ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 11, November 2017

Evaluation of MANET Based On QoS Parameter Using Routing Protocols with Trust Model

Manisha Yadav [1], Dr. Sujata Kulkarni [2]

P.G. Student, Department of Electronics and Telecommunication Engineering, Thakur college of Engineering and Technology, Mumbai, Maharashtra, India[1]

Associate Professor, Department of Electronics and Telecommunication Engineering, Thakur college of Engineering and Technology, Mumbai, Maharashtra, India[2]

ABSTRACT*:* MANET that is mobile ad-hoc network comprise of numerous wireless nodes without any central infrastructure. Since it is decentralized network hence nodes are self organizing and free to move to and from network Design of routing protocols in MANET is challenging because of mobility and dynamic nature of MANET **so as to seek out** efficient route with minimum overheads. Cryptographic mechanisms require Certificate Authority (CA) for authentication or a Key Distribution Center (KDC), which are difficult to deploy MANET. Routing protocol **is employed** to route information from **transmitter** to destination **however** it **doesn't** describe nature **of every** nodes **within the** network.

To overcome these issues the proposed system makes use of routing protocols with trust model. Ad-hoc on demand distance vector (AODV) routing protocol perform interactions between nodes and trust model calculates trustworthiness of each node in terms of forwarded and dropped packet. Networks with different no. nodes have been simulated using NS2. Using tracegraph2.02 software overall performance evaluation has been performed. At the end comparison of performance matrix with increasing no. of nodes has been achieved.

KEYWORDS: MANET, Routing protocols, AODV, NS2, tracegraph2.02 Average end to end delay, Throughput, PDR, Trust matrix.

I. INTRODUCTION

Wireless networking is an emerging technology that allows users to access information and services regardless of their geographic position. Further, the development of ubiquitous mobile computing devices has also raised increasing demand in sharing streaming video and audio in various applications like video conferencing, video chat, etc. along with simple file transfers [1]. In general, there are two communication approaches for wireless mobile nodes and they are:

Infrastructure-based **w**ireless mobile networks: These are based on cellular networks. They depend on a good infrastructure. Mobile devices communicate with an access point, including a base station, which in turn is attached to a fixed network infrastructure [1].

Infrastructure-less wireless mobile networks: Manet belongs to this type of network. It consists of a set of dynamic nodes that form a network. The nodes communication takes place in the network without any central infrastructure [1].

The MANET routing protocols are used to establish a communication between nodes and exchange the messages with less overhead and computational burden with the support of routing information.

In MANET the routing protocols are classified into 3 different types and they are Proactive, Reactive and Hybrid routing protocol.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 11, November 2017

In proactive routing protocol all of the nodes usually store their information within the form of tables whilst any trade inside the network topology takes place. As in changing network topology, routing tables are up to date. However in proactive routing protocol, the value associated with this is extensively more than reactive routing protocol. one primary gain of proactive routing protocol does now not cause any discovery delay when building a new route [2]. Reactive or on demand routing protocols are coming across the route while it wished that means it is based totally on demand for simplest the reactive routing protocol will find out the route. This reduces the control message overhead and the cost of elevated latency when coming across new route discovery. At some stage in message transmission it consumes low bandwidth [2].

The combination of both reactive and proactive routing protocols is known as hybrid routing protocol. Hybrid routing protocol overcomes the problem of both existing routing protocols. In that the control message overhead of proactive protocol is minimized and the latency problem associated in reactive protocol is decreased [3].

Trust management approach is one of the approved mechanisms to improve security in MANET, and which is utilized to deal with misbehaving nodes and stimulate them to cooperate. Trust is a social idea can be defined as the diploma of subjective perception about the behaviour of a selected entity. Trust in MANET is the opinion held by way of one node (known as the evaluating node) about every other node (known as the evaluated node), based totally upon the node's past behaviour and on pointers from other nodes inside the network, called recommending nodes. Current trust control frameworks for MANET can be categorized into two types. The first establishes believe relationships between nodes based totally on direct interactions only. The second type is based on direct observations of the node itself and guidelines provided by using different nodes in the network [4].

II. RELATED WORK

A. Commonly used routing protocols are as follows:

a. DSDV: Distance sequence vector DSDV, is a proactive routing protocol, every node maintains the routing table with all attainable destinations among the network and therefore the variety of needed hops to achieve the destination. The sequence variety is assigned for every destination to distinguish out stale routes and prevent routing loops [5].

b. AODV: Ad-hoc on-demand routing protocol uses destination sequence number (measure route only by the number of hops) to ensure the freshness and loop freedom of the route, to minimizes the number of broadcasts by making routes supported demand, that isn't the case for DSDV. AODV has 2 steps: Route discovery further as route maintenance mechanism [5].

c. DSR: Dynamic source routing is totally permitting the network to be self organizing and self configuring. DSR route discovery method is employed to spot path between sources to explicit destination. This method is completed by Route Request (RREQ) and Route Reply (RREP) [6].

a. ZRP: It is a type of hybrid routing protocol in which the routing is based on the technique of zones. In this technique whole network area is divided into the number of zones. ZRP is a hybrid routing protocol it used the both proactive and reactive approach for routing of packets in the network. It uses proactive routing technique for intra-zone communication and reactive routing technique for inter-zone communications [6].

B. Different trust management frameworks based on their key properties and characteristics:

a. RFSTrust: It is a trust model based on fuzzy recommendation, which is presented to quantify and evaluate the trustworthiness of nodes [7].

b. CORE: This model has a watchdog component complemented by a reputation system that distinguishes between three types of information; subjective reputation by means of observations, indirect reputation by means of positive reports by others, and functional reputation by means of task-specific behaviour [7].

c. CONFIDANT: It is a mechanism which supports cooperation in ad hoc networks by detecting and isolating malicious nodes using direct observations and recommendations [8].

d. ATMS: It provides a uniform up-to-date trust knowledge throughout the network with a minimum monitoring overhead, reducing the impact of double-face attacks. ATMS does not consider any mechanism to distinguish between correct and false recommendations [8].

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 11, November 2017

e. OTMF: It provides a uniform view on node's trustworthiness to reduce the impact of double-face attacks. An important feature of OTMF is the use of a confidence value which evaluates the quality of opinions [8].

III. METHODOLOGY

A. Routing protocol: Routing protocol routes the data from source to destination. The proposed model used AODV (Ad-hoc on demand distance vector) routing protocol. Ad-hoc on-demand routing protocol is a type of reactive routing protocol in mobile ad-hoc network. AODV routing protocol establishes a route to the destination on demand only [9]. It has two specific processes which are

a. Route Discovery
b. Route Maintenance

In AODV Hello message plays a vital role for maintaining network connectivity. Hello messages are used to identify the coverage range of nodes. The main aim of hello messages is to maintain local connectivity between the nodes. Hello messages can able to identify whether its next hop is within coverage range or not. AODV can able to perform unicast, broadcast and multicast operations. If a source node decides a path to the destination means the source node broadcast route request (RREQ) packet to the entire network. The nodes receiving these packets from reverse path and update their route table and the destination node send unicast route reply (RREP) message to the source through selected path. The nodes which are forward information are known as active route. The RREQ contains information of current sequence number, source IP address, broadcast ID, and also contains most recent sequence number of the destination that source node aware. The broadcast ID of each RREQ is incremented for every source node that initiates path discovery process.

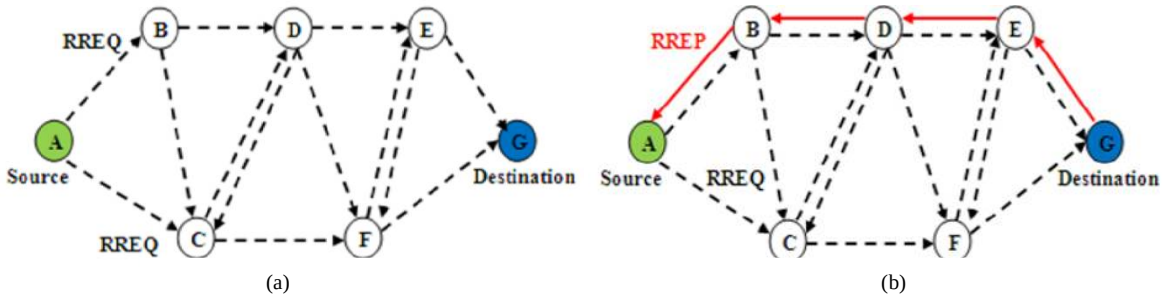


Figure 1 AODV Routing Protocol (a) AODV RREQ broadcast (b) Path discovery from source to destination

Source node receives RREP from the destination node, the node setup forward pointers to the destination node. This process is defined as path discovery in AODV. Source node starts packet transmission from source to the destination when the source node receives RREP from destination node. If the source node receives RREP later means RREP have same sequence number with smaller hop count. Then it updates its routing table and inform to the destination for getting new better route from source to destination. In AODV link between nodes are normally symmetric in nature. Link failure occurs when the route is in active and the node up steams its Route Error RERR message to the source node for finding new route. After receiving RERR message the source node decide to reinitiate route discovery. The route maintenance applied when the node moves and reinitiates its routes using our route discovery protocol to find out new freshest route from source to destination [10].

B. Trust Model

In MANETs, direct trust is obtained when two nodes have already initiated a trust relationship and they can immediately interact with each other (at least for a specific period of time, when they are within the same range, because of nodes' mobility), without requiring a third-party opinion or recommendation. The trust value is updated based on whether the previous interactions between two nodes have been successful or not. Proposed model makes use

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 11, November 2017

of use of Bayesian statistical approach for computing trust values based on the assumption that they follow a beta probability distribution.

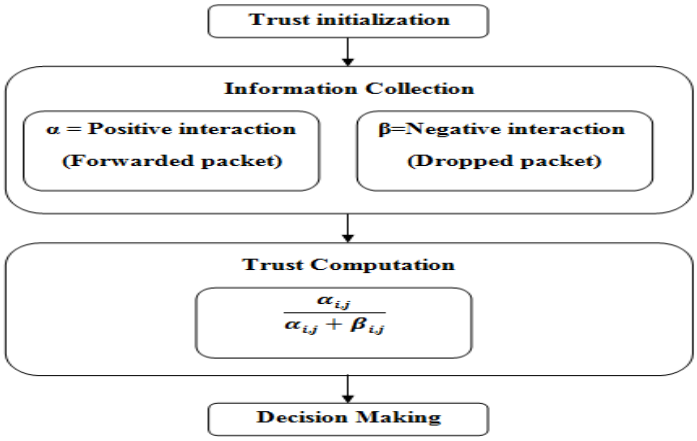


Figure 2 Trust Framework

Beta distribution is estimated by two parameter α and β where α represents accumulation of positive observations (forwarded packets) and β represents accumulation of negative observations (dropped packet) [11]. Then $\alpha_{i,j}$ represents the accumulated positive interactions while $\beta_{i,j}$ which represents the accumulated negative interactions of node *i* on *j*. The calculation is based on the beta-function by applying the values of $\alpha_{i,j}$ and $\beta_{i,j}$ in Eq.1

$$T_{i,j=}\frac{\alpha_{i,j}}{\alpha_{i,j}+\beta_{i,j}} \quad \text{.....(1)}$$

C. Experimental Setup:

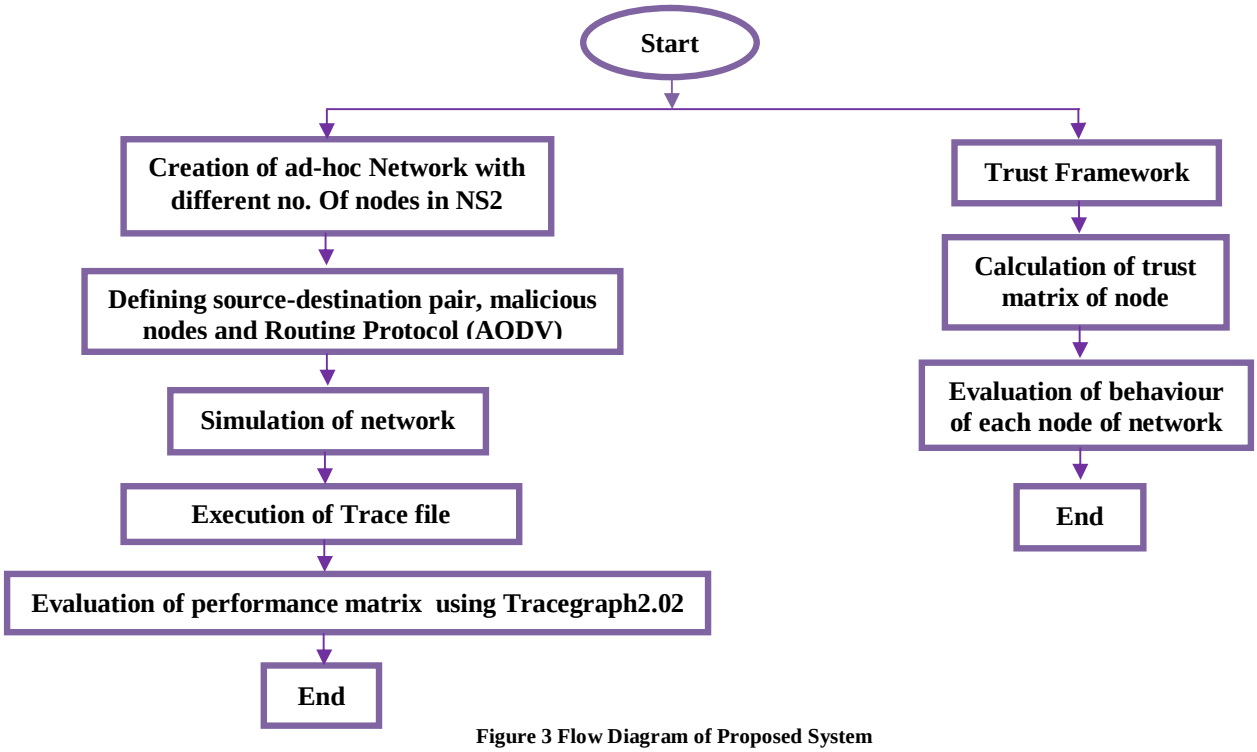


Figure 3 Flow Diagram of Proposed System

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 11, November 2017

Execution Flow of Proposed System is as follows

a. Implementing ad-hoc network using NS2 network simulator for 25 nodes, 35 nodes, 50 nodes and 60 nodes.
b. Introducing normal as well as malicious nodes in the network. Property of malicious is defined in terms of forwarded and dropped packet that means it will never forward packet.
c. Defining no. of source and destination pair for different network. Node will always use TCP that is transmission control protocol is used to transmit data and FTP that is file transfer protocol application is being used.
d. Implementing AODV routing protocols.
e. Interacting the nodes and routing data between nodes using AODV routing protocols.
f. Simulation of network (creation of NAM file).
g. Execution of trace file in Tracegraph software
h. Evaluation of performance matrix (throughput, average E2E delay, PDR) of different network implemented in terms of increasing no. of nodes.
i. Using trust formula calculating the value of trust matrix of nodes.Evaluation of each node of network based on trust matrix.

D. Performance Matrix

Performance matrix of network is combination of Packet delivery ratio, throughput, average end to end delay.

a. PDR is defined as the ratio between the received packets by the destination and the generated packets by the source [12].
b. Throughput is defined as the total number of packet delivered at a unit of time [12].
c. Average end to end delay is the time taken by a packet to reach its destination through the desired route from source. It is also defined as the sum of all time differences between the data packet sent and received divided by the number of packets [12].

IV. SIMULATION

The simulation is conducted by the NS2 simulator. Several nodes are randomly selected. Each source transmits packets per second with FTP. The packet size is 1500 bytes and the simulation time is 30s. For every network some nodes are defined as malicious nodes malicious nodes as they never forward packet. Configuration of network is shown below in table 1.

Table 1 Ad-hoc Network Configurations

Parameter	**Value**			
Nodes	25	35	50	60
Area	1100×500	1500×1000	2000×1000	2000×1000
Radio Range	250m	250m	250m	250m
Movement	Random waypoint	Random waypoint	Random waypoint	Random waypoint
No. of source destination pair	4	6	9	10
No. of malicious nodes	4	7	10	12
Routing Protocol	AODV	AODV	AODV	AODV
MAC	802.11	802.11	802.11	802.11
Application	FTP	FTP	FTP	FTP

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

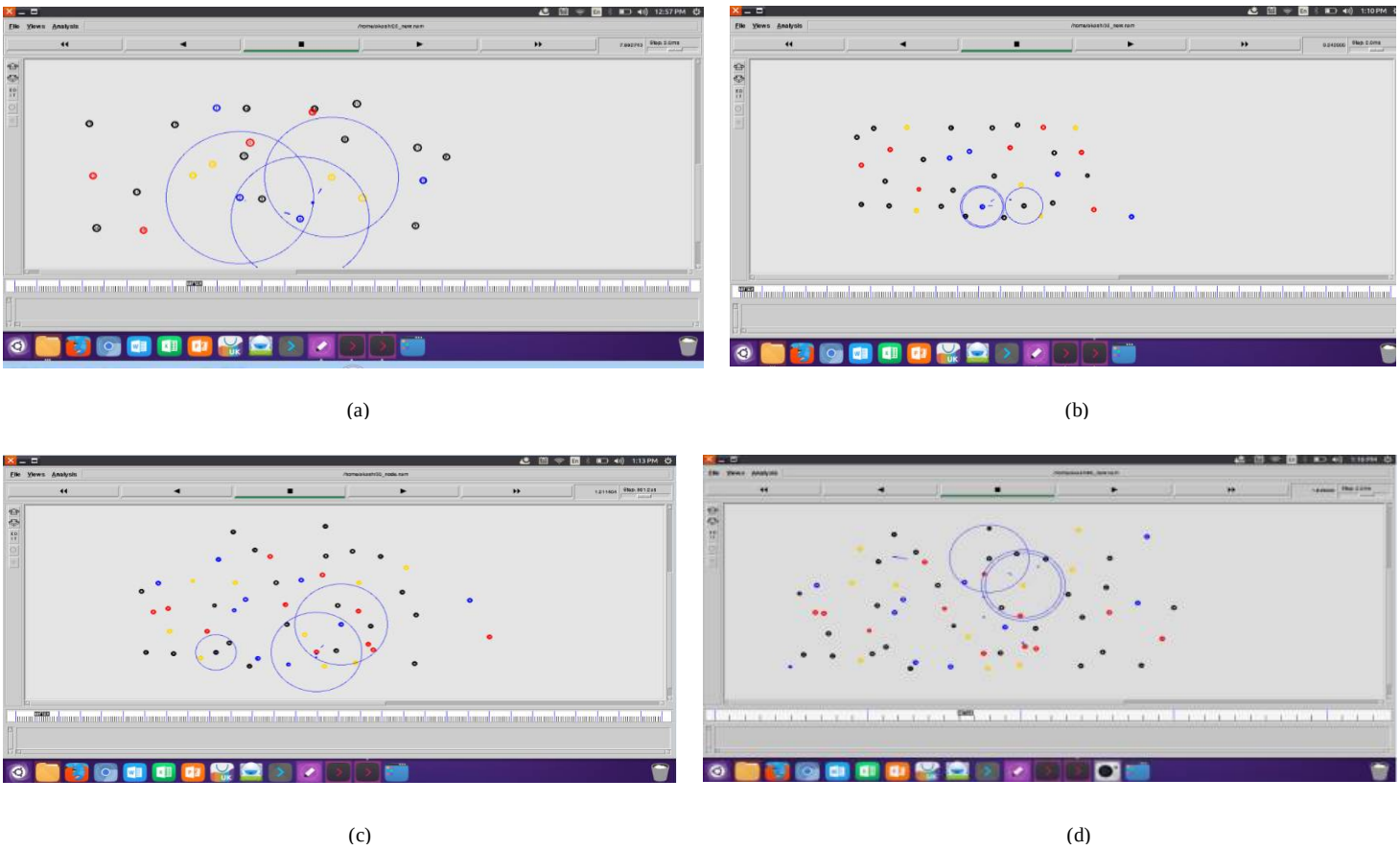
(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 11, November 2017

Packet size	1500 byte	1500 byte	1500 byte	1500 byte
Simulation time	30 sec.	30 sec.	30 sec.	30 sec.
Trust Threshold	0.2	0.2	0.2	0.2

Simulation of 25, 35, 50 and 60 nodes are done in NS2. In every network blue nodes are transmitter and gold nodes are receiver. Malicious nodes are represented by red colour and black nodes are remaining communicating nodes. Transmission of data is indicated by dash, acknowledgement is indicated by continuous dotted line and dropping od packet is indicated by dots. NAM file of every network is shown below.



(a) (b)

(c) (d)

Figure 4 Simulation (a) Simulation with 25 nodes (b) Simulation with 35 nodes (c) Simulation with 50 nodes (d) Simulation with 60 nodes

Simulation of 25 nodes shows that dropping of data from node 12 which is malicious node. Simulation of 35 nodes shows that dropping of data from node 6 which is malicious node. Simulation of 50 nodes shows that sending of data from node 10 and dropping of data from node 8 which is malicious node. Simulation of 60 nodes shows that sending of data from node 59 which is transmitter and dropping of data from node 12 which is malicious node.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

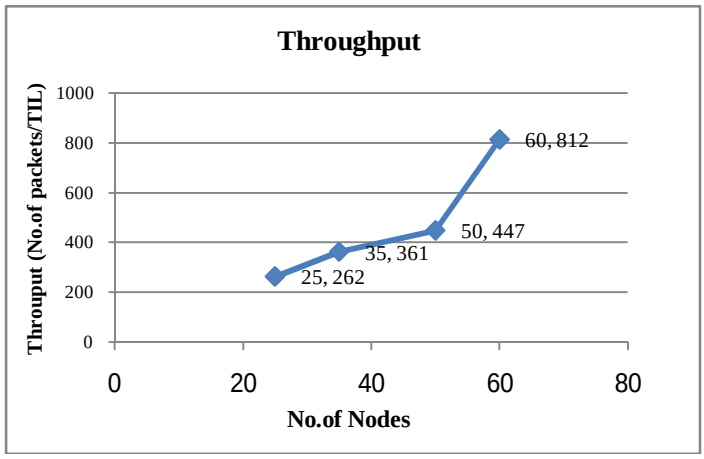
(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

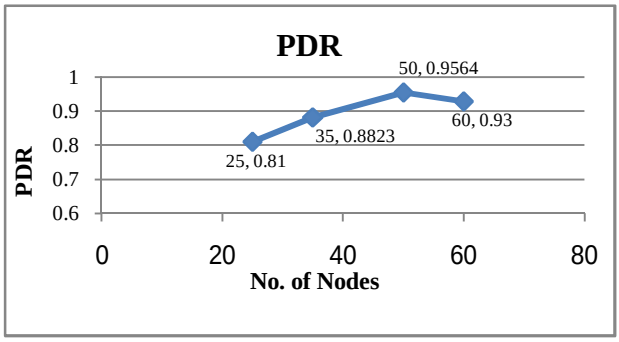
Vol. 6, Issue 11, November 2017

V. EXPERIMENTAL RESULTS

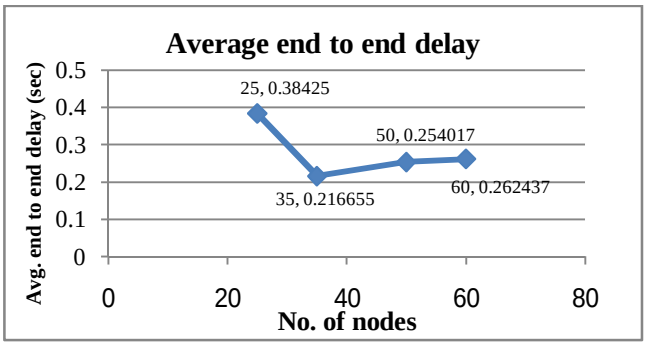
A. Performance Matrix: Evaluation of performance of network is carried out in terms of performance matrix. Performance matrix includes throughput, average end to end delay and packet delivery ratio. Evaluation of network in terms of performance matrix is shown with increasing no. of nodes.



(a)



(b)



(c)

Figure 5 Performance Matrix (a) Throughput Vs No. of Nodes (b) PDR Vs No. of Nodes (c) Average end to end delay Vs No. of Nodes

a. **Throughout:** Analysis of throughput shows that throughput of network becomes better as we increase the no. of nodes in the network. As increasing no. of nodes routing protocol gets more paths to deliver data at receiver hence throughput becomes better as we increase no. of communicating nodes.

b. **Packet delivery ratio:** PDR of network becomes better as we increase the no. of nodes in the network since nodes routing protocol gets more paths to deliver data to receiver. The PDR of network of 60 nodes is less than network of 50 nodes network as with increasing communicating nodes the no. of source destination pair and malicious nodes are also increasing. Malicious nodes lead to delay in packet delivery.

c. **Average end to end delay:** Average end to end delay: Average end to end delay of network becomes less as we increase the no. of nodes in the network. Average end to end delay also depends upon routing protocol, intermediated nodes etc. Here 25 nodes network is having maximum delay and other network shows less delay as compared to 25 nodes network. Delay of 50 nodes network is little more than 35 nodes network because

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 11, November 2017

with increasing communicating nodes the no. of source destination pair and malicious nodes are also increasing. Malicious nodes lead to more delay in the network.

B. **Trust Matrix:** Beta distribution is estimated by two parameter α and β where α represents accumulation of positive observations (forwarded packets) and β represents accumulation of negative observations (dropped packet). Trust matrix is calculated using formula $\frac{\alpha_{i,j}}{\alpha_{i,j}+\beta_{i,j}}$ where $\alpha_{i,j}$ represents the accumulated positive interactions while $\beta_{i,j}$ which represents the accumulated negative interactions of node i on j. Based on this formula we can come to know the behavior of each node of network.

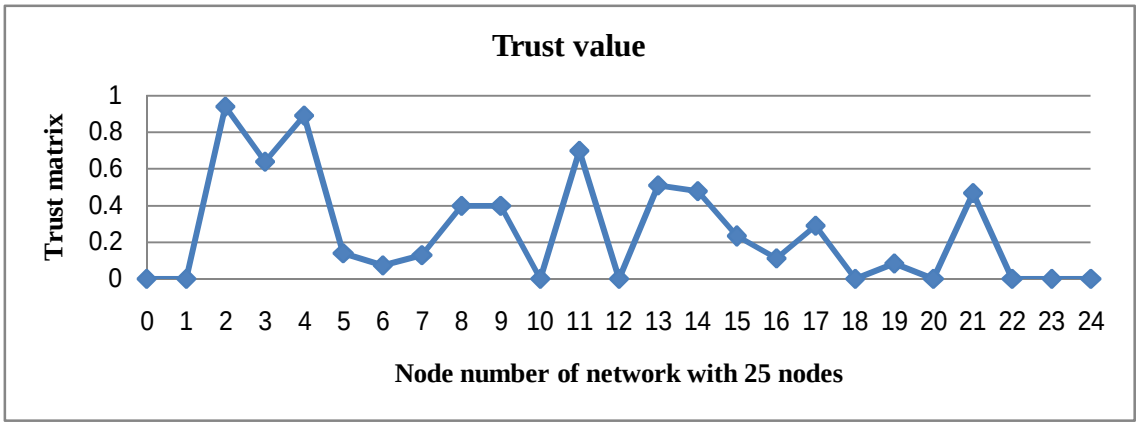


Figure 6 Trust matrix of network with 25 nodes

The below analysis shows trust values of each node of 25 nodes network based forwarded and dropped packet. Here node 0, 12, 18, 22, 24 having trust value 0 hence they are considered as malicious nodes. Node 2, 3, 4, 8, 9, 11, 13, 14, 21 shows better result in terms of trust. Node 5, 6, 16, 19 shows trust values less then threshold value hence they can be considered as misbehaving nodes. Node 1 and 10 also shows trust values of 0 but they are not malicious nodes as they are transmitter so their main concern is to generating and sending packets during processing of 30 seconds instead forwarding packet. Node 15 and 17 shows trust values slightly greater than threshold value hence they may be trusted node. Node 7 and 20 shows less trustworthiness since they receiver and hence their main concern is to receive data during processing. Similarly analysis can be done on each nodes of other network depends on their trust values.

VI. CONCLUSION

Simulation and analysis of network shows that with increasing no. of nodes the performance matrix shows better result. Since MANET is infrastructure less network therefore accomplishing routing is challenging tasks. Reactive routing protocol gives better result as compared to others. AODV and DSR both perform very well but AODV gives better PDR. Routing protocols only routes data from source to destination based on their algorithm but it does not evaluate the nature of each node of network. Proposed system has evaluated the nature of nodes in terms of trust matrix which is based on forwarded and dropped packets.

REFERENCES

[1] Y. Du, C. Herrmann, P. May, S. N. Hulyalkar and D. Evans, "Wireless ATM LAN with and without infrastructure," *Broadband Switching Systems Proceedings, 1997. IEEE BSS '97., 1997 2nd IEEE International Workshop on*, Taiwan, 1997, pp. 120-128.

[2] H. Deng, W. Li, and D. P. Agrawal, "Routing security in wireless ad hoc networks," *Communications Magazine, IEEE*, vol. 40, pp. 70-75, 2002.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 11, November 2017

[3] R. R. Nair and S. Indira Gandhi, "Performance analysis of threshold based hybrid routing protocol for MANET," *2015 3rd International Conference on Signal Processing, Communication and Networking (ICSCN)*, Chennai, 2015, pp. 1-6.

[4] Z. Ullah, M. H. Islam and A. A. Khan, "Issues with trust management and trust based secure routing in MANET," *International Bhurban Conference on Applied Sciences and Technology (IBCAST)*, ISSN: 2151-1411, pp. 402-408, 2016.

[5] M. Imran and M. A. Qadeer, "Evaluation Study of Performance Comparison of Topology Based Routing Protocol, AODV and DSDV in MANET," *2016 International Conference on Micro-Electronics and Telecommunication Engineering (ICMETE)*, Ghaziabad, 2016, pp. 207-211.

[6] V.G.Muralishankar and Dr. E.D. Prakashraj, "Routing Protocols for MANET: A Literature Survey," *International Journal of Computer Science and Mobile Applications*, ISSN: 2321-8363, vol.2, pp. 18-24, ISSN: 2321-8363, 2014.

[7] A.Shabat, K.Dahal, S.Bista and k.Awan, "Recommendation Based Trust Model with an Effective Defence Scheme for MANETs", *IEEE Transactions on Mobile Computing*, ISSN: 1536-1233 , vol.14, pp. 2101-2115, 2015.

[8] Z.Movahedi, Z.Hosseini and F. Bayan, "Trust-distortion Resistant Trust Management Frameworks on Mobile Ad-hoc Networks: A Survey," *IEEE Communications Surveys & Tutorials*, vol.18, no. 2, pp. 1287-1309, 2016.

[9] M. N. Alslaim, H. A. Alaqel and S. S. Zaghloul, "A comparative study of MANET routing protocols," *The Third International Conference on e-Technologies and Networks for Development (ICeND2014)*, Beirut, 2014, pp. 178-182.

[10] D.Bhatia and D.Sharma, "A Comparative Analysis of Proactive, Reactive and Hybrid Routing Protocols over Open Source Network Simulator in Mobile Ad-hoc Network", *International Journal of Applied Engineering Research*, pp: 3885-3896, ISSN No.0973-4562, vol.11, 2016.

[11] A.Shabut, K.Dahal and I.Awan, "Friendship Based Trust Model to secure routing protocols in Mobile Ad-hoc Networks," *International Conference on Future Internet of Things and Cloud*, pp: 208-287, ISSN No. 14834354,2014.

[12] P. Kaur, Dr. D. Kaur and Dr. R. Mahajan, "The Literature Survey on Manet, Routing Protocols and Metrics," *Global Journals Inc.(USA)*, ISSN: 0975-4350 , vol.15, 2015.