Journal of Engineering Design and Analysis
Volume 4, Issue 1 - 2021, Pg. No. 20-33
Peer Reviewed Journal

Article

Preventing Black Hole Attack in AODV Routing Protocol Using

Bhawna Gupta[1], AK Verma[2], LR Raheja[3]

[1]Professor, Geeta Engineering College, Panipat.
[2]Professor, Thapar University.
[3]Professor(Retd.), IIT Kharagpur.

I N F O

Corresponding Author:
Bhawna Gupta, Geeta Engineering College, Panipat.
E-mail Id:
bhawnaguptacse@yahoo.co.in
How to cite this article:
Gupta B, Verma AK, Raheja LR. Preventing Black Hole Attack in AODV Routing Protocol Using. *J Engr Desg Anal* 2021; 4(1): 20-33.

Date of Submission: 2021-04-20
Date of Acceptance: 2021-05-03

A B S T R A C T

Detection of black hole is a challenging task. Further, isolating such malicious nodes from communication is also a great challenge. Several previous works addresses trust based model for detection and prevention of malicious nodes. Trust based models will consume time to study the neighbor transmissions and will try to identify trustable nodes based on their data forwarding behavior. But this approach will need considerable quantity of time to identify malicious nodes by constantly monitoring the traffic of the neighbor nodes. Another drawback in this model is, false positives – that is, the standard trust based detection mechanisms may wrongly mark a trustable node as non-trustable node if that node, by chance, is not participating in communication even without any bad intention. In this work, the performance of the algorithm is increased using a Dynamic Trust Handshake based detection mechanism (DTH-AODV). Dynamic Trust Handshake based detection mechanism will detect the malicious nodes very quickly and efficiently in a short time military rescue like MANETSscenario without much increase in overhead. To prove its better working, a MANETSshort time communication scenario is simulated and the performance of standard AODV with and without black hole attack is measured using NS2.35 and compared it with Dynamic Packet Forwarding based Trust AODV (DTH-AODV) protocol in terms of different metrics like total number of packets sent received and dropped, throughput, EED, battery consumed etc. The proposed DTH-AODV will use a Dynamic Trust Handshake mechanism for the reliable detection of malicious behavior in MANET.

Keywords: AODV, DTH-AODV, Dynamic Trust Handshake, Performance, Throughput

Introduction

Mobile Adhoc network (MANET)[1] is a collection of nodes in wireless network in which nodes keeps on changing its position to have a dynamic topology. Topology keeps on changing therefore the path from source node to destination node also keeps on changing which further is determined by routing protocol. In this work, we are using the reactive routing protocol called Adhoc On Demand Distance Vector Routing Protocol (AODV)[2,3] where the route is determined on demand i.e. whenever there is a requirement of route then and only then current route from the source to destination is determined.[4-9] AODV routing protocol has several vulnerability such as:

a. A malicious node can drop any of the control packet or

data packets.

b. A malicious node can modify any field of the control packet and can then forward the packet to its immediate neighbor.
c. The malicious node can send the faked RREP or route reply acknowledgment (RREP_ACK) in response to the control message or it may send fake response message of its own.
d. In such way, the malicious node may cause the route breakage which may lead to node isolation or flooding of packets which may lead to resource consumption. Due to property that malicious node can also modify fields of the control packet, the malicious mode may impersonate any other node or it may leak the confidential information to the unauthorized node.

In AODV routing protocol, the working depends on the genuine cooperation of node. If any of the intermediate nodes is selfish or non-cooperating or malicious, then the working of complete protocol is compromised. Attacks are targeted to damage basic aspects of security like integrity, confidentiality and privacy. The nodes performing adverse effects on MANETS are classified into two categories: malicious node[10] and selfish node.[11] Malicious nodes are those nodes that perform an active attack on MANETS and may be active in route establishment or data forwarding phase, while selfish node performs passively by not forwarding the packet just for sake of saving battery energy.

Due to above said vulnerabilities a number of attacks[12-20] are possible in AODV routing protocol. These attacks are broadly classified into two categories called passive or active attack.

Passive Attack

In a passive attack, the attacker's goal is just to obtain information. This means that the attack does not modify data or harm the system. However, the attack may harm the sender or receiver of the message. Main techniques of passive attack are: eaves dropping and timing analysis.

Active Attack

Active attack may change the data or harm the system. Attacks that threaten integrity and availability are active attacks. Examples of active attacks on AODV are:

- Attacks by dropping the packets: Such as Blackhole[21-30] or Gray hole attack.[31]
- Attacks using modification of protocol message: It may include redirection due to modification of Hop-Count or Modified Destination Sequence number. A Very Common Attack in this category is Denial of Service attack[32-34] where the malicious nodes generate unwanted request packets so as to make the resources unavailable to the other nodes.
- Attacks using impersonation where malicious node impersonates other node.
- Attacks using fabrication: Here, Malicious nodes generate false route error message or false routing table overflow message.
- Other attack Such as Worm Hole attack[35-38] or Byzantine Attack[39,40], etc.

This paper focuses mainly on blackhole attack. In Blackhole attack, the malicious node intends itself as having the shortest path through it. Once it is chose as the intermediate node for the path from source to destination, it drops all the control packets and data packets that are transmitted through it. So, it impacts the performance of the protocol.

Implementation of Black Hole Attack in Aodv Routing Protocol

Black hole Attack

Black hole problem is type of active attack in which malicious node first claims to have the shortest path. Source node chooses the route containing the malicious node to the destination. Once the traffic is routed through itself, it drops the entire data packet routed through it.[41-44] As shown in Figure 1, let 1 be the source node and 3 be the destination node and 4 is the malicious node. 4 claims to have the shortest path that is why route through 4 (1-4-5-6-3) is selected instead of 1-2-3. But after being selected in the final route 4 drops the entire data packet. The working of black hole attack is further summarized in Figure 2. The figure shows that if the packet forwarded is data packet and the node is malicious, then it drops the entire packet. Otherwise, if the packet if RREQ control packet and the node is malicious then it sends the fake RREP so as to claim itself as having the shortest path. Once it is chosen as the intermediate node, it drops the entire data packet routed through it. In all other cases, it behaves normally.[88-90]

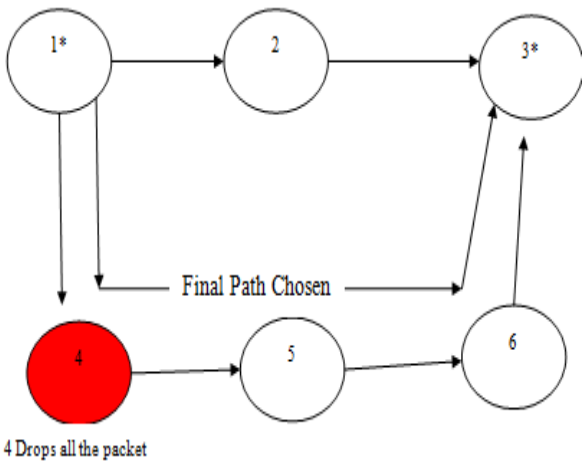

Figure 1.Example showing the working of black hole attack where 1 is the source node, 3 is the destination node and 4 is the malicious node

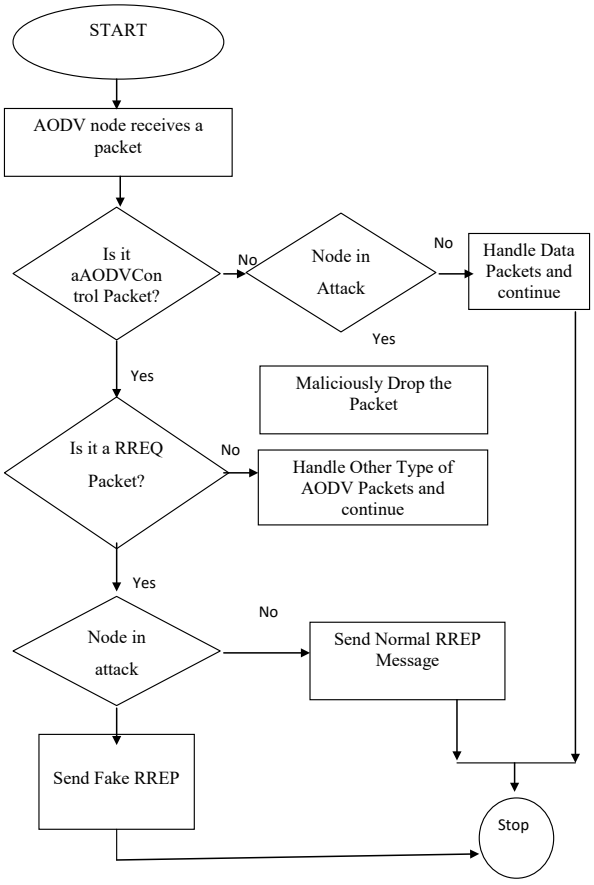

Figure 2.Pseudo code of AODV routing Protocol

Proposed Work

A lot of research work has been done to find the secured AODV routing algorithm.[45-54] The trust[55-58] based on the packet forwarding behavior of neighbor can be used for detecting misbehavior. This model has been previously presented in several literatures.[59-63] But, by the same trust based logic, some of the neighbors those who were silent and not actively participated in communications will get wrongly identified as malicious. So, simple trust based models will mark a lot of non malicious nodes as malicious nodes. This will initiate lot of link failures. That is, the link between source to destination will get broken at different locations on their path because of this false identification of malicious nodes.

The dynamic packet forwarding based trust AODV (DTH-AODV) proposed in this paper will overcome that problem and reduce the possibility of such false marking of non malicious nodes as malicious nodes. A simple Dynamic Trust Handshake mechanism will help to prevent such false identification.

The main advantage of the proposed detection and prevention scheme is: it will detect and prevent the malicious nodes in the very early stage of AODV route discovery process. So, it will not need any manipulation in routing tables in the route resolving process, because, by the design, it will avoid including malicious hops in routing table even at the route discovery process itself.

In this work, trust value is associated with each node and initialized to 0. If the node is working genuinely i.e. forwarding the packet as per the routing protocol instruction then trust value is incremented otherwise it is decremented.

```
void TrustNode::increaseTrust ( )
{
        trustValue++;
}
void TrustNode::decreaseTrust ( )
{
        trustValue--;
}
```

Figure 3.Calculation of trust values

Malicious and faulty nodes are then isolated from the network once they obtain a minimum threshold value.

```
bool Trust Node::is Node Trusted ()
{
        if (trust Value < = threshold value)
        {
                return false;
        }
                else
        {
                return true;
        }
}
```

Figure 4.Calculation of Malicious Node

Packets Acknowledgment: Acknowledgment is a method of ensuring that packets sent for forwarding have been forwarded. There is a couple of ways that this is possible but Passive Acknowledgment is by far the easiest to implement. Passive Acknowledgment uses promiscuous mode to monitor the channel, this allows the node to detect any transmitted packets, irrelevant to the actual destination that they are intended for. With this, the node can ensure that packets it has sent to a neighboring node for forwarding are indeed forwarded. This has been implemented within PTH-AODV using promiscuous mode to monitor the channel.

Packet Precision: As defined by Pirzada et. al.[64] Packet Precision ensures the integrity of the data and control packets that are either received or forwarded by other nodes in the network. This type of detection aims to spot packets that have either been corrupted due to a faulty node or have been generated maliciously. This could be done by monitoring the control packets that lead to suitable successful routes. Another possible means is to check the packet information is within certain tolerances. For example,

it may be ensured that the sequence number within a reply is not inconceivably higher than the sequence number within the request, as this suggests that the replying node is trying to ensure it is part of the final route.

Destination Unreachable Messages: Although Pirzada[64] mentions that it is possible to use Destination Unreachable Messages, no such messages are returned by Ns2.

Implementation of The Proposed Malicious Behavior Detection in AODV

Implementation of Dynamic Trust Handshake Mechanism

Generally, a trust factor based on the packet forwarding behavior of neighbor can be used for detecting misbehavior as previously presented in several literatures. For example, a trust factor of a node can be derived based on the number of forwarded packets at that neighboring node. But, by the same trust based detection logic, some of the neighbors.

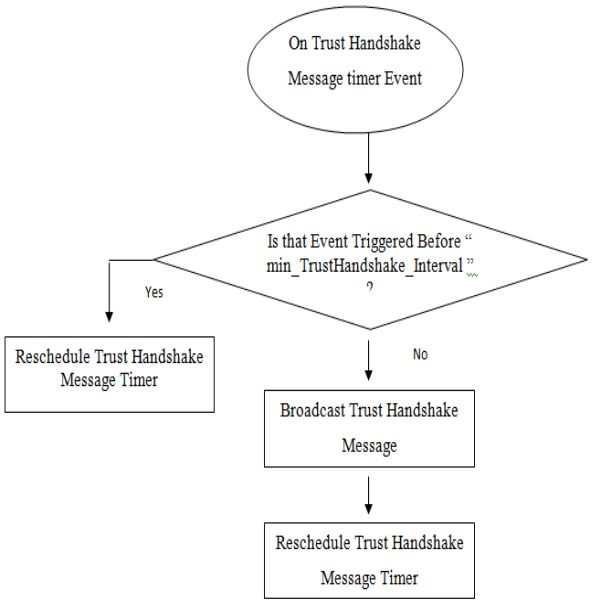

Figure 5.The Dynamic Trust Handshake Mechanism

those who were silent and not actively participated in communications will get low trust factor and will be wrongly identified as malicious. Because of this, the link between source to destination will get broken at different locations on their path because of this false identification of malicious nodes. In our proposed dynamic trust handshake based AODV (DTH-AODV), it will overcome that problem and reduce the possibility of such false marking of non malicious nodes as malicious nodes by introducing a Dynamic Trust Handshake mechanism. The following flow diagram in Figure 5, explains the implementation of Dynamic Trust Handshake Mechanism in AODV routing agent.

The Trust Handshake Message Triggering Mechanism. In this model, the nodes will send a "trust handshake" in a dynamic fashion based on its local state. This Dynamic Trust Handshake mechanism ensures that at least one handshake packet will be send just before any new transmission event. But the frequency of such "trust handshake" message will be controlled by two variables the min_TrtustHandshake_ Interval and max_TrtustHandshake_Interval. So, it will not increase the message overhead tremendously.

The trust handshake message function will be called from different function of AODV whenever a change in state is expected. For example, after doing a regular route table update, the trust handshake message function will be triggered. But according to the way in which The Dynamic Trust Handshake Mechanism working, it will not actually send a handshake message whenever it is triggered. The trigger mechanism may rapidly call the trust handshake message sending function, but it will actually send a new message if an only if there was a considerable gap (min_TrtustHandshake_Interval) between two consecutive messages. This will avoid over sending the Trust Handshake messages. The following flow diagram explains the implementation of Dynamic Trust Handshake Based Malicious Node Detection and Prevention in AODV routing agent.

The process flow and pseudo code of Dynamic Trust Handshake Based Malicious Node Detection and Prevention in AODV routing protocol is shown in Figure 6 and 7.

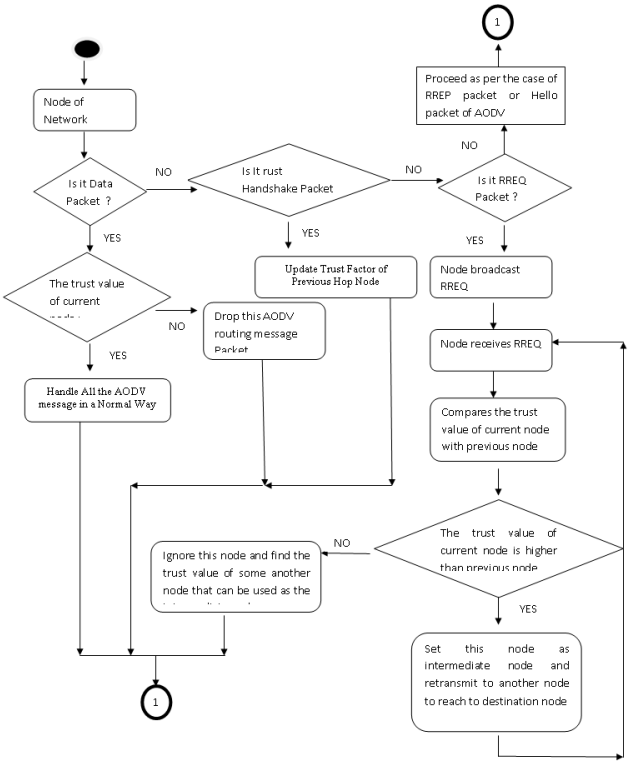

Figure 6.The process flow of Periodic Trust Handshake Based Malicious Node Detection and Prevention in AODV

```
Forward (RREQ pkt, delay) {
        // the node receives the RREQ control packet
        // checks whether it is destination node
        if destination{
                //considers the path with highest trust value and sends the route reply along thatpath
                compute_highest_trust_level ()
                        {
                        // the optimal path with highest value value is chosen and route reply is sent along that path
                        highest_trust_value(path)
                        sends_RREP_to_source
                        }
        else (not_destination){
                // if the next intermediate node is not destination then intermediate node checksfor the packet by
                computing the trust level
                ifRREQ_packet{
                compute_trust_level ()
                        {
                        // compares the trust value of current node with the tryst value of previousnode
                        trust_current_node>trust_previous_node
                        }
                if (found not ok)
                // intermediate node drops the packet if its trust level is lesser then previous path
                drop(pkt)
                else  {
                // if the new path has more trust value then update trust and hop count andrebroadcast it to next
                neighbour node
                trust++
                // total number of intermediate nodes is incremented by 1
                hop_count++
                // the RREQ packet is rebroadcasted to next neighbour node
                rebroadcast RREQ
                                }
                        }
                }
                }

Receive (RREP pkt, delay) {
                //waits for specified period
                ifno_duplicate{
                        wait_rrep_wait_time
                        update_trust_metric
                        updatenext_hop}
                        else
                        {
                        computetrust_path
                        }
                }
Update_Trust_Metric (interval){
        //wait for the minimum trust handshake interval
        wait_trust_handshake_interval();
        broadcast_trust_hanshake;
        trust_value>trust_threshold {
```

```
trust_current_node = trust_current_node + trust_previous_node
        }
else {
        drop (pkt);}
}
```

Figure 7.The Pseudo code of PTH-AODV

The Changes Made in NS2 AODV code for Malicious Node Detection and Prevention

The following two files were modified to incorporate the proposed malicious node detection and prevention mechanism in AODV routing agent.

Changes Made in AODV.h

The additional function definitions for detection and prevention of malicious behavior and the variables that will be bound with TCL are declared in AODV.h. By using the variables from a TCL simulation code, we can control the behavior of the routing agent and bring it to detection and prevention mode.

Changes Made in AODV.cc

The actual code of the additional function definitions for detection and prevention of malicious behavior were implemented in AODV.cc. And here the new interfaces to the code through the control variables that will be bound with TCL are written here. By setting the variables from a TCL simulation code, we can control the behavior of the routing agent and bring it to detection and prevention mode.

The Functions Modified for Attack Detection and Prevention

The function TrustHandshakeTimer()

The Dynamic Trust Handshake Mechanism is implemented with the help of a new timer function in AODV.

The function AODV::Send Trust Handshake Packet()

This function will generate a Trust Handshake packet and transmit it with respect to the conditions explained in the Figure 4.

The function AODV::recvAODV()

In this function, the trust based detection of malicious behavior has been implemented. As shown in the figure4 of previous section. The malicious behavior detection is done based on the trust factor of the previous hop node from which the message was received.

Results and Discussion

We used network simulator version NS2.35 under Ubuntu linux operating system for obtaining this results.[65] We have implemented the black hole attack as well as attack detection and prevention mechanism on the AODV code of NS2 and did the simulation with the parameters presented in this section and evaluated the performance with respect to the metrics discussed in this section.

The Simulation Parameters

Common Parameters: The following common parameters are used for setting up the network. Moreover following parameters are also used to set TCP/UDP flows.

Variable Parameters: The following parameters are used

Table 1.Parameters values of Network in NS2

Common parameters	Values	Traffic parameters for TCP flows	Values
Topographical Area (m*m)	1800 X 500	Transport Agent	TCP
Mobility	20m/s	No Flows	10
Pause Time	20s	Traffic Type	CBR
Total SimulationTime	100s	Packet Size	1KB
Routing Protocol	AODV	Interval	100ms
Mobility Modal	RandomWaypoint	Rate	10KB
Channel Model	WirelessChannel	Traffic parameters for UDP flows	Values
Propagation Model	TwoRayGround	Transport Agent	TCP
PhyModel	WirelessPhy	No Flows	10
MacModel	802_11	Traffic Type	CBR
AntennaModel	OmniAntenna	Packet Size	1KB
Queue	DropTail-PriQueue	Interval	100ms
Queue Length	50	Rate	10KB

as variables for analyzing the impact of the attack and detection on different condition.

Analytic Results With Respect to Different Network Size

Here we see the analytic results of comparison of black hole attacks with normal AODV (it means performance without any attack). And it is studied with respect to different network size. In the following analysis the total number of nodes in the network is varied as 40, 50 and 60 and among them, the number of malicious nodes kept as 15 and the impact is measured using different metrics.

The following line graph in Figure 8, shows the impact of attack and detection and prevention mechanism in terms of total data packets sent at application source. As shown in the line graph, under the presence of Blackhole Attack, the application source itself can not able to send much. But while detection the proposed DTH-AODV was able to send as much as normal AODV without any attack.

Table 2.Total number of nodes, number of malicious node and different attack scenarios

Parameters	Values
Malicious Nodes	15
Total Nodes	40,50,60
AODV with	a) No Attack b) Black Hole Attack c) PTH Attack Detection

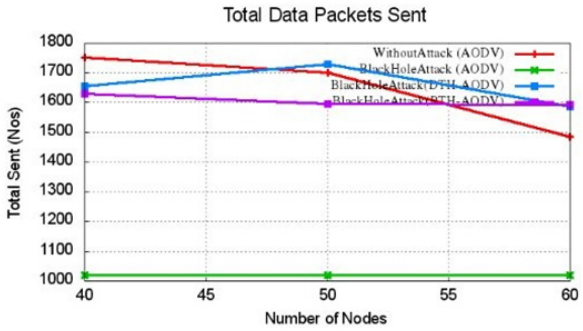

Figure 8.Network Size vs Sent Packets

The following line graph in Figure 9, shows the impact of attack and detection and prevention mechanism in terms of total data packets received at application destination. As shown in the line graph, under the presence of Blackhole Attack, destination itself is not able to receive anything. But while detection the proposed DTH-AODV was able to receive as much as normal AODV without any attack.

The following line graph in Figure 10 shows the impact of attack and detection and prevention mechanism in terms of routing load. As shown in the line graph in Figure 10, under the presence of Blackhole the routing load is very high. But with proposed DTH-AODV based detection and prevention

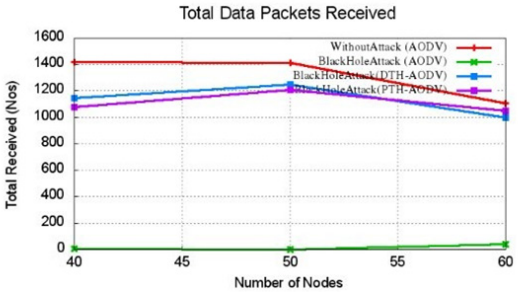

Figure 9.Network Size vs Received Packets

mechanism, the routing load was almost equal to that of normal AODV. In terms of routing load, the performance of Normal AODV, proposed DTH-AODV are almost equal.

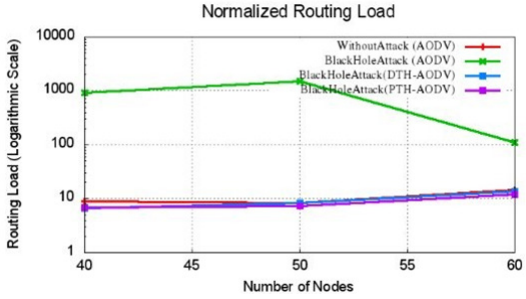

Figure 10.Network Size vs Routing Load

The following line graph in Figure 11, shows the impact of attack and detection and prevention mechanism in terms of MAC load. As shown in the line graph, under the presence of Blackhole the MAC load is very high. But with proposed DTH-AODV based detection and prevention mechanism, the MAC load was almost equal to that of normal AODV. In terms of MAC load, the performance of Normal AODV, proposed DTH-AODV are almost equal.

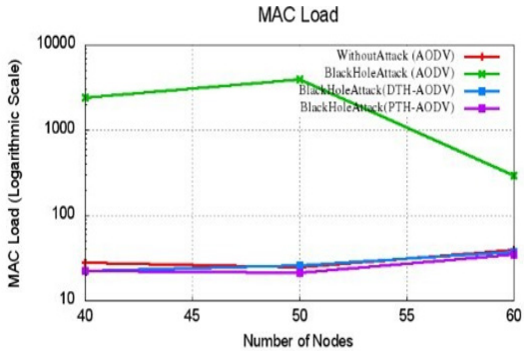

Figure 11.Network Size vs MAC Load

The following line graph in Figure 12, shows the impact of attack and detection and prevention mechanism in terms of total dropped packets at application layer. As shown in the line graph, under the presence of Blackhole Attack the lot of packets were dropped at application layer. But while detection, the packet dropping of proposed DTH-AODV was very much reduced and al most equal to that of normal AODV without any attack. In terms of application layer dropped packets, the proposed DTH-AODV dropped little

bit high number of packets this is because, the DTH-AODV will try to send more packets than Normal AODV.

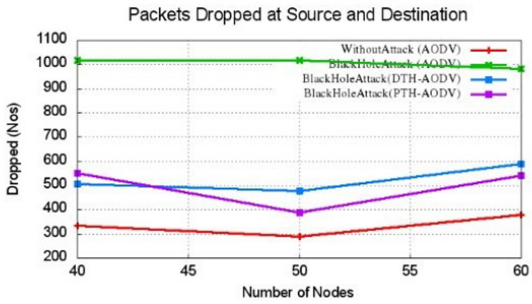

Figure 12.Network Size vs Packets Dropped at Application Layer

The following line graph in Figure 13, the impact of attack and detection and prevention mechanism in terms of throughput. As shown in the line graph, under the presence of Blackhole Attack the throughput was almost equal to zero. But with detection, the throughput of proposed DTH-AODV was very much improved and almost equal to that of normal AODV without any attack.

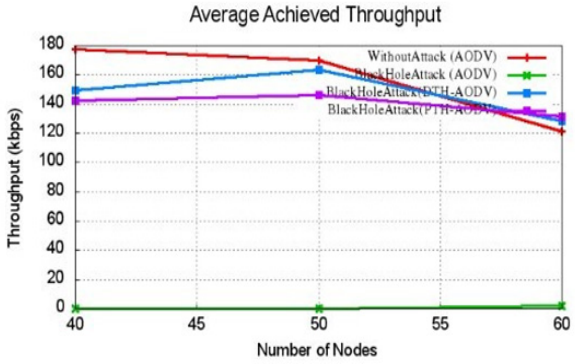

Figure 13.Network Size vs Throughput

The following line graph in Figure 14, shows the impact of attack and detection and prevention mechanism in terms of PDF. As shown in the line graph, under the presence of Blackhole Attack the PDF was almost equal to zero. And at low network density PDF is equal to zero. For example, at 40 nodes, it is zero because, among the 40 nodes, 15 are malicious- so that they will able to break all the communication between other nodes. But with detection, the PDF of proposed DTH-AODV was very much improved and almost equal to that of normal AODV without any attack. In terms of PDF, the performance of Normal AODV, proposed DTH-AODV are almost equal.

The following line graph in Figure 15, shows the impact of attack and detection and prevention mechanism in terms of End to End Delay (EED) of data flows. With respect to the increase of no of nodes in the network, the performance getting decreased. As shown in the line graph, Blackhole Attack seems to be providing lower EED than normal AODV

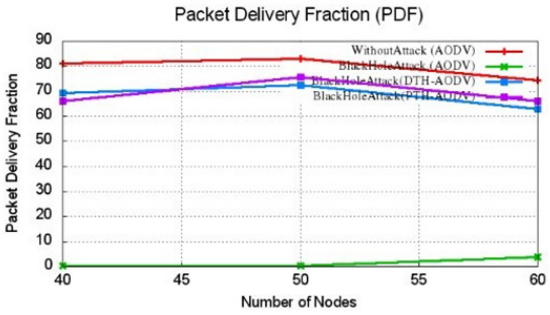

Figure 14.Network Size vs PDF

(without attack) but certainly it does not mean that Black hole Attack is improving the performance of the network. The low end to end delay under attack is due to a strange fact that the attack makes disconnection in TCP flows and since the packets are not at all forwarded to any further nodes, indirectly it is reduce the message overhead in the network and reduced bandwidth usage otherwise it will be consumed by the forwarded data packets. So, the flows that were unaffected by Blackhole Attack (the connections where there is no neighboring attack nodes) utilizes that extra bandwidth and gains some performance. Further, keep in mind that the end to end delay is only calculated based on the time in which a packet is sent and received. So if a packet is not received, in that case end to end delay can not be calculated. So this average EED is only the average EED of successfully delivered packets.

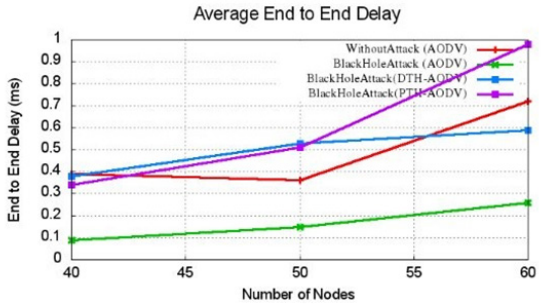

Figure 15.Network Size vs End to End Delay

The EED of DTH-AODV was little bit higher than normal AODV. Because, under attack detection and prevention, alternate route will be resolved by avoiding malicious nodes on a path, So that the path length will get increased and hence will increase the end to end delay.

The following line graph in Figure 16, shows the impact of attack and detection and prevention mechanism in terms of consumed battery energy. As shown in the line graph, in the presence of Attack the battery consumption is lesser than Normal AODV (without attack) but certainly it does not mean these Attacks are improving the performance in terms of energy consumption. The low energy consumption under attacks are due to a strange fact that these attacks makes disconnection in data flows and since the packets are not

at all forwarded to any further nodes, indirectly it is reduce the battery consumption at the other nodes otherwise it will be consumed for forwarding the data packets. So, the nodes that were unaffected by Attacks (where there is no neighboring attack nodes) preserves some battery power. Understanding this strange fact requires a better visualization of the whole network scenario. It is simple without any attack, AODV was able to send much and maximum nodes were able to participate in that communication and utilized their energy for transmission/ forwarding of packets so that the energy is consumed in most of the nodes. But in the presence of attack, the packets are getting dropped intermediately and the battery powers on other nodes that are not at all forwarding the packets get preserved. With respect to the increase of no of nodes in the network, the performance seems to be getting decreasing.

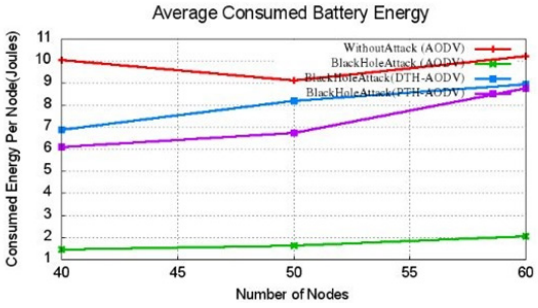

Figure 16.Network Size vs Battery Energy

But, interestingly, the energy consumption in the case of proposed DTH-AODV is little bit lesser than normal AODV. This obviously proves the better working of proposed detection model.

Lot of previous papers saying that the attacks will increase energy consumption. Of course, it also may be true but not in the same sense. For example if an application will continuously try to send data under attack, then the battery of the sending node and some other nodes between sender and attacker nodes will get reduced rapidly. If the application will vigorously try to do retransmission due to loss, then this will increase the energy consumption. But the transport protocol will handle loss scenario and just reduce the sending rate to avoid further loss. That is why the average energy consumed in the network seems to be getting reduced under attack. Understanding this strange fact requires a better visualization of the whole network scenario.

The following line graph in Figure 17, shows the impact of attack and detection and prevention mechanism in terms of overhead. As shown in the line graph, under the presence of Blackhole the overhead is minimum because, the black hole just breaks all the communication. But with proposed DTH-AODV based detection and prevention mechanism, the overhead becomes equal to that of normal AODV – it signifies that the proposed DTH-AODV works almost equal to normal AODV.

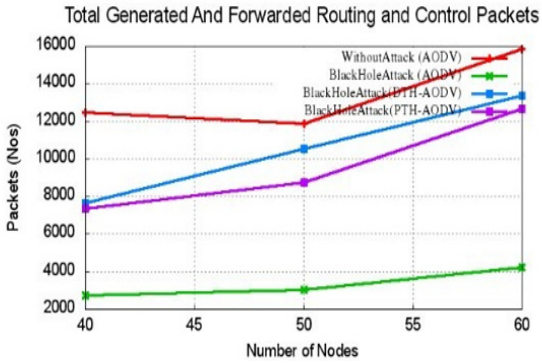

Figure 17.Network Size vs Overhead

Table 2.Comparison of characteristics of existing AODV based trust routing protocol with PTH-AODV and DTH-AODV

Secure Routing Algorithm	Characteristics	Advantages	Disadvantages
Collaborative Trust-Based Secure Routing against Colluding Malicious Nodes (T. Ghosh et. al. [66])	This Protocol design assumes the prior distribution of trust to all the nodes. This protocol also assumes the presence of public key infrastructure because whenever the node transmits RREQ message containing trust metric to intermediate node, the next node authenticates the previous node by signing with its private key.	This protocol is highly resistant towards attack where a malicious node claims to have genuine identity such as	This protocol aims to find the shortest path to the destination node irrespective of presence of malicious node therefore it is more susceptible to internal attacks. The prior distribution of trust makes the network less dynamic and adaptable to changing situations. The Use of Public key infrastructure makes the protocol highly expensive to use and it also causes more overhead to maintain all the keys. This protocol fails under the situation of compromised node.

Trust-Embedded AODV (T-AODV) (T. Ghosh et. al. [67])	This Protocol is an extension of 131 with the difference that the trust factor is periodically updated by the exchange of routing messages. However this protocol also assumes the existence of public key infrastructure and it also assumes the radio rage of all the node are same which is more theoretical to study.	In this protocol the following actions done by the malicious node is avoided. If the malicious node provides the wrong information in the RREQ packet by changing the hop count field r the destination address etc. If the malicious node decrypts the sign given by the genuine node with the intention to alter the information given in the header. It is more adaptale to topology changes	This protocol faikls to find the secure end-to-end path from source to destination. More overhead of public key infrastructure.
Trust Establishment in Pure Ad-hoc Networks [68]	This protocol does not require trusted third party infrastructure for its operation. All node computer the trust value based on direct feedback	Malicious node are bypassed during route discoveries. This protocol achieves better throughput in presence of malicious node.	Extra overhead in added due to nature of the protocol. The accuracy of protocol depends on the weight values that are assigned in the calculation of trust values. This protocol is more susceptible to IP spoofing attack and MAC spoofing attack. This protocol fails when the malicious node collude.
Opinion Based Trusted Routing Protocol – TAODV [69]	This Protocol uses soft encryption technique.	The encrypted parts of message are forwarded through different routes so malicious node hardly have access to complete message	This protocol is suceptibe to internal attack. It takes more time in route selection. It is also possible not to route all the messages securely
Friendship based routing algorithm – frAODV [70]	Each node stores the list of friends nodes and friendship value. The friendship value determines the level of trustworthiness. During control packet transmission the friendship balue is also exchanged between the nodes.	The performance gives better results for the more dynamic network.	The experiment is performed based on 5 number of nodes so the performance of protocol for the large number of node is undetermined.

DTH-AODV	This protocol does not require public key infrastructure. It also do not use any encryption technique. The However the Trust value is exchanged by the nodes only when there is a need of route establishment and the trust value depends on the feedback given by the previous neighbour in the successful communication.	Additional overhead caused by periodic exchange of trust metric is also avoided. This protocol detects all the selfish and malicious node due to exchange of trust value between the nodes. Moreover sometimes some genuine node that are not participating in the communication for over a long time are falsely interpreted as the selfish node. This protocol also avoids false accusation of genuine node as the selfish node.	More work can be done in case of trust dispersal and trust decay over time. Trust can also be gathered by the malicious scenarios. More work can also be done in case of malicious colluding nodes.

Comparison of DTH-AODV with other Trust Based Routing Algorithm

The Table 2 compares the characteristics of conventional AODV based trust routing algorithm with newly developed algorithm DTH-AODV.

Table 2: Comparison of characteristics of existing AODV based trust routing protocol with PTH-AODV and DTH-AODV

Conclusion

In this work we proposed a dynamic trust handshake based detection of black hole attack. We implemented out DTH-AODV under NS2 and compared its performance with the results of Standard AODV and Standard AODV under attack. The main advantage of the proposed DTH-AODV is : it will detect and prevent the malicious nodes in the very early stage of route discovery process. So, it will not need any manipulation in routing tables in the route resolving process, because, by the design, it will avoid including malicious hops in routing table of normal nodes at the route discovery process itself.

A lot of simulation and analysis is done to arrive at significant and interpretable results. The impact of the attack is measured on the detection and prevention mechanism with suitable metrics and explained the improvements in performance. According to the arrived results, proposed dynamic trust handshake based malicious node detection and prevention mechanism worked good and successfully detected black hole nodes in the network and avoided establishing routes though them. As shown in the results of the previous section, the proposed DTH-AODV improved the throughput and PDF almost equal to that of Normal AODV. In this work, we used unencrypted trust handshake messages in the design. But in future works, we may explore the possibility of using a private key/public key based encryption mechanism for more secure operation. It may increase the operational overhead, so that one may address issues related with overhead due to encryption based trust handshake mechanism.

References

1. Chlamtac, Imrich, Conti M et al. Mobile ad hoc networking: imperatives and challenges. *Ad hoc networks* 2003; 1.1: 13-64.
2. Perkins, E Royer. Ad Hoc On-Demand Distance Vector Routing. 2nd *IEEE Wksp. Mobilecomp Sys and Apps* 1999.
3. Kaur, Dilpreet, Kundra S. Comparative Analysis and Improvement in AODV Protocol for Path Establishment in manets. *International Journal of Computer Science and Information Security* 2016; 14.12: 213.
4. Sajid, Ahthasham et al. Performance Evolution of Reactive, Proactive and Hybrid Routing Protocols in MANET. *International Journal of Computer Science and Information Security* 2016; 14.12: 144.
5. Kodole, Amruta, Agarkar PM. A survey of routing protocols in mobile ad hoc networks. *Multi-Disciplinary Journal of Research in Engineering and Tech* 2015; 2.1: 336-41.
6. Neeli, Jyoti, Cauvery NK. Comparative Study of Secured Routing Protocols in Wireless Ad hoc Networks: A

Survey." International Journal of Computer Science and Mobile Computing 4.2 (2015): 225-229.

7. Royer EM , Toh CK. A Review of Current Routing Protocols for Ad-hoc Mobile wireless networks. *IEEE Personal Communications Magazine* 1999; 46-55.
8. Verma AK, Dave M, Joshi RC. Classification of Routing Protocols in MANET. *National Symposium on Emerging Trends in Networking & Mobile Communication* (NSNM-2003) 2003; 132-139.
9. Abolhasan M, Wysocki T, Dutkiewicz E. AReview of Routing Protocols for Mobile Ad hoc Networks. *Ad Hoc Networks* 2004; 2(1): 1-22.
10. Khan, Saleem M. Isolating Misbehaving Nodes in MANETS with an Adaptive Trust Threshold Strategy. *Mobile Networks and Applications* 2017: 1-17.
11. Das, Debjit, Majumder K et al. Selfish node detection and low cost data transmission in MANET using game theory. *Procedia Computer Science* 2015; 54: 92-101.
12. Khan, Saleem M, Jadoon QK et al. A Comparative Performance Analysis of manetsrouting Protocols under Security Attacks. *Mobile and Wireless Technology 2015. Springer Berlin Heidelberg* 2015; 137-145.
13. Ferdous, Raihana, Muthukkumarasamy V. AComparative Performance Analysis of manets Routing Protocols in Trust-Based Models." Computational Science and Computational Intelligence (CSCI), 2016 *International Conference on. IEEE* 2016.
14. Simaremare Harris. Security and performance enhancement of AODV routing protocol. *International Journal of Communication Systems* 2015; 28(14): 2003-2019.
15. Gharehkoolchian, Mahsa AM, Hemmatyar A et al. Improving Security Issues in MANETS AODV Routing Protocol. International Conference on Ad Hoc Networks. *Springer* International Publishing, 2015.
16. Ngadi, Md A, Khokhar RH et al. A Review Current Routing Attacks in Mobile Ad-hoc Networks. *International Journal of Computer Science and Security* 2008; 2(3): 18-29.
17. Ponsam J, Godwin, Srinivasan R. A survey on MANET security challenges, attacks and its countermeasures. *International Journal of Emerging Trends & Technology in Computer Science* (IJETTCS) 2014; 3(1).
18. Hu YC, Perrig A. Asurvey of secure wireless ad hoc routing. *IEEE Security & Privacy* 2004; 2(3): 28-39.
19. Nguyen, Lan H, Nguyen UT. A study of different types of attacks on multicast in mobile ad hoc networks. *Ad Hoc Networks* 2008; 6(1): 32-46.
20. Wu, Bing, Chen J et al. A survey of attacks and countermeasures in mobile ad hoc networks. *Wireless network security* 2007: 103-135.
21. Bala, Kanchan. A Survey of Black Hole Detection Policies in Mobile Ad Hoc Networks. *International Journal of Future Generation Communication and Networking* 2016; 9(12): 295-304.
22. Prave en KS, Gururaj HL, Ramesh B. Comparative Analysis of Black Hole Attack in adhoc Network Using AODV and OLSR Protocols. *Procedia Computer Science* 2016; 85: 325.
23. Khanna, Nitin. Avoidance and Mitigation of All Packet Drop Attacks in manetsusing Enhanced AODV with Cryptography. *International Journal of Computer Network and Information Security* (IJCNIS) 2016: 8(4): 37.
24. Shahabi, Sina, Ghazvini M et al. A modified algorithm to improve security and performance of AODV protocol against black hole attack. *Wireless Networks* 2016; 22(5): 1505-1511.
25. Ghugar, Umashankar, Pradhan J et al. A Novel Intrusion Detection System for Detecting Black Hole Attacks in Wireless Sensor Network using AODV Protocol. *IJCSN-International Journal of Computer Science and Network* 2016; 5(4).
26. Mjahidi, Mohamedi M. A Survey on Security Solutions of AODV Routing Protocol against blackhole Attack in MANET.*International Journal of Computer Applications* 2015; 113(15).
27. Kumar, Sushil, Rana DS et al. Analysis and Implementation of AODV Routing Protocol against Black Hole Attack in MANET. *International Journal of Computer Applications* 2015; 124(1).
28. Kumar, Vimal, Kumar R. An Adaptive Approach for Detection of Blackhole Attack in Mobile Ad hoc Network. *Procedia Computer Science* 2015; 48: 472-479.
29. Jayachandra SH. Analysis of Black Hole Attack in Ad Hoc Network Using AODV and AOMDV Protocols. Emerging Research in Computing, Information, Communication and Applications. *Springer India*, 2016; 99-108.
30. Alem, Fantahun Y, Xuan ZC. Preventing black hole attack in mobile ad-hoc networks using Anomaly Detection." Future Computer and Communication (ICFCC), 2010 2nd *International Conference* IEEE 2010; 3.
31. Patel, Ankit D, Chawda K. Dual security against grayhole attack in manets. Intelligent computing, communication and devices. *Springer India* 2015; 33-37.
32. Chhabra, Meghna, Gupta BB. An efficient scheme to prevent ddos flooding attacks in mobile ad-hoc network (MANET). *Research Journal of Applied Sciences, Engineering and Technology* 2014; 7(10): 2033-2039.
33. Chhabra, Meghna, Gupta B et al. A novel solution to handle DDOS attack in MANET. *Journal of Information Security* 2013; 4(3): 165.
34. Gupta, Anurag. Improved AODV Performance in DOS and Black Hole Attack Environment. Computational Intelligence in Data Mining. Springer India, 2015; 2:

541-549.
35. Patel, Bipin N, Patel TS. A Survey on Detecting Wormhole Attack in Manet. *Journal of Engineering Research and Applications* 2014; 4(3): 653-656.
36. Shastri, Ashka, Joshi J. A Wormhole Attack in Mobile Ad-hoc Network: Detection and Prevention. Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies. ACM, 2016.
37. Sharma, Dhruvi, Kumar V et al. Prevention of Wormhole Attack Using Identity Based Signature Scheme in MANET. *Computational Intelligence in Data Mining*, *Springer India,* 2016; 2: 475-485.
38. Shastri, Ashka, Joshi J. A Wormhole Attack in Mobile Ad-hoc Network: Detection and Prevention. Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies. ACM, 2016.
39. Kar, Sumit, Sethi S et al. Security challenges in cognitive radio network and defending against Byzantine attack: a survey. *International Journal of Communication Networks and Distributed Systems* 2016; 17(2): 120-146.
40. Agrawal, Neha, Joshi KK et al. Performance Evaluation of Byzantine Rushing Attack in ADHOC Network. *International Journal of Computer Applications* 2015; 123(6).
41. Patel, Kumar NJ, Tripathi K. Trust Value based Algorithm to Identify and Defense Gray-Hole and Black-Hole attack present in MANET using Clustering Method 2018.
42. Tseng, Hsun F, Chiang HP et al. Black Hole along with Other Attacks in manets: A Survey. *Journal of Information Processing Systems* 2018; 14(1).
43. Nayak, Divyashree, Kiran YC. Malicious Node Detection by Identification of Gray and Black Hole Attacks using Control Packets in manets. *Imperial Journal of Interdisciplinary Research* 2017; 3(7).
44. Yadav, Sakshi. Securing AODV routing protocol against black hole attack in MANET using outlier detection scheme. *Electrical, Computer and Electronics* (UPCON), 2017 4th IEEE Uttar Pradesh Section International Conference on. IEEE, 2017.
45. Khan, Mahmood S, Nilavalan R et al. A Novel Approach for Reliable Route Discovery in Mobile Ad-Hoc Network. *Wireless Personal Communications* 2015; 83(2): 1519-1529.
46. Gupta, Brij, Agrawal DP et al. Handbook of research on modern cryptographic solutions for computer and cyber security. IGI Global, 2016.
47. Yadav, Anita, Singh YN et al. Improving routing performance in AODV with link prediction in mobile Adhoc Networks. *Wireless Personal Communications* 2015; 83(1): 603-618.
48. Mathew, Melvin, Let GS et al. Modified AODV routing protocol for multi-hop cognitive radio ad hoc networks. Artificial Intelligence and Evolutionary Algorithms in Engineering Systems. Springer India, 2015. 89-97.
49. Rathee, Geetanjali, Saini H. Secure Modified Ad Hoc On-Demand Distance Vector (MAODV) Routing Protocol. *International Journal of Mobile Computing and Multimedia Communications* (IJMCMC) 2017; 8(1): 1-18.
50. Yang, Hua, Liu Z. A Genetic-Algorithm-Based Optimized AODV Routing Protocol. *International Conference on Geo-Informatics in Resource Management and Sustainable Ecosystems.* Springer, Singapore, 2016.
51. Karthikeyan B, Ganesh SH, Kanimozhi N. Security Improved Ad-Hoc on Demand Distance Vector Routing Protocol (sim AODV). *International Journal on Information Sciences and Computing* 2016; 10(2).
52. Kaur, Pawanjeet, Singh M. Comparision Between Aodv And Modified Aodv In Manet. *Global Journal of Computers & Technology* 2016; 5(1): 239-240.
53. Yang, Licai, Liu H. A Data Transmitting Scheme Based on Improved AODV and RSU- Assisted Forwarding for Large-Scale VANET. Wireless Personal Communications 2016; 91(3): 1489-1505.
54. Choudhury, Roy D, Ragha L et al. Implementing and improving the performance of AODV by receive reply method and securing it from Black hole attack. *Procedia Computer Science* 2015; 45: 564-570.
55. Cho, Jin-Hee, Swami A et al. A survey on trust management for mobile ad hoc networks. *IEEE Communications Surveys & Tutorials* 2011; 13(4): 562-583.
56. Vijayan R, Jeyanthi N. A survey of trust management in mobile ad hoc networks. *International Journal of Applied Engineering Research* 2016; 11(4): 2833-2838.
57. Govindan, Kannan, Mohapatra P. Trust computations and trust dynamics in mobile adhoc networks: A survey. *IEEE Communications Surveys & Tutorials* 2012; 14(2): 279-298.
58. Yan, Zheng, Zhang P et al. A survey on trust management for Internet of Things. *Journal of network and computer applications* 2014; 42: 120-134.
59. Subramaniam, Sridhar, Ramachandran B. Energy-and Trust-Based AODV for Quality- of-Service Affirmation in manets." Artificial Intelligence and Evolutionary Algorithms in Engineering Systems. Springer India, 2015; 601-607.
60. Babu, Kennedy N. Establishing Security in Manets Using Friend-Based Ad Hoc Routing Algorithms. *Journal of Computer Science Engineering and Software Testing* 2018; 4(1).
61. Janani VS, Manikandan MSK. Efficient trust management with Bayesian-Evidence theorem to

secure public key infrastructure-based mobile ad hoc networks. *EURASIP Journal on Wireless Communications and Networking* 2018; 1: 25.

62. Ahmed, Adnan, Bakar KA. Muhammad Ibrahim Channa, Khalid Haseeb, and Abdul Waheed Khan. A survey on trust based detection and isolation of malicious nodes in ad-hoc and sensor networks. *Frontiers of Computer Science* 2015; 9(2): 280-296.
63. Cho, Jin-Hee, Swami A et al. A survey on trust management for mobile ad hoc networks. *IEEE Communications Surveys & Tutorials* 2011; 13(4): 562-583.
64. Pirzada AA, Mcdonald C. Trust Establishment In Pure Ad-hoc Networks. *Wireless Personal Communications, Springer* 2006; 139-163.
65. Fall K, Varadhan K. The ns manual. Notes and documentation on the software NS2-simulator, 2002." URL: www. Isi. Edu/nsnam/ns.
66. Ghosh T, Pissinou N, Makki K. Collaborative Trust-based Secure Routing Against Colluding Malicious Nodes in Multi-hop Ad Hoc Networks. in Proc. 29th Annual IEEE International Conference on Local Computer Networks, pp. 224-231, 2004.
67. Ghosh T, Pissinou N, Makki K. Towards Designing a Trusted Routing Solution in Mobile Ad Hoc Networks. Mobile Networks and Applications, *Springer Science,* 2005; 10: 985-995.
68. Pirzada AA, Datta A, Mcdonald C. Trust-based routing for ad-hoc wireless networks. *IEEE* 2004; 326-30.
69. X Li, Lyu MR, Liu J. A Trust Model Based Routing Protocol for Secure Ad Hoc Networks. in Proc. Aerospace Conference, *IEEE* 2004; 2: 1286-1295.
70. Eissa, Tameem, Razak SA et al. Trust-based routing mechanism in MANET: Design and implementation. *Mobile Networks and Applications* 2013; 18; 5: 666-677.