ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, Issue 3, March 2013

Investigation on Performance of Trust Based Model and Trust Evaluation of Reactive Routing Protocols in MANET

Dharam Vir, Dr. S.K.Agarwal, Dr.S.A.Imam

***Abstract*— In this paper we investigate and implementing trust based route selection in mobile wireless ad hoc networks. A system that stores and updates trust values for nodes encountered in mobile ad hoc networks. Since a route consists of many nodes that are grouped, different strategies for evaluation of routes based of the nodes trust values have been designed and implemented. We apply trust based route selection to the DSR, AODV and DYMO Protocols, in order to secure the protocol and improve route selection, which can increase throughput in situations where malicious nodes are present in the network. To evaluate the performance impacts of applying trust based route selection in sending, receiving and forwarding of packets. The performance is calculated in terms of metrics like throughput, packet delivery ratio and average jitter. The evaluation of trusted AODV, DSR and DYMO with implemented trust has been done with the help of QualNet 5.0 simulator**

***Index Terms*; Ad hoc Network, AODV, DSR, DYMO, Trust, route, protocol, QualNet 5.0**

I. INTRODUCTION

There are two primary motivations associated with trust management in MANETs. At first, *trust evaluation* helps distinguish between good and malicious entities. Creating trust history, one entity can remember others' behaviours. This memory provides a method for good entities to avoid working with 'ex-convict' or suspect ones. Secondly, *trust management* offers a prediction of one's future behaviour and improves network performance. The results of evaluation can be directly applied to an incentive for good or honest behaviours while a penalty for selfish or malicious behaviours in the network. The feedback reminds network participants to act more responsibly. These motivations have interested researchers from the areas of information security and computer network in trust management of MANETs [1] [9].

An ad hoc network is a collection of wireless mobile nodes that dynamically functions as a network without the use of any existing infrastructure and centralized administration. Nodes

move around which can cause links to be broken and established. Due to the relatively short transmission range of wireless devices, nodes in the network collaborate to route data to destinations that might be out of the sender's transmission range. An ad hoc network is illustrated in Figure 1. As illustrated all nodes are not in direct connection with each other but can use other nodes as relays in order to transmit to a destination. The figure also illustrates another important property of the shown ad hoc network, the inaccessibility to servers or centralized administration [2].

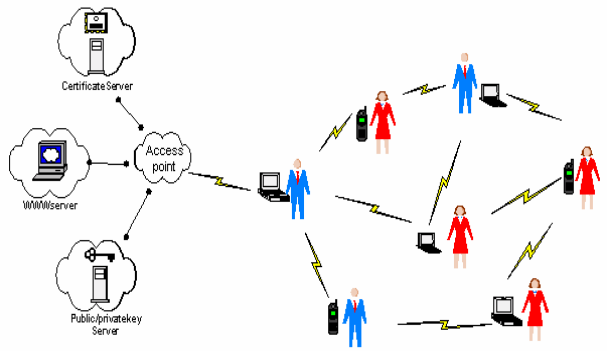

Figure 1: Mobile wireless ad hoc network

Ad hoc networks are often proposed for search and rescue mission and military operations where existing infrastructure have been damaged and is inoperative. In such situations the nodes are related by outside factors such as organizational hierarchies. Another type of ad hoc networks, often referred to, as collaborative networks are networks where agents with no common relations join together to achieve their own personal goal of sending packets to a destination. The structure of collaborative ad hoc networks is untraditional, since nobody can claim ownership and control of the network and thereby attend to administration of the network and require payment for its use. The structure of the ad hoc network gives rise to security issues of different severity, since malicious nodes can seek to exploit the openness of the network.

In this paper we investigate several existing security solutions for ad hoc networks and propose a trust based route selection solution. The solution addresses the problem that occurs when malicious nodes starts to drop packets they were supposed to forward. Most common protocols for mobile

Manuscript received March 05, 2013.
***Dharam Vir**, Department of Electronics Engg., YMCA University of Science & Technology, Faridabad, India.*
Mobile No: 09999067810
***S.K.Agarwal**, Department of Electronics Engg., YMCA University of Science & Technology, Faridabad, India.*
Mobile No: 09953393520
***S.A.Imam**, Department of Electronics & Comm. Engg., Jamia Millia Islamia, New Delhi, India.*
Mobile No: 09818732747

wireless networks build on the assumptions that nodes in the network are willing to participate to the networks existence by forwarding packets for other nodes [6].

In general most mobile devices operate on battery power, which means that each transmission has a cost in terms of power consumption. This results in a conflict, since nodes have to perform the task of forwarding data, from which they achieve no benefits and as a result consume their own battery power. There is little reason to assume that some nodes will not try to achieve the benefits of participating in the network and avoid the disadvantages it involves. This could mean that some nodes refuse to forward packets as supposed and thereby decrease the efficiency of the network. Because of the nature of the ad hoc network it is difficult to identify nodes that express such malicious behavior, because the node originating the transmission might be out of range to detect the malicious act.

• By allowing an unknown node to forward data, nodes perform a trust-based decision. Trust is a well-known sociological concept that humans on a daily basis base decision on [9].

• By incorporating trust in ad hoc routing protocols and thereby mimicking human behavior, it is expected that the establishment and evolution of trust can be used to detect nodes that betrays the trust placed in them [9].

• By detection of untrustworthy nodes can be used to apply trust based route selection strategies to ad hoc routing protocols and thereby increase the effectiveness of the network [10].

We design and implement a system that can be used for trust based routing. The system must make it possible for nodes to store and updates crisp values that represent their trust in other nodes. These values should be adjusted based on the experiences the nodes have. When a route is selected is must be selected by an evolution of the nodes on the routes values. It is the aim that such a system can be applied to the DSR protocol to achieve route selection strategies that can avoid nodes with low values [10].

The rest of the paper as follows Section II describes Ad hoc routing protocol and analysis of protocols. Section III describes implementation of trust evolution function. Section IV simulation based design scenarios and implementation in QualNet of all above protocols. Section V presented results, conclude and feature work in section VI.

II. AD HOC ROUTING PROTOCOLS

There are several different principles that can be applied when constructing routing protocols for ad hoc networks.

Proactive: Protocols can be proactive (also called table driven) which means that nodes periodically registers changes in the topology and updates routing information. The routes are stored and maintained in routing tables. Proactive protocols have the advantage that there is little latency since routes are already available, but the disadvantage that they require nodes to periodically update routing tables. In a highly dynamic network this increases routing related traffic.

Reactive: The opposite approach is the reactive (also called on-demand) protocols. Routes are first discovered on demand, when data needs to be transmitted to a node where no route has yet been discovered. The major advantage of on demand routing is that it saves bandwidth because it limits the routing overhead. The disadvantage is the latency at the beginning of transmission to nodes when no route, have yet been discovered.

Hybrid: Hybrid Routing Protocols combines the merits of proactive and reactive routing protocols by overcoming their demerits. Proactive routing uses excess bandwidth to maintain routing information, while reactive routing involves long route request delays. Reactive routing also inefficiently floods the entire network for route determination [3] [4] [8].

A. Dynamic Source Route (DSR) Protocol:

The protocol is specifically designed for use in multi-hop wireless ad hoc networks. The protocol does not require any existing network infrastructure or administration and is completely self-organizing and self- configuring. The protocol basically consists of the two mechanisms: Route Discovery and Route Maintenance, where the Route Discovery mechanism handles establishment of routes and the Route Maintenance mechanism keeps route information updated [3].

Assumptions of Dynamic Source Route Protocol: Some assumptions concerning the behavior of the nodes that participate in the ad hoc network are made. The most important assumptions are the following [3]:

- All nodes that participate in the network are willing to participate fully in the protocol of the network.
- The diameter of the network are often small, e.g. in the interval of nodes.
- Nodes can detect and discard corrupted packages.
- The speed at which nodes move is moderate with respect to packet transmission latency.
- Each node can be identified by a unique id by which it is recognized in the network.

Mode of operation: DSR operate on demand, which means that no data, such as route advertisement messages, is send periodically and therefore routing traffic caused by DSR can scale down and overhead packages can be avoided [3].

DSR is a source routing protocol, which means the entire route is known before a packet transmission is begun. DSR stores discovered routes in a Route Cache [8].

Table 1: Fields of the ROUTE REQUEST message are used to indicate fields used for the more advanced features of DSR.

Fields	Explanation
Initiator ID	The address of the initiator.
Target ID	The address of the target.
Unique Request ID	A unique ID that can identify the message.
Address List	A list of all addresses of intermediate nodes that the message passes before its destination. This is empty when the message is first send.
Hop Count Limit	The hop count limit can be used to count limit the number of nodes that the message is allowed to pass.
Network Interface List	If nodes have several network interfaces this information can be stored in this

Acknowledgment	There is an option of setting a bit so that the receiver returns an acknowledgement when a packet is received.

The two mechanisms: Route Discovery and Route Maintenance are described below.

a) Route Discovery:

When a node source sends a packet to the destination, it first searches its Route Cache for a suitable route to destination. If no route from source to destination exists in source's route cache, source initiates Route Discovery and sends out a ROUTE REQUEST message to find a route. The sending node is referred to as the initiator and the destination node as the target. The fields of the ROUTE REQUEST message are explained in Table 1.

The initiator initializes the Address List to an empty list and set the Initiator ID, the Target Id and the Unique Request Id in the ROUTE REQUEST message and then broadcasts the message. This causes the packet to be received by nodes within the wireless transmission range. The initiator keeps a copy of the packet in a buffer, referred to as the send buffer. It time stamps the message so it can be examined later to determine if it should be send again. If no route is discovered within a specified time frame, the packet is dropped from the send buffer. Packets are also dropped from the send buffer if the buffer overruns [3].

When a node receives a ROUTE REQUEST message it examines the Target ID to determine if it is the target of the message. If the node is not the target it searches its own route cache for a route to the target. If a route is found it is returned. If not, the nodes own id is appended to the Address List and the ROUTE REQUEST is broadcasted. If a node subsequently receives two ROUTE REQUESTs with the same Request id, it is possible to specify that only the first should be handled and the subsequent discarded.

If the node is the target it returns a ROUTE REPLY message to the initiator. This ROUTE REPLY message includes the accumulated route from the ROUTE REQUEST message. The target searches its own Route Cache for a route to the initiator. The reason that the target node doesn't just reverse the found route and use it is that that would require bi-directional links. If a route is not found in the targets Route Cache, it performs a route discovery of its own and sends out a ROUTE REQUEST where it piggybacks the ROUTE REPLY for the initiator [3] [11].

Acknowledgment can be performed either by using mechanisms in the underlying protocol such as link-level acknowledgment or passive acknowledgment. If none of these mechanisms are available, the transmitting node can set a bit in the packets header to request a specific DSR acknowledgment. If a node transmits a packet and does not receive an acknowledgment it tries to retransmit a fixed number of times. If no acknowledgement is received after the retransmissions, it returns a ROUTE ERROR message to the initiator of the packet. In this message the link that was broken is included. The initiator removes the route from its Route Cache and tries to transmit using another route from its Route Cache. If no route is available in the Route Cache a ROUTE REQUEST is transmitted in order to establish a new route.

B. Ad-Hoc On Demand Distance Vector (AODV) Protocol:

The AODV protocol was presented in 1997 and is designed by Charlie E. Perkins and Elizabeth Royer, who also designed the DSDV protocol. The protocol is a hybrid of the DSR protocol and the DSDV protocol. It uses a route discovery process much similar to the one used by DSR and makes use of hop-by-hop routing like DSDV. The primary objectives for the AODV algorithm are:

- To broadcast discovery packets only when necessary.
- To distinguish local connectivity management (neighbour nodes) from changes in the entire topology.
- To try to forward information concerning changes in local connectivity to neighbour nodes who are likely to need it.

As mentioned the route discovery process is much similar to the one used by the DSR protocol. AODV differs from DSR in the way that nodes do not store the entire route to a destination [5].

C. DYNAMIC MANET ON-DEMAND (DYMO) Protocol:

The Dynamic MANET On-demand (DYMO is a reactive, multihop, unicast routing protocol. The DYMO is a memory concerned routing protocol and stores minimal routing information and so the Control Packets is generated when a node receives the data packet and it doesn't have any valid route information. The basic operations of DYMO are:

a) Route Discovery:

The source router generates Route Request (RREQ) messages and floods them for destination routers for whom it doesn't have route information. Intermediate nodes store a route to the originating router by adding it into its routing table during this dissemination process. The target node after receiving the RREQ responds by sending Route Reply (RREP) message. RREP is sent by unicast technique towards the source. An intermediate node that receives the RREP creates a route to the target and so finally it reaches to originator. Then routes have been established between source and destination in both directions [7] [6].

b) Route Maintenance:

Route maintenance consists of two operations. It avoids expiring good routes and so it updates reverse route lifetime on data reception and forward route lifetime on data transmission. The DYMO nodes monitors link over which traffic is flowing in order to cope up with dynamic network topology. A Route Error (RERR) message is generated when a node receives a data packet for the destination for which route is not known or the route is broken. The DYMO routing protocol is designed for memory constrained devices in mobile ad hoc networks (MANETs) as it quickly determines route information dynamically [7].

III. Implementing Trust Evolution Function

To protect against different types of attack a different number and type of trust metrics is employed. However, the implementation of any trust model comes at the cost of [11]:

Power consumption: for processing of information and execution of more complex routing protocols, as well as for transmission of the reputation information, power consumption is trustable [11].

Bandwidth consumption: for the exchange of trust protocol messages such as status request and status responses are depending on the trust model type, it can also introduce latency in the message travel to the base station [9].

A. Parameters of performance evaluation for trust model:

Packet Loss: The packet loss indicates the total number of data packets lost legitimately or through malicious action without any notification. It is a metric typically used to evaluate the performance of sensor networks where the link quality, available transmission power and mobility may reason a packet to fail traveling to its destination [10].

Packets Forwarded: It represents the number of data packets that were successfully forwarded by the intermediary nodes. In combination with the number of lost packets, it can express the loss ratio (Packet loss divided by the number total number of packets transmitted).

Overhead: This is the ratio between the total numbers of control packets generated for the trust information exchange to the total number of data packets received.

Energy consumption: Since the implementation of a trust management system for avoid security attacks leads to power consumption, this is an important metric and can also be considered a constraint for the design of a trust model.

Average Latency: It gives the mean time in seconds taken by the data packets to reach their respective destinations. This metric quantifies the additional time needed for executing a more complex algorithm to take any routing decision in the case of proactive trust models [10].

Probability of Detection: It is the ratio between the numbers of nodes whose behavior (malicious or benevolent) is identified correctly to the actual number of such nodes present in the network.

Scalability: As emerging WSNs and consequently VSN consist of high volumes of devices, the capability of the routing protocol to scale well with the network dimensions is of prime importance for the wide applicability and acceptance of the protocol.

B. Trust based routing:

The main scheme behind trust based routing is to store information about the trust that one node has in other encountered nodes. These trust values are adjusted based on the nodes experiences, such as packet drops or acknowledgements receipts [12].

C. Different categories of trust:

Trust is subjective and depends on both agent and situation/action, which makes it difficult to specify general rules. The trust constructs relates to each other as antecedents and consequents, and facilitates scientific measurements and predictions. The trust constructs are:

General trust: This represents the trust of one agent node in another agent node.

System Trust: This means the extent to which one believes that proper impersonal structures are in place to enable one to anticipate a successful future endeavor.

Dispositional Trust: This is the extent to which one consistently trusts in a wide variety of situations and in different persons.

Belief Formation Process: which is the process where experience and information is used to create new trusting beliefs [12].

Situational trust: which is the trust that one agent node has in another agent node in a given situation.

Importance and utility: This expresses the utility an agent node, gains from a situation.

Trust Evolution: ES × N → T

Identify sixteen possible properties, such as *minimal* and *maximal initial trust*, of trust evolution functions. An interesting property is the *degree of memory based on window N* that expresses the number of experiences back in time that should be used in the calculation. This property is interesting since its value can lead to quite different results. Figure 1 illustrates a small example [13]:

Trust evolution function	ES	$T_{N=8}$	$T_{N=4}$
$T = \frac{1}{N} \blacktriangleleft^{N} ES$	[-1, -1, -1, -1, 1, 1, 1, 1]	0	-1

Figure 2: Using the degree of memory based on window n for trust evolution functions.

As the example illustrates quite different result is achieved by using a window size of 8 instead of a window size of 4.

Trust Update Function:

The trust update functions differ from the trust evolution function since it uses the current experience and the last calculated value of the trust to calculate the new trust value. The trust update function is defined as:

Trust Update: E × T → T

A trust update function uses a prior determined value of trust and a new experience to calculate a new value for trust [13].

D. Analysis of AODV, DSR and DYMO:

This section presents an analysis of the different events that can take place during communication within the DSR protocol, the possible outcome and possible reactions to the outcome. The relevant events can be divided into the following three categories:

- **Sending of packets –** the case where a node is the source of the packet.
- **Receiving of packets –** the case where the node is the final destination of the packet.
- **Forwarding of packets –** the case where a node is a hop on the route to the final destination.

IV. Simulation Analysis

A. Simulation Environment setup and Metrics:

The network simulator used for trust evolution is QualNet

5.0 and the simulation parameters are as shown in Table.1. It consists of total number of nodes as 50, the Terrain area chosen is 1500 m *1500 m, the Constant Bit Rate of packet size is 512, the Simulation time chosen over here is 30 seconds, and the mobility is Random way point, most. It shows the trust value performance of various protocols such as AODV, DSR and DYMO with respect to physical layer model to define the performance effectiveness of routing protocols. We applying trust based route selection in sending of packets, receiving of packets and forwarding of packets to the different scenarios with varying CBR traffic load [14].

Table; 1 Simulation setup parameter for QualNet

Parameters	Value
Simulator	QALNET 5.0
Protocols	AODV, DSR,DYMO
Number of Nodes	50
Simulation Time	30s
Simulation Area	1500 X 1500
Mobility Model	RWP
Energy Model	Mica-Motes
Traffic Type	Constant-Bit Rate
Node Placement Model	Random
Battery Model	Linear Model
Antenna Model	Omni direction
Available bandwidth	1 Mb/s
Radio Range	250 m

B. Snapshot for running scenario

CBR is chosen over TCP because the protocol is much simpler which makes the results easier to analyze. Furthermore, it seems to be best practice to use CBR for ad hoc simulations. The traffic scenarios are also generated randomly, but similar to the movement scenarios they are deterministic once created. The traffic scenarios specify which nodes should start transmitting to some destination at a specific time. Since the objective of the simulations is to compare the standards of AODV, DSR and DYMO with trust based route selection, using number of scenario is considered satisfying result, as long as one protocol does not gain advantages over the other from the scenario.

C. Metrics Evaluation:

There are several different metrics that can be applied to measure protocols performance against. Studies of performance evaluations of protocols for mobile ad hoc networks indicate that the following metrics is usually used;

Throughput: This is the ratio between the number of packets send by the application layer and the number of packets received at the application layer. The throughput is used to compare the standard DSR, AODV and DYMO equipped with different trust based routing strategies, because it is a very common metric and because it expresses how well the protocol is at delivering packets for an overlying (application) layer, which in the end, is the primary task of the protocol.

Path optimality: which is the difference between the number of hops the packet took and the length of the shortest path. Using path optimality in the common way is not considered relevant because trust based routing is based on the avoidance of malicious nodes, which is expected to lead to the use of longer routes.

Routing overhead: this expresses the total number of routing packets that are sending.

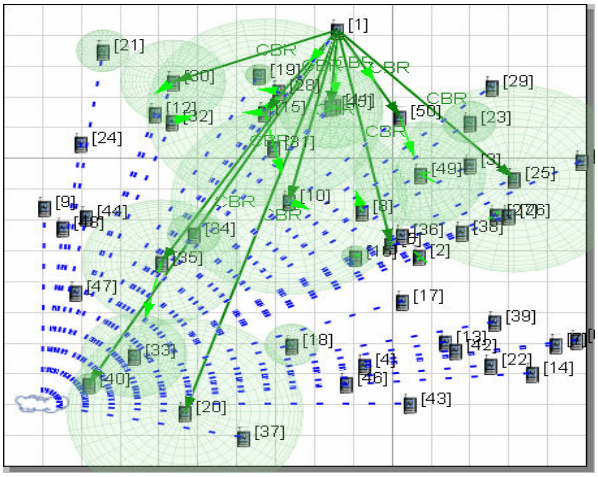

Figure 3. Snapshot of simulation scenario representing path optimality and route request mechanism of 50 nodes for DSR routing protocol.

V. RESULTS

Comparison performance analysis of trust based AODV, DSR and DYMO protocols.

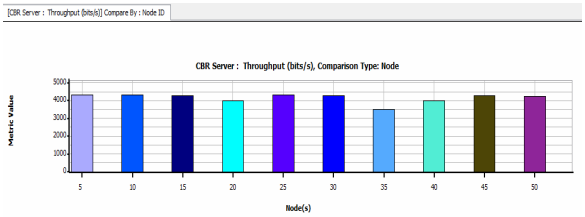

Figure 4. Snapshot of outcome of simulation scenario of throughput of 50 nodes for DSR routing protocol.

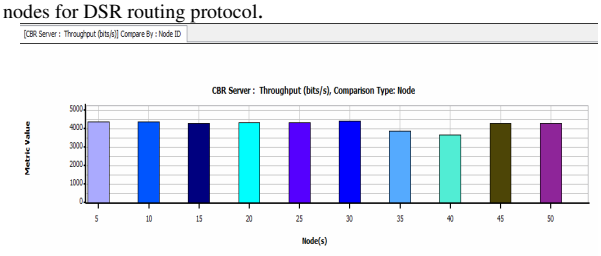

Figure 5. Snapshot outcome of simulation scenario of throughput of 50 nodes for AODV routing protocol.

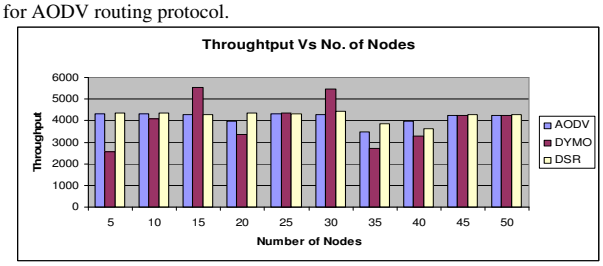

Figure 6. Comparison of Trust based throughput of 50 nodes for AODV, DSR and DYMO routing protocol.

The comparison will be evaluated along three axes: the cross layer routing, the virtualization and the trust aspects, but priority will be given to the trust model validation. In this

case AODV highest trusted routing protocol followed by DSR than DYMO.

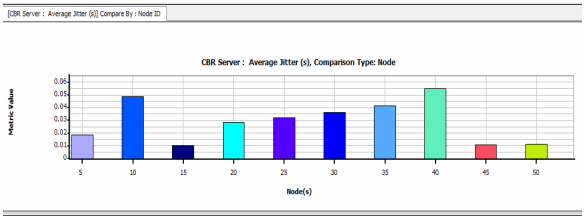

Figure 7. Snapshot of outcome of simulation scenario of average jitter of 50 nodes for DSR routing protocol.

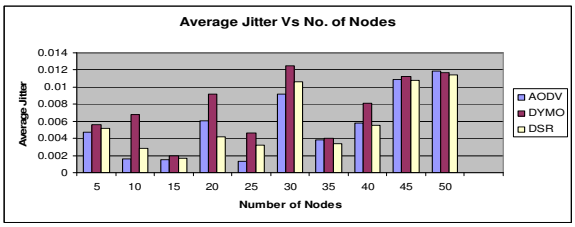

Figure 8. Comparison of Trust based average jitter of 50 nodes for AODV, DSR and DYMO routing protocol.

The comparison in Trust based average jitter AODV is able to achieve a remarkable improvement in the average jitter and prevent most malicious attacks.

VI. Conclusion and Future Work

The results show that DSR and AODV deliver over 65% of the packet regardless of the mobility rate of nodes used for the simulations. The abilities of DSR and AODV to deliver packets depend on the movement patterns of nodes in the network; the more rapidly the nodes move the more packets be dropped. In this paper we have described a simple trust model based on packet forwarding ratio to evaluate trust based neighbours' behaviours . Combined with the model, a novel multipath reactive routing protocol (AODV, DSR and DYMO) is projected to discover trust worthy forward paths and alleviate the attacks of malicious nodes. In these protocols, a source can find multiple trusted paths to a destination in a single route discovery round. New route discovery is needed only when all paths break or fail to meet the trust requirement. These protocols provide a flexible and feasible approach to choose a shortest path in all trusted paths to meet the dependable or trust requirements of data packets. Multiple paths can also be used to balance load by forwarding data packets on multiple paths at same time.

Performance comparison of AODV, DSR and DYMO routing protocols shows that AODV is able to achieve a remarkable improvement in the throughput; average jitter and PDR prevent most malicious attacks. For future work, we plan to extend our trust model to other MANET routing protocols like LAR, ZRP and OLSR. We will also conduct a comprehensive performance evaluation to compare AODV with other trust-based routing protocols.

REFERENCES

[1] P. Papadimitrates and Z.J. Hass, secure Routing for mobile Ad Hoc Networks in proceeding of *SCS Communication Networks and Distributed system modeling and simulation Conference (CNDS)*, San Antonio, TX, Jan. 2002.

[2] H. Karl, A. Willig, "Protocols and Architectures for Wireless and Sensor Networks", *Wiley*, 2005

[3] D. Johnson and D. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks", *Mobile Computing*, T. Imielinski and H. Korth, Ed., pp. 153-81. Kluwer, 1996.

[4] Belding-Royer,E.M. and C.K. Toh, , "A review of current routing protocols for ad-hoc mobile wireless networks", *IEEE Personal Communication magazine* pp:46-55,1999.

[5] C. Perkins, E. B. Royer, and S. Das, "Ad hoc On Demand Distance Vector Routing Protocol", *IETF Experimental RFC*, July 2003.

[6] Marga Nacher et.al., "Multipath Extensions to the DYMO routing protocol", In Proceedings of the 9th International Conference on *Mobile and Wireless Communications Networks*, Cork, Ireland, September 19-21, *IEEE*, 2007.

[7] Chakeres, I. and C. Perkins, "Dynamic MANET On demand (DYMO) Routing", *draft ietf manet* dymo 21.

[8] M.Lakshmi and P.E.Sankaranarayanan, "Performance Analysis of Three Routing Protocols in Wireless Mobile Ad hoc Networks", *Information Technology Journal*, 5(1), pp.114-120, 2006.

[9] Idris M. Atakli , Hongbing Hu, Yu Chen, Wei Shinn Ku , Zhou Su, "Malicious node detection in wireless sensor networks using weighted trust evaluation" *Spring simulation multi conference*, Ottawa, Canada, 2008.

[10] Hongbing Hu and Yu Chen, Wei Shinn Ku, Zhou Su, Chung Han J. Chen "Weighted trust evaluation based malicious node detection for wireless sensor networks", *Int. J. Information and Computer Security*, Vol. 3, No. 2, 2009, pp.132 - 149.

[11] K. Kar, M. Kodialam, T. Lakshman, L. Tassiulas, "Routing for network capacity maximization in energy constrained ad hoc networks", *Proc. INFOCOM'03, IEEE*, 2003.

[12] S. Venkatasubramanian, A cross layer based multipath routing protocol to improve QoS in Mobile Ad hoc Networks, *Int. Journal on Network Security*, Vol.1, No. 1, Jan,. 2010, pp.42 - 48.

[13] Ferdous, R., Muthukkumarasamy, V., Sattar, A.: Trust Management Scheme for Mobile Ad-Hoc Networks. In: *IEEE 10th International Conference on Computer and Information Technology* (CIT), 2010.

[14] "Qualnet 5.0 user's Guide", [online] Available : http://www.scalablenetworks.com/

Author' Profile

Dharam Vir (dvstanwar@gmail.com) received the M.Tech Degree form MDU Rothak (Haryana) and B.E Degree in Electronics and Communication Engg. From Jamia Millia Islamia, Central University, New Delhi 2004, 2008 respectively. He started his carrier as R&D Engineer in the field of computer networks engineer, since 1992, now he is the part of YMCA University of Science & Technology as Head of Section (Electronics & Inst. Control) in the Department of Electronics Engineering. He has more than 15 publications in journals and conf. of repute. He is pursuing his PhD in the field of Mobile Ad hoc Networks. Presently he is working in the field performance improvement in MANET routing (Power aware routing protocol). His current interest in power control in wireless network system, wireless communication, computer networks

Dr. S.K. Agarwal (sa_3264@yahoo.co.in) received the M.Tech Degree from Delhi Technical University .New Delhi and PhD degree in Electronics Engg from Jamia Millia Islamia Central University. New Delhi in 1998 and 2008, respectively, Since 1990. He has been part of YMCA University of Science & Technology Faridabad (Haryana), where he is Dean & Chairman in Department of Electronics and Communication Engineering. He has more than 30 publication in journals and conf. of repute. His current research interests are in the field of Control System ,electronics and biosensors, Analog Electronics, wireless communication and digital circuits.

Dr. Syed A Imam (imam_jmi@yahoo.co.in) received the B.E Engg degree (Electrical Engg) from Jamia Millia Islamia, M. Tech (Instrumentation & Control System) from AMU, Aligarh and PhD degree in Electronics & Comm. Engg from Jamia Millia Islamia (a Central University), New Delhi, in 1990, 1998, and 2008, respectively. Since 1990, he has been part of Jamia Millia Islamia University, where he is Assistant Professor in the Department of Electronics and Communication Engineering. He has more than 80 publications in journals and national/international conferences of repute. His current research interests are in the field of sensing technologies, electronic and bioinstrumentation, signal processing and digital circuits.