if the acknowledgment is received, and decrement them if the acknowledgement is not received. The updates of the fidelity values are exchanged over the network. When the fidelity value of the replying node drops to zero, both of the node and its next hop are considered as a cooperative team of black hole nodes and eliminated from the network.

The proposed solution in [29] modifies the behavior of AODV to include a mechanism for checking the sequence number of the received RREP. As the source node receives the RREP it compares the sequence number of the received RREP to a threshold value. The replying node is suspected to be a black hole if its sequence number is greater than the threshold value. The source node adds the suspected node to its black list, and propagates a control message called an alarm to publicize the black list for its neighbor.

INTRODUCTION

Ad hoc network is self forming network of mobile devices connected by wireless link. It is also called wireless ad hoc network. In this, every device works as a router and device works as a router and free to move in any direction. Using this property, we can send data over a long distance. Due to the dynamic topology and mobility of nodes, Mobile Ad hoc Networks are more vulnerable to security attacks than conventional wired and wireless network. In general, it is looking very simple processing. But in practical it is a complex procedure. Because, we have to care about many hinges that will be used during the communication process. Security constrain is one of them. Now a day, to send secure data is a very important and burning issue in the field of Mobile Ad hoc Network. Whenever we exchange message between mobile devises within an area (zone) or mobile devices from different areas (zone or ad hoc networks), it is necessary to send information securely over a medium. Due to the mobility of the nodes it is impossible to use static routing table maintained at fixed routers. Now a day, it is necessary to find out best or optimal path between nodes during the communication. Ad hoc networks have the following features: power limitations, node mobility, topology changes, broadcast transmission medium, self organization and configuration of the nodes. These features have a direct impact on the following: link reliability, routing information, and network security [3, 4]. Ad hoc network communication systems consist of five layers. Each layer is implemented separately and provides a set of services to the next higher layer. The following are the layers

of ad hoc networking systems: physical layer, data link layer, network layer, transport layer, and application layer [16, 17].Routing is an essential operation in ad hoc networks. Any Successful breakthrough for the routing has a direct impact on the performance of the whole network. This is the reason for which the routing is being targeted by different kinds of attacks.

2 .BLACK HOLE ATTACK- OVERVIEW

In black hole attack [1], black hole node acts like black hole in the universe. In this attack black hole node absorbs all the Traffic towards itself and doesn't forward to other nodes. Whenever, source node wants to send packet to the destination node. To attract all the packet towards it, this malicious node advertise that it has shortest path through it to the destination node. The problem occurs when a malicious node referred as black hole joins the network and snoops on its neighboring nodes. The black hole receives the route requests from its neighboring nodes and sends fake route replies immediately claiming that it has a direct link to the destination node. The incoming route reply from the malicious node could be received by the source before receiving other routes. In such case, the source node uses a route containing the malicious node and sends its data through it. As the malicious node receives data packets, it drops them instead of sending them to the destination, resulting in more message overhead and causing a failure in the routing protocol that covers a part of the network. The occurrence of the black hole problem and the operations of the malicious node depend on the routing Protocol.

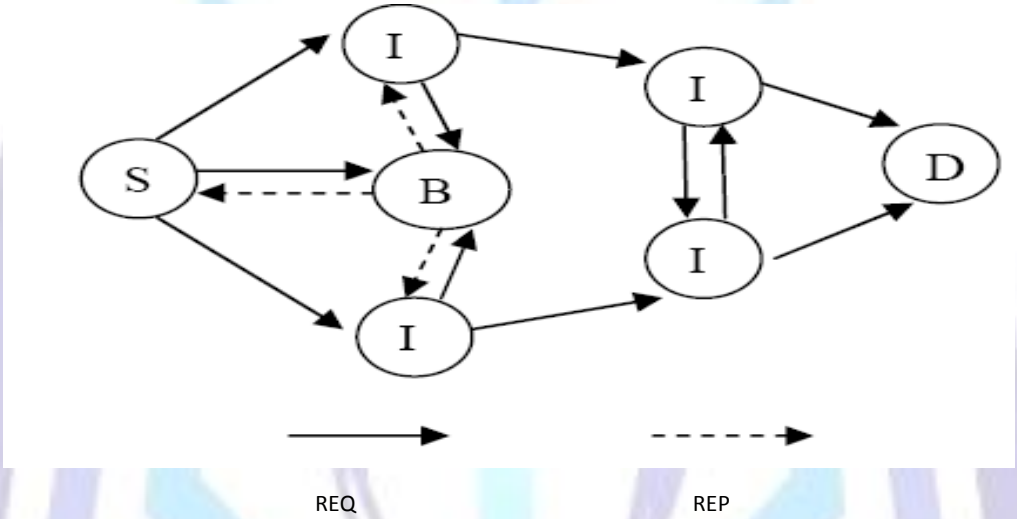


Figure 1**:** Black hole problem

Figure 1 shows a network consisting of seven nodes: the Source (S), the destination (D), the black hole (B), and four Intermediate nodes (Ij). Firstly, S sends a REQ asking for a route to D. The REQ is received by all of its neighboring Nodes (I1, BH, and I2). As shown in Figure 1, both I1 and I2 re-broadcast the REQ. On the other hand B does not rebroadcast the REQ, where B is a black hole. Instead it replies immediately claiming that it has a direct link to D.

As usual, S responds to the REP by sending the data to D Through B. Once the data is received by B, it will be Dropped directly. Moreover, B will also send the same REP to both I1 and I2 as soon as it receives the rebroadcasted REQ from them. This implies that B will be added to the route table of both I1 and I2 as the first hop to D.

There are two types of black hole attack-

2.1 Black hole attack with single malicious node -

In the Black hole attack with single malicious node [2, 3], only one node will act as malicious node in a zone. Other nodes of the zone will be authentic.

2.2 Black hole attack with multiple malicious node - In the Black hole attack with multiple malicious node [4, 5],more than one node will act as malicious node in a zone.These malicious nodes can work with collaboration.

3. PROTOCOLS USED -

There are mainly three types of protocol categories used in the wireless sensor network for finding routes between nodes-

3.1 Proactive Protocol

Proactive protocols [8] constantly update network topology information and ensure that it is available to all nodes. That means it ensures routes to all destination are up to-date and ready for use when required. These protocols reduce network latency but increase data overhead by constantly updating routing information. This lead to Consuming of large amount of bandwidth. Examples of Proactive protocols are DSDV (Destination-Sequenced Distance Vector Routing) protocol and OLSR (Optimized Link State Routing) protocol.

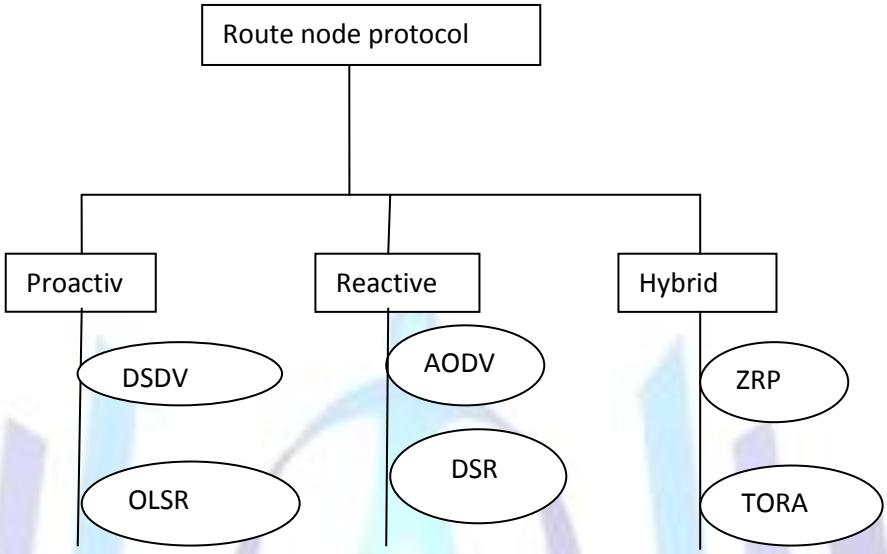


Figure 2: Wireless route node protocol

3.2 Reactive Protocol

Reactive protocols [9, 10] determine routing paths only when required. These protocols are associated with lower

Protocol overheads but longer packet delays. These protocols cause delays since the routes are not already available and flooding lead to additional control traffic again putting strain on the limited bandwidth. Examples of reactive protocols are AODV (Ad hoc Distance Vector Routing) protocol and DSR (Dynamic Source Routing) protocol.

3.3 Hybrid Protocol

This type of protocols combines the advantages of proactive And of reactive routing. The routing is initially established with some proactively prospected routes and then serves the Demand from additionally activated nodes through reactive Flooding. The choice for one or the other method requires Predetermination for typical cases. Advantage of these Protocols depends on the amount of nodes activated. Reaction to traffic demand depends on gradient of traffic volume. Examples of hybrid protocols [11] are ZRP (Zone Routing Protocol) protocol and TORA (Temporally Ordered Routing) protocol.

5. Proposed Protocol

The default case in any routing protocol is to send the data packets through the first received route. Such behavior reduces the burden of the following: setting a timer, waiting for further routes, and buffering more data packets. In the typical cases, the protocol works properly and performs the task with the desired results, but when the network is Attacked by a black hole node, the performance of the protocol decreases dramatically. To propose a solution to the problem, the behavior of the black hole node needs to be Addressed more specifically.

5.1. Behavioral Analysis of the Black Hole Node

The black hole node is a strange malicious node joins the network with the intention of dropping the transmitted data packets instead of delivering them to the desired destination.

The following are the main behavioral characteristics of the black hole node:

It snoops on its neighbors to discover which node is preparing to send a RREQ. For any received RREQ, the black hole node propagates a RREP claiming that it has a direct link to the destination.

It constantly attempts to locate itself within the transmission range of any source node in order to reply as quickly as

possible. This requires a continual movement of the black hole in the network. Moreover, its movement speed may be higher than the normal nodes.

Referring to the second characteristic, the black hole never contributes in the operation of route discovery (i.e. never broadcasts the received RREQs). Moreover, for any route including a black hole, the black hole always appears as the last hop before the destination.

Referring to the third characteristic, the number of the routes that the black hole contributes in them is greater than the number of routes that the normal node contributes in them.

5.2. The Proposed Protocol

The proposed protocol modifies the behavior of the original AODV to include the following techniques:

-Every node is provided with a data structure referred as faith table. This table is responsible for holding the addresses of the reliable nodes.

-The REP is extended with an extra field called faith field.This field indicates the reliability of the replying node (i.e. the propagating node of the REP).

-The source node sends its data only if the REP is propagated by a reliable node. Otherwise it waits for further REP.

-The details of the protocol are given in the following subsections.

5.2.1. Route Discovery

When a source node (S) needs to communicate with a destination node (D), the source node initiates the process of route discovery by flooding the network with a REQ.

If S has data packet to send and there is no route to D then it does the following:

Prepare the REQ Broadcast it

5.2.2. The Faith Table

Before the communication takes place the faith table is Initialized to null for all the participating nodes. In order for a node to be added to the faith table of another node, it needs firstly to pass the behavioral analysis filter. This filter considers the following aspects:

1)The black hole moves continually resulting in a continual change in the state of the neighborhood with the other nodes. Normal node can detect such behavior by observing changes in its neighborhood table.

2)Number of active connections that a node is part of. Normal node can detect this by checking its route table.

3)The link activity duration. The duration of the link activity between a given node and the black hole is long compared to the normal average duration of the link activity.

4) Each node in the network keeps a file of history Registers information along with special code about its neighbors regarding the mentioned above aspects. This file is saved in the cache and acts as a reference which supports the filter with the needed information about a given node (i.e. the broadcasting node of the REQ). Once the network is flooded with a REQ, each node receives the REQ checks whether the broadcasting node passes the filter or not. Once the broadcasting node passes the filter, it is added to the faith table. The process is repeated until the REQ is received by the replying node.

ISSN 2277-3061

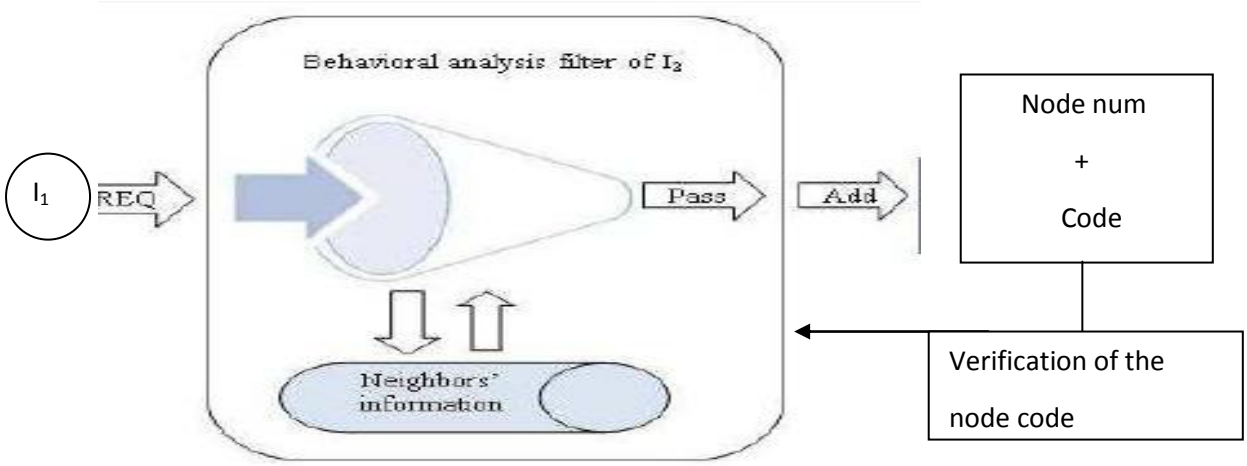


Figure 3: The behavioral analysis filter

Note:-When the broadcasting node passes through the filter each node had a special code, as the node added to the faith table that special code is also remains with it.

Verification of the node num and code can be easily done with the history information file (contain node num and its code) which present in each node of the network and the faith table. So , it provide more safe and secure protocol as compare to other one.

Algorithm of handling REQ by the intermediate nodes.

If (broadcasting_ node pass the filter)

Add broadcasting_ node to its faith table

If has a route to D then

It propagates a REP

Else

It re-broadcasts the REQ

The process of adding a new input to the faith table during the trip of the REQ from the source to the destination.

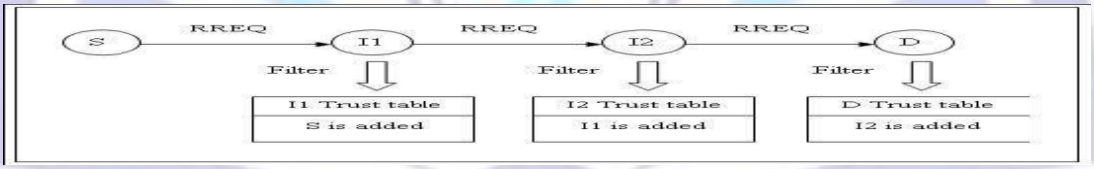


Figure 4: Adding a new input to the faith table

5.2.3. Handling REQ by the Replying Node

The replying node is one of the following three possibilities: the destination itself, an intermediate node has a real route tothe destination, or a black hole claims having a route. Once the replying node receives the REQ, it prepares the REP.The REP is overloaded with an extra field to indicate the reliability of the received route. The replying node extends the original REP of the AODV with a field of integer value to express the reliability of the replying node. This field is initialized to zero by the replying node, and may change its value in the first hop of the reverse path.

Note- that the replying node only initializes the field. The reliability of the route is not given by the replying node.

Evaluating the reliability of the route takes place in the first hop of the reverse path, because it is the most expected node to have information about the replying node. The algorithm of handling the REQ and preparing the REP is given below.

The algorithm is given in case the replying node is the destination itself. The scenario of the other two cases is similar to that of the destination.

When D receives a REQ, it does :

If (broadcasting _node pass the filter)

Adds the sending node to its faith table

Prepares REP, and initializes its faith field to 0

Sends the prepared REP through the reverse path

5.2.4. Handling REP by the Remaining Nodes

Once the REP is received by the first hop of the reverse path, the identity of the replying node is determined, and the value of the faith field is modified accordingly. Basically, the first hop of the reverse path is the most critical node in it. It is the only node which is qualified to determine the identity of the replying node and change the value of the faith field accordingly.

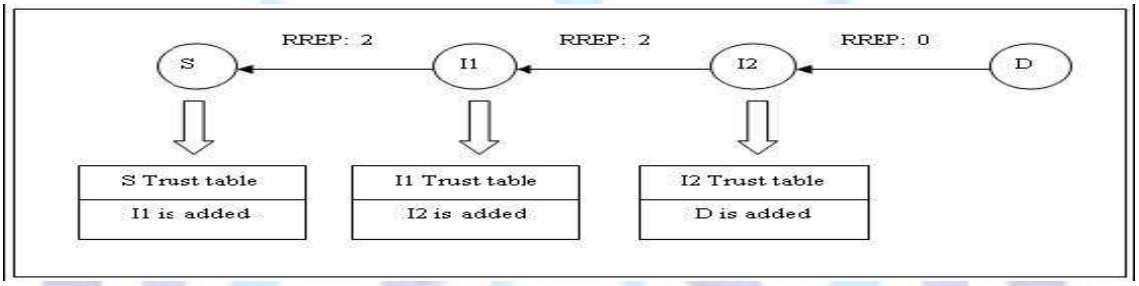
By receiving the REP by the first hop in the reverse path, the value of the faith may be modified as follows:

If the replying node is the destination itself, the faith value is changed from 0 to 2.

If the replying node is not the destination, but still exists in the faith table, then the faith value is changed from 0 to 1.

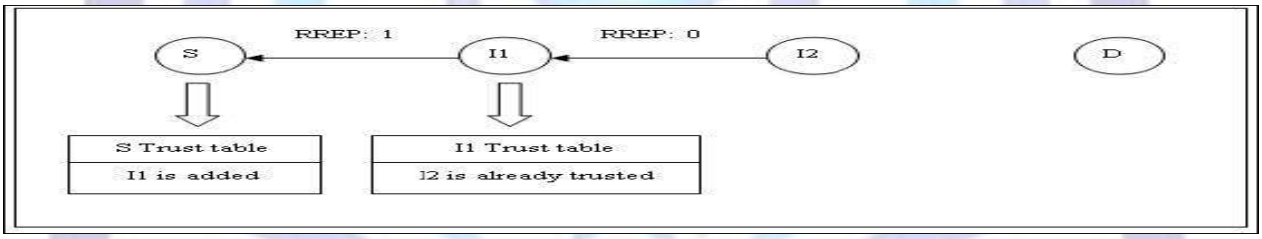
If the replying node is neither the destination nor exists in the faith table, then the faith value is not changed.

Given figure shows how the REP is handled by the first hop of the reverse path, in case of receiving a REP from the destination itself.



Figures 5: Frist case of Algorithm

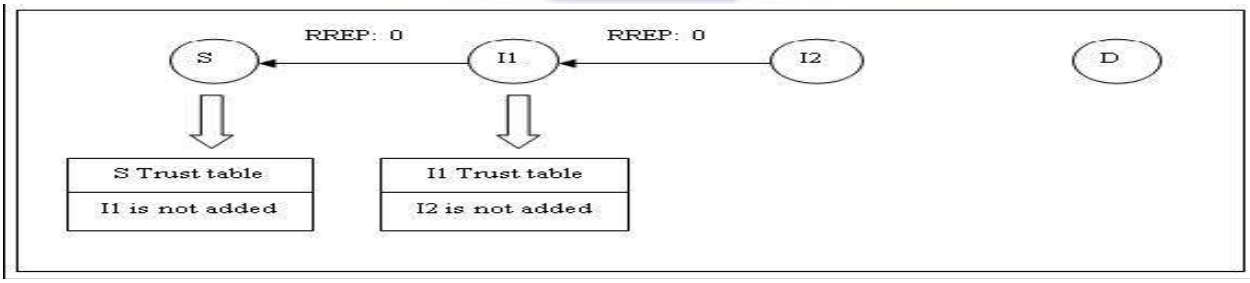
Next given figure shows how the REP is handled by the first hop of the reverse path, in case of receiving a REP from a reliable intermediate node (exist in the faith table).



Figures 6:Second case of algorithm

Next given figure shows how the REP is handled by the first hop of the reverse path, in case of receiving a REP

from a node which is not exist in the faith table (could be black hole).



Figures 7:Third case of algorithm

As the REP moves in the reverse path, each node checks the faith field. If the faith field is 1, or 2, then the current node not adds its last hop to its faith table for further use.

Shows the algorithm of handling REP by the first hop of the reverse path.

Case 1: the replying node is an intermediate node, and not

exists in faith table

REP is sent through the reverse path without

modifying the faith field

Case 2: the replying node is an intermediate and exists in

the faith table

Modify faith field from 0 to 1, then send the REP

Case3: the replying node is D

Modify faith value from 0 to 2, then send the REP

For the rest of the nodes in the reverse path, the algorithm of handling the REP is given:

When receives REP, it just forward it to the next hop

Depending on the value of the faith field in the REP, the source node chooses either to send the data through the route or to wait for another route. For the faith value equals to 1 or 2, the source node sends the data. Otherwise the source node waits for another route. The algorithm for handling the REP by the source is given below.

When S receives the REP, it checks the faith value and does the following:

If (faith value = 1 or 2)

S sends the data packet

Else

S waits for further faithed route

6.Conclusion and Future Work

The proposed protocol modifies the behavior of the original AODV to check the reliability of the received routes before sending the data packets. The main priority of the protocol is to send the data through reliable route. The protocol need to be supported by a technique to eliminate the black hole node from the network. The modification with which the researcher came up can be summarized as given below. -Each node has a table prepared to hold the addresses of the reliable nodes. During the process of route discovery, for each node receives a REQ, it checks the behavior of the broadcasting node.

- Once the behavior of the broadcasting node is normal, it is added to the faith table of the receiving node. REP is overloaded with an extra field to indicate the reliability of the replying node. -The value of the faith field is initialized to zero by the replying node and might modified by its previous hop during the trip of the REP.

-The value of the faith field could be modified either to 2 if the replying node is the destination itself or

to 1 if the replying node is not the destination but still exist in the faith table.

- Once the REP is received by the source node, it decides whether to send the data or to wait for further route.

-In case the faith field value equals to 1 or 2, the source node sends, otherwise the source node waits for further route.

The protocol reduces the bad affects of the black hole problem and outperforms the original AODV in terms of packet

delivery ratio, number of dropped packets, end-to-end delay, and overhead.

For example, the results show that, when the node is attacked by two black hole nodes and the pause time

is set to zero, the protocol outperforms the original AODV by 13%, 51%, 46%, and 14% regarding the mentioned

above metrics respectively.

The conditions of passing the behavioral analysis filter are not satisfied enough so it can be enhanced to judge the reliability of the node. Moreover, the protocol does not consider the behavior of two black hole nodes working together as a team. In future step need to mention which support the protocol with a certain mechanism to handle the problem for more than one black hole working as a team. The overhead stands as a barrier in the face ofmrealizing the protocol. More researches need to be devoted to reduce it.

7. References

[1] Johnson, B. Maltz, A. and Josh, B. (2001). “DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks,” in Perkins, Charles E. *(ed.) Ad Hoc Networking*, Chapter 5, Addison-Wesely, pp. 139-172.

[2] Perkins, Charles E. and Royer, Elizabeth M. (1999).“Ad-hoc On-Demand Distance Vector Routing”.Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (IEEE WMCSA '99), New Orleans, ouisiana, February 1999: 90-100.

[3] Li, Wenjia. and Joshi, Anupam. "Security in mobile ad hoc network *(survey)*". Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County.[4] Ghaffari, Ali. (2006). "Vulnerability and Security of Mobile Ad hoc Networks", Proceedings of the 6th WSEAS International Conference on Simulation, Modeling and Optimization, Lisbon, Portugal, September 22-24.

[5] Kargl, F. , Schlott, S., Klenk , A., Geiss, A. and Weber, M. (2002). "Securing Ad hoc Routing rotocols",Proceedings of the 1st ACM Workshop on Wireless Security. Atlanta, GA, USA. Pages 1-10.

[6] Tamilselvan, Latha and Sankaranarayanan, V. (2007)."Prevention of Black hole Attack in MANET", The 2nd

International Conference on Wireless Broadband and Ultra Wideband Communications (Aus Wireless 2007)

India, 2007 IEEE.

[7] Hu, Y., Perrig, A. and Johnson, D. (2002). "A secure On-demand Routing Protocol for Ad Hoc Networks", in

Proceedings of ACM MOBIC' 02. Atlanta, USA September 23–26.

[8] Marti, S., Giuli , T. J., Lai, K. and Bake, M. (2000). Mitigating Routing Misbehavior. In *Mobile Ad hoc networks. 6th MobiCom*, BA Massachuestts.[9] Tamilselvan, Latha and Sankaranarayanan, V. (2008)."Prevention of cooperative black hole attack inMANET", in *Journal of Networks*, Vol. 3, NO. 5, MAY 2008.

[9] Deng, Hongmei , Li, Wei and Agrawal, Dharma P (2002). "Routing Security in Wireless Ad Hoc Network", in IEEE Communications Magazine, vol. 40, no. 10, October 2002.

[10] Gatzianas, Marios and Georgia is, Leonidas (2008). "A Distributed Algorithm for Maximum Lifetime Routing

in Sensor Networks with Mobile Sinks", IEEE Transactions on Wireless Communications 7(3): 984- 944.

[11] Sobeih A. (2002). "Reliable Multicasting in Wireless Mobile Multi-Hop Ad Hoc Network Ms". Master thesis.

Cairo: Cairo University.

[12] Zimmehrman T. (1996). "Personal Area Networks:Near-field Intrabody Communication". In IBM Systems Journal 35(3&4), 1996. 609-617.[13] Singh, Amandeep, Singh, Charanjit, and Kaur, Rajbir (2007). "Security Issues in Wireless ad hoc Network".Proceeding of COIT, RIMT-IET, Manadi Gobindgarth.

[13] F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E.Cayirci (2002). "Wireless Sensor Networks: A survey".In Computer Networks Journal 38(4), 2002. 393-422.

[14] Stalling, William (2001). High Speed Networks and Internets, second edition, New Jersey: prentice hall.

[15] Stalling, William (2001). Wireless Communication and Networks, first edition, New Jersey: prentice hall.

[16] Lidong Zhou, Zygmunt J. Haas (1999). "Securing Ad Hoc Networks". In IEEE network, special issue on network security, November.

[17] Perkins C. (2000). "Ad Hoc Networking an Introduction". In Addison-Wesley Professional, November 28; 13-19.

[18] Royer E., and Toh C. (1999). "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks". In IEEE Pers. Commun. Apr; 6(4): 46-55.

[19] Perkins C. and Bhagwat P. (1994). "Highly Dynamic Destination-Sequenced Distance-Vector routing(DSDV) for Mobile Computers". Proceedings of the Conference on Communications architectures, protocols and applications. London, United Kingdom, October;24(4): 234-244.

[20] Murthy S., Garcia-Luna-Aceves J. (1996). "An Efficient Routing Protocol for Wireless Networks". ACM Mobile Networks and Applications, October 1996; 1(2): 183-197.

[21] Perkins C. (1994). "Highly Dynamic Destination- Sequenced Distance-Vector Routing (DSDV) for Mobile Computers". Proc. ACM SIGCOMM; 234-344.

[22] Yaqoub, Zahi (2008). "Black hole Avoidance in Ad Hoc Networks". Master thesis, Jordan, Al-albayt University.

[23] Mishra, Amitabh and Nadkarni, Ketan M. (2003)."Security in Wireless Ad Hoc Networks". In The Handbook of Ad Hoc Wireless Networks (*ed*.) (Chapter 30), CRC Press LLC.

[24] Abdalla, A. M. (2005). "Reputed Authenticated Routing for Ad Hoc Networks Protocol (Reputed-ARAN)". Doctoral dissertation. Cairo, the American University in Cairo.

[25] Wedian, S. (2009). "Neighborhood-based Route Discovery Protocols for Mobile Ad hoc Networks".Master thesis, Jordan, Jordan University of Science and Technology.

[26] Zeng, X., Bagrodia, R. and Gerla, M. (1998)."GloMoSim: A Library for Parallel Simulation of Large-scale Wireless Networks". Proceeding of the 12th Workshop on Parallel and distributed simulation, Banff,Alberta, Canada; 1998: 154-161.

[27] Payal, N. Raj, B. and Prashant, Swadas. (2009)."DPRAODV: A Dynamics Learning System Against Black hole Attack in AODV Based Manet ", in IJCSIInternational Journal of Computer Science Issues, Vol.2.

Author's biography with Photo

Ms.Reeta Mishra has completed her M.Tech in Computer Science and Engineering in 2011 from S.I.T.E,Meerut.Currently she is working as Asistant Professor in K.I.J.T ,Savli,Vadodara.She had published several research paper in national and international journals and conference of repute.Her research areas are Computer Networks And Security, Cyber Forensic ,Wireless Networks etc. She is an active Editorial Board member of "International Journal Of Adanvce Research In Scence and Engineering", impact factor is-1.4 as well as few more international journals.