RESEARCH ARTICLE OPEN ACCESS

# Avoidance of Black Hole Attack using Revised AODV protocol and Trust Mechanism

**J.Gautam*, C.V.Shanthi**, S.Arul Armstrong***,D.Arputha Jeron Xavier******

*(Information Technology, K.L.N.College of Engineering, Pottapalayam
Email: gautamjprakash@gmail.com)
** (Information Technology, K.L.N.College of Engineering, Pottapalayam
Email: shanthivengateshc@gmail.com)
*** (Information Technology, K.L.N.College of Engineering, Pottapalayam
Email: s.arularmstrong@gmail.com)
**** (Information Technology, K.L.N.College of Engineering, Pottapalayam
Email: jeroncool@gmail.com)

## Abstract:

Mobile Ad-hoc Network(MANET) is a consistently self-configuring, infrastructure-less network of mobile devices connected wirelessly. Since the nodes communicate with each other, they co-operate by forwarding data packets to other nodes in the network. Ad-hoc On-demand Distance Vector (AODV) is one of the most appropriate routing protocol for the MANETs and it is more susceptible to black hole attack by the detrimental nodes. Black hole attack is the one in which, malicious node incorrectly sends the RREP (route reply) that it has the shortest route to destination and then it drops all the receiving packets. The aim of the project is to avoid Black hole attack using Trust mechanism. Trust is the degree of reliability about other node for performing certain action by keeping track of all past transaction or interactions with nodes by direct or indirect observation. However, the communication will only be secure if the initial assumption of trust is true. Therefore, it is made clear that in order to ensure security it is necessary that the packets are forwarded only through the trusted nodes.

*Keywords* **—Mobile Ad-hoc Network, Routing Protocol, Black Hole Attack, Trust.**

## I. INTRODUCTION

Network is the spine for telecommunication, Wi-Fi networks like cellular network. As aftermath of the remarkable exploit of hand held gadgets, Mobile Ad-Hoc Network (MANET)is a thriving technology in today's scenario. A MANET is a multi-hop temporary proclamation network of cell nodes that operates with Wi-Fi transmitters and receivers without the assistance of any pre-existing network infrastructure. The nodes are equipped to manoeuvre freely. Every nodes are self-configuring in nature, this gives the node a free will to either stay or leave the network at any instance. Every node can participate in the venture of transferring the packets. The nodes keep up a correspondence through sending packets to distinct nodes within its radio range. Routing meet specified standards with a chief function in the safety of the entire network. Thus, these operations bring several security issues in MANET. The wireless link characteristics are time-varying in nature: There are transmission impediments like fading, path loss, blockage and interference that adds to the prone behaviour of wireless channels. The responsibility of wireless transmission is resisted by various factors. Packet losses attributable to errors in transmission – MANETs expertise higher packet loss attributable to factors like hidden terminals that ends up in

collisions, wireless channel problems (high bit error rate (BER)), interference, frequent breakage in ways caused.

***A.Trust and its Properties in MANET:***

The term Trust Management is known as a separate part of security services in networks and processed that Trust evaluation and management toils the assorted methodology for marking the decipher security policies, endorsement and relationships. Trust management in MANETs is required once collaborating nodes, with no previous interactions, need to determine a network with an appropriate level of trust relationships among them-selves. Additionally, trust management has numerous relevance in several higher cognitive processes like intrusion detection, authentication, access management, key management, uninflected misbehaving nodes for effective routing, and different functions. Trust management, trust update, and trust revocation, in MANETs is additionally rather more difficult than in ancient centralized environments. Further, resource constraints usually confine the belief analysis method solely to native data. The dynamic nature and characteristics of MANETs end in uncertainty and wholeness of the trust proof. The contributions of evaluating the belief value is to allow a transparent definition of trust within the communication and networking field, knowing upon the definitions from totally different disciplines and to reveal about the future analysis areas supported the thought of social and psychological feature networks. Some schemes use continuous or separate values to live the extent of trust for instance, trust is represented by never-ending price in [0, 1] or measured as separate price in [−1, 1]. Threshold based mostly approaches also are wont to live the trust.

Trust process comprise of 3 parts: experience, suggestion and learning. The experience a part of trust for each hub is straight forwardly measured by their fast neighbours. The trust table is unfold to each single different hub as suggestion a chunk of the trust.

***B. Outline of AODV:***

For enabling security ad-hoc On-Demand Routing (AODV) protocol uses Trust based approach, which overcomes the overhead and select the belief node for its packet transmission. Ad hoc Wi-Fi networks expect no pre-deployed infrastructure is on hand for routing packets end-to-result in a network, and alternatively rely on intermediary node.

Some of the intermediary nodes may act as malicious nodes and most of the attacks will also be carried out using these malicious nodes. These malicious nodes accept the route request, route response or data packets and drops it at the same time sending it to the following node. So these malicious nodes ought to be detected and avoided within the network, because the intention of those malicious nodes is to discontinue the packet exchange between the source and destination. Fig2 explains about path establishment by AODV from source to destination. When a source sends request to destination in many ways, the destination may respond to the source that have shortest path. The first node (1) indicate source and last node (6) indicates destination.

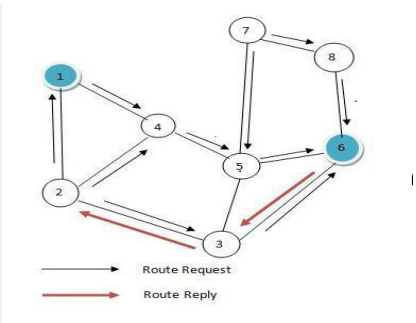


Fig 1: Path establishment in AODV Routing Protocol

## II.RELATED WORK

Rahul Patel, Maiterey Patel[1] proposed to prevent the black hole attacks in the MANET. In this method checking whether there is large difference between the sequence number of source nodes or intermediate node who has sent back RREP. If there exists much more differences between source and destination sequence number, then the Intermediate node or destination node is malicious node.

Abdul-Rahman Salem, Dr.Rushdi Hamamreh[2] projected the detection of the malicious nodes and mitigation their effects can be achieved by creating and maintaining dynamic blacklist in each node according to some criteria.

Mohammed Abdel-Azim, Hossam El-Din Salah, Menas Ibrahim[3] introduced an optimized fuzzy based intrusion detection system to detect and prevent the effect of a black hole attack.

Monika Shivhare, Prof.Praveen Kumar Gautam[4] contempt anindex based on-demand routing

protocols for knowledge transmission below black hole attack in MANET.

## III. PROPOSED WORK

### *A.Network simulation:*

Simulation is regulated using NS3. Because of the link stability and route lifetime, no route overhead was considered in our simulation. In 500 X 500 area, mobile nodes exist. Square area is used to increase average hop length of a route with relatively small nodes. Every mobile node is, moving based on the mobility data files that were generated by mobility generator module. Several 50 nodes are created. The transmission range is fixed at 100 meters. 100 nodes have destinations and try finding routes to their destination nodes. Maximum speed of node is set to 20 m/sec. The nodes are assigned with an initial position. All nodes do not stop moving and the simulation second is 500 seconds.

TABLE I
SIMULATION PARAMETERS

| Parameter | Values |
|---|---|
| Coverage area | 500m×500m |
| Simulation Time | 500s |
| No.of nodes | 50 |
| Traffic type | UDP-CBR |
| Packet Size | 512 bytes |
| Maximum Speed | 20 m/s |
| Routing Protocol | AODV |
| Mobility Model | Random Way Point |

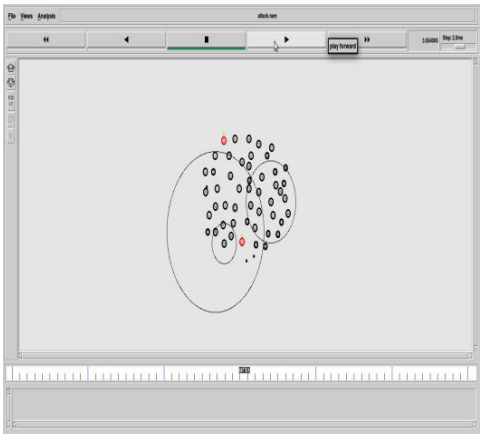

Fig 2. Network Formation

### *B. Routing operations in RAODV:*

In this novel approach three new fields has been piggybacked into each node's original routing table viz., positive events, negative events and opinion. Positive events are the efficacious communication times concerning two nodes. Afore mentioned negative events are the disastrous communication between any two entities. Opinion states the node's belief towards another node's trustworthiness as defined before. The value of opinion can be calculated per Formula 1. These three fields are the main factors when performing trusted routing in MANET.

| Destination IP | Destination Seq | .. | Hop count | ... | Life time | +ve events | -ve events | Opinion |
|---|---|---|---|---|---|---|---|---|

Fig 3. Trusted Routing

### *C. Trust Judging Rules:*

The proffered trust model is an addendum of the exemplar trust model in subjective logic. In our trust model, opinion is a 3-dimensional metric and is defined as follows:

***Definition 1***

Let T(A,B)=[b(A,B),d(A,B),U(A,B)] denote node A's opinion about node B's trustworthiness in a MANET, where the first, second and third component correspond to belief, disbelief and uncertainty respectively.

The sum up of all three values is always one. These three elements should be able to satisfy b(A,B)+ d (A,B)+U(A,B) = 1. In this definition, belief corresponds to the probability of a node B can be trusted by a node A, and disbelief corresponds to the probability of B cannot be trusted by node A.Then uncertainty fills the void inthe absence of both belief and disbelief, and sum of these three elements is always 1.

A node in MANET will convene and preserve all the positive and negative evidences concerning the other nodes trustworthiness in MANET, which will be interpreted in detail in Section 5. With these accumulated evidence, we can hoard the opinion value by exploiting the following mapping equation.

***Definition 2 (Mapping)***

Let T(A,B) = b(A,B)+d(A,B) +U(A,B) be node A's opinion about node B's trust-worthiness in a MANET, and let p and n respectively be the positive and negative evidences collected by node A about node B's trustworthiness, then T(A,B) can be expressed as a function of p and n according to:

$$b(A,B) = p/(p+n+2)$$
$$d(A,B) = n/(p+n+2)$$
$$u(A,B) = 2/(p+n+2)$$

Formula 1.

where p is positive packet transmission from A to B, n is negative packet transmission from A to B i.e., the packets that are not possibly delivered to the exact destination.

(1) If node A's opinion towards node B's trust-worthiness, the first component belief of opinion T(A,B) is larger than 0.5, A will trust B and continue to perform routing related to B.

(2) In node A's opinion towards node B's trust-worthiness, if he second component disbelief of opinion T(A,B) is larger than 0.5, A will not trust B and will refuse to performing routing related to B. Accordingly the route entry for B in A's routing table will be disabled and deleted after an expire time.

(3) In node A's opinion towards node B's trust-worthiness, if the third component uncertainty of opinion T(A,B) is larger than 0.5, then the energy of node B will be noted. If the energy level is higher, then the node B will be considered for performing the routing.

(4) In node A's opinion towards node B's trust-worthiness, if the three components of opinion T(A,B) are all smaller than or equal to 0.5, then the energy of node B will be noted. If the energy level is higher, then the node B will be considered for performing the routing.

(5) If node B has no route entry in node's routing table's opinion about B is initialized as (0,0,1).

| Belief | Unbelief | Uncertainty | Action |
|---|---|---|---|
| | | >0.5 | Request and Verify Digital signature |
| | >0.5 | | Distrust a node for an expire time |
| >0.5 | | | Trust node and continue routing |
| <=0.5 | <=0.5 | <=0.5 | Request and Verify Digital signature |

Fig 4. Trust Judging Rules

In our proposed methodology, we have enhanced the routing protocol by additionally calculating the belief, unbelief and uncertainty values before generating the path, which enhances the existing protocol. We have designed a model that identifies the malicious nodes that drops packet while forwarding and calculated the packet loss ratio and end to end delay. The calculated delay value is lower than already existed delay value without any malicious node behaviour in the network. These values are made reliable in Revised AODV

## IV. IMPLEMENTATION OF TRUST BASED ROUTING

Initially the opinion of the node can be calculated using highly trusted and least trusted. First the network formation of the node take place. Then comes route establishment of every node can be done. While establishing the route, the trust value should be calculated. For that we should obtain the trust table information.

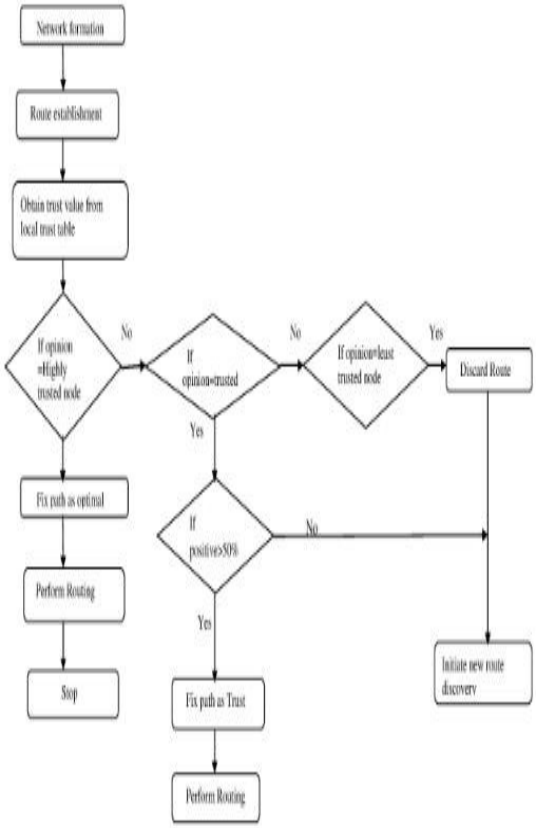


Fig 5. Trust Based Routing

The trust table information may contain three nodes as highly trusted, trusted and least trusted. If the opinion is equal to highly trusted node, then fix the path as opinion and perform the following routing. If the condition is not true, then check whether opinion is equal to trusted value then these nodes

provide 50% positive opinion and fix the path as trusted. If the node is less trusted, then discard the route and initiate new path. In the below flow chart, trust value can be calculated as explained above.

```
trust_store::trust_insert(nsaddr_t node_id, nsaddr_t prev_node,nsaddr_t next_node,int32_t trust_value)
{
  trust_entry *rp;
  //assert(tr_lookup(dst_seq_no) == 0);
  rp = new trust_entry;
  assert(rp);
  rp->node_id = node_id;
  rp->prev_node = prev_node;
  rp->next_node = next_node;
  rp->trust_value = trust_value;
  LIST_INSERT_HEAD(&trusthead, rp, trust_link);
  return rp;
}
```

Fig 6. Coding for trust table

In our paper categorize the nodes based on trust value such as highly trusted nodes, trusted nodes, and least trusted nodes.

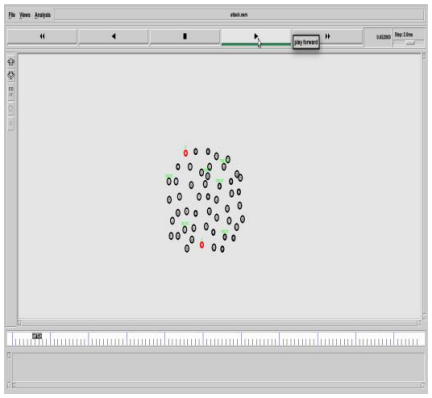

Fig 7. Identification of highly trusted nodes and trusted nodes.

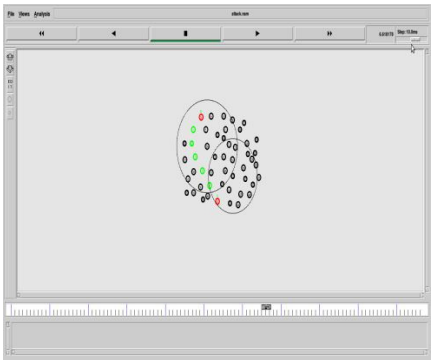

Fig 8. Constructing optimal path from source to destination via trusted nodes

This approach reveals the highly-trusted nodes in a network. Before constructing the path from source to destination it is devoir to make certain the nodes that are about to partake in the routing process are highly trusted nodes. Once the source receives RREP it pioneers trust monitoring scheme that counsels the trust value of every node in the route. The route is firmly established only if all the nodes are highly trusted or nodes that meets the threshold value. If least trusted nodes are located within the recommended route, then the route is ignored and the process is initiated again until the route is optimal. In this degree, since only trusted nodes are granted to partake in the routing process the route will always remain flawless where selfish nodes or malicious nodes are completely isolated from the routing process.

## V. PERFORMANCE ANALYSIS

Trust based Routing algorithm generates better packet delivery ratio and throughput than the existing traditional methods. The results are discussed below. Packet drop due to misbehaving nodes, traffic or congestion is estimated during runtime as shown in the figure 9.

```
if(malicious==true){
if( ch-> ptype_==PT_CBR){
drop(p,DROP_RTR_ROUTE_LOOP);
return;//Required if you get pkt flow not specified error.
//DROP_RTR_ROUTE_LOOP is added for no reason.
}
}
if(index==0)
{
if(ch->ptype_==PT_CBR){
fcount++;
}
}
```

Fig 9. To estimate the run time packet drop due to malicious node

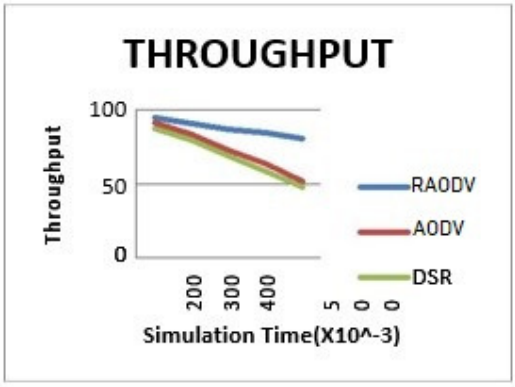


Fig 10. Variation of throughput with time

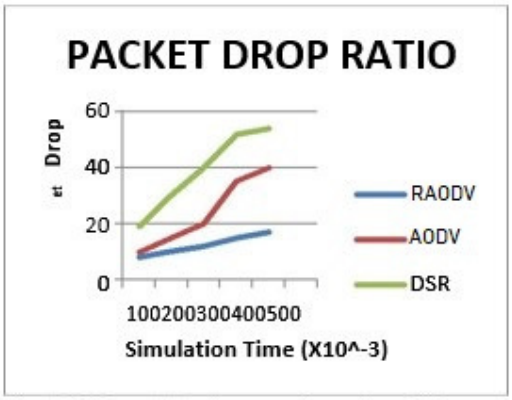


Fig 11. The relative decrease in packet delivery rate in RAODV

## VI. CONCLUSION

An ad-hoc network is a set of limited range of wireless nodes that function in a cooperative manner to increase the overall efficiency of the network. In this Paper, the malicious nodes which are one of the major impact in the network has been identified and a trusted route is established after calculating the belief value and the path is computed using RAODV routing protocol that isolates the malicious nodes from the routing process. This ends up in increased reliability Packet delivery in MANET thereby increasing the quality of service and throughput in the network. This is because RAODV protocol computes the trust values of each node andallows only the trusted nodes to get involved in the routing process. Our future work is to implement RAODV protocol for alternate threats in MANET.

## REFERENCES

[1] Rahul Patel, Maiterey Patel "Preventing DSR Protocol against Black Hole Attack for MANET" International Research Journal of Engineering and Technology, Vol:03, Issue:06, 2016

[2] Abdul-Rahman Salem, Dr.Rushdi Hamamreh "Efficient Mechanism for mitigating Multiple Black Hole Attacks in MANET" Journal of Theoretical and Applied Information Technology, Vol:83, Issue:01, 2016

[3] Mohammed Abdel-Azim, Hossam El-Din Salah, Menas Ibrahim "Black Hole Attack Detection using Fuzzy based IDS" International Journal of Communication Networks and Information Security, Vol:09, Issue:02, 2017

[4] Monika Shivhare, Prof.Praveen Kumar Gautam "Prevention of Black Hole Attack in MANET using Indexing Algorithm", International Journal of Engineering Science and Computing, Vol:07, Issue: 06,2017

[5] Royer, Elizabeth M. and Chai-Keong Toh, "A review of current routing protocols for ad hoc mobile wireless networks", Personal Communi-cations IEEE 6(2) 46-55 (1999).

[6] B. Kannhavong, H. nakayama, Y. Nemoto and N. Kato, "A survey of routing attacks in mobile ad hoc networks", Wireless communications IEEE 14(5): 85-91 (2007).

[7] Zapata, Manel Guerrero, "Secure ad hoc on-demand distance vector routing", ACM SIGMOBILE Mobile Computing and Communications Review 6(3): 106-107 (2002).

[8] S. Yi, P. Naldurg, and R. Kravets, "Security-aware ad hoc routing for wireless networks", Proc. ACM Mobihoc (2001).

[9] Papadimitratos, Panos, and Zygmunt J. Haas, "Secure routing for mobile ad hoc networks", the SCS Communication Networks and Distributed Systems modeling and Simulation Conference (CNDS), San Antonio, TX, January 27-31 (2002).

[10] Sanzgiri, Kimaya, et al., "A secure routing protocol for ad hoc networks", Network Protocols, Proceedings. 10th IEEE International Conference on IEEE (2002)

[11] Hu, Yih-Chun, Adrian Perrig and David B. Johnson, Ariadne, "A secure on-demand routing protocol for ad hoc networks", Wireless networks 11(1-2): 21-38 (2005).

[12]Abusalah, Loay, AshfaqKhokhar and Mohsen Guizani, "A survey of secure mobile ad hoc routing protocols", Communications Surveys & Tutorials, IEEE 10(4): 78-93 (2008).

[13] Li, Xiaoqi, Michael R. Lyu and Jiangchuan Liu, "Trust model based routing protocol for secure ad hoc networks", Aerospace Conference Proceedings IEEE Vol. 2 (2004).

[14] Chandni Garg1, Prashant Rewagade, "Trust Evalua-tion for Detecting Black Hole Attack on AODV Routing Protocol by using Back Propagation Algorithm of Neural Network", Proc. of Int. Conf. on Advances in Computer Science and Applica-tion Pp. 775 - 780 (2013)

[15] Eric Chiejina, Hannan Xiao and Bruce Christianson, "A Dynamic Reputation Management System for Mobile Ad Hoc Networks", Computers 4: 87-112 (2015).