ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

An Enhanced Fuzzy Approach For Relay Node Selection in Manets

Er.Hemant Sharma, Er. Navneet Kaur

M.Tech Student (Wireless Network), Dept of Computer Science & Engineering(CSE), Global Institute of Management & Emerging Technology, Amritsar, affiliated to Punjab Technical University, I K Gujral, Kapurthala, Punjab, India.

Associate Professor, Dept. of Computer Science & Engineering (CSE), Global Institute of Management & Emerging Technology, Amritsar, affiliated to Punjab Technical University, I K Gujral, Kapurthala, Punjab, India

ABSTRACT: MANETs are Mobile ad hoc networks which comprises of mobile nodes and the host node relies on each other in order to maintain the connectivity of the network. The MANETs are more prone to security attacks that can ruin the confidentiality of the information. The various attacks such as unauthorized access to data by unauthenticated users, wormhole attack, and spoofing, eavesdropping, denial of service are the most common attacks that can take place in MANETs to break the security of sensitive information. There is wide variety of secure routing techniques in the market but all of those techniques did not consider all the relevant parameters for establishing a security for data plane in network. This study develops a secure routing protocol by using fuzzy logics, delay factor, packet delivery ratio, indirect trust and direct trust with OLSR routing protocol. The results section shows the output graph of the proposed work.

KEYWORDS: Ad Hoc Networks, MANETs, Trustworthiness. Security, OLSR, Direct Trust, Indirect Trust, PDR, Delay

I. INTRODUCTION

Ad hoc networks are wireless network which did not follow any physical topology and poses a feature of multi-hop data packets[1]. MANETs are a type of ad hoc networks that comprises of large number of mobile nodes which are interconnected through wireless medium and do not have any centralized device or server. MANETs are the advantageous network as compare to other networks as it comprises of low infrastructure maintenance cost, less complex to implement[2], fault tolerance etc. The MANETs are widely used wireless network but there are some issues that have adverse effects on reliability of the network. These issues are lacking of centralized structure due to which each and every hub in the network act as a router [3]. In MANETs each node is responsible for delivery of data packets to destination node [4].MANETs also suffers from security issues. The node's mobility and wireless property of MANET makes it more prone to come in contact with malicious nodes that can affect the confidentiality of the nodes [5].There are lots of routing protocols are available in the market that claims to achieve high security level in wireless networks[6]. But after having a review to the previous research work that had been conducted in this field it is concluded that these protocols were proved beneficiary only when more than one protocols were used collaboratively [7].

Trust based routing is one of the techniques that is used to provide security to the data in the MANETs [8]. This study is mainly conducted to implement a secure routing approach i.e. OLSR (Optimized Link State Routing) by using direct trust, Indirect trust, packet delivery ratio, and delay which act as membership function to fuzzy logics and then relay node or next hop will be selected on the basis of overall rating of nodes that is generated by fuzzy logics as an output to attain high level security of data planes in ad hoc network[9].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

Direct Trust:
Direct trust refers to the term or values which is evaluated for a node to another node. It is based on the process of communication with other node [10]. On the basis of this concept the actions of the network are categorized into two forms i.e. Positive events and Negative Events. Positive events refer to the events or actions such as route error, route request, route reply or data flow. Whereas the events like flooding, deletion of routes, packet dropping falls into the category of negative events. Direct trust is evaluated by using the following equation:

$$DT^{A,B} = W_H^{DT} \times \left[\prod (tm_1^{A,B}, tm_2^{A,B}, tm_3^{A,B}, \dots tm_k^{A,B})\right]^{(1/k)} + W_L^{DT} \times \frac{1}{l}\left[\sum tm_1^{a,b}, tm_2^{a,b}, \dots tm_k^{a,b}\right]$$

$$DT^{A,B} = W_H^{DT} \times \left[\prod_{m=1\ to\ k} tm_m^{A,B}\right]^{1/k} + W_L^{DT} \times \frac{1}{l}\left[\sum_{n=1\ to\ l} tm_n^{a,b}\right] \quad (1)$$

Indirect Trust or Recommended Trust:
In this form of trust the node which provides reference corresponding to the particular node is known as recommender node [11]. The node, against which the reference is added in known as recommended node. In this the route data packets are responsible to obtain the recommendations. Following equation is used for calculating indirect trust value in trust models:

$$IT^{A,B} = W_H^{IT} \times \left[\prod_{i=1\ to\ r} W_{A,N_i} \times T^{N,B}\right]^{1/r} + W_L^{IT} \times \frac{1}{S}\sum_{j=}^{s}\left(W_{A,N_j} \times T^{N_j,B}\right) \quad (2)$$

Packet Delivery Ratio:
PDR is a parameter that is calculated to rate the overall performance of wireless ad hoc network. PDR depicts the amount or ratio of the data packets that are delivered to the destination node [12].
Delay: Delay or average delay is a parameter that is used to measure the delay that takes place while delivering data packets from source to destination node [13].
Fuzzy Logics: Fuzzy Interference system is a logical mechanism that is based on multi valued logics. These multiple values are in the form of membership functions that are input to the fuzzy logic system [14]. Then these membership functions are fuzzified by using defined set of rules and generate a single output. It is one of the prominent techniques that is widely used in every field to enhance the overall performance of the systems.

III. PROBLEM FORMULATION

Ad hoc networks are wireless sensor networks in which the nodes are distributed spatially and are specialized to sense the surrounding data such as temperature, sound, pressure etc. Then this sensed data transmitted to the sink node by creating route by utilizing various adjacent nodes. The more modern networks are bi-directional, also enabling control of sensor activity. Due to the characteristics such as openness and dynamic topology, ad-hoc networks suffer from various attacks in the data plane. Even worse, some attacks can subvert or bypass the frequently used identity-based security mechanisms. To secure the data plane of ad-hoc networks, trust management system was proposed. In the tradition approach fuzzy logic is used to calculate path trust basis on average delay (AD) and PDR (Packet Delivery ratio).

IV. PRESENT WORK

Ad hoc networks are a kind of wireless network that poses various features like self organization, and also follows the temporary network structure. It comprises of large number of sensor nodes. But it has various disadvantages such as security issues as MANETs are more vulnerable to security attacks. Many researches were done were based on the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

security of the system but as discussed in above section the number of parameters that was considered was quite less and insufficient for achieving the high security. So there is a need to propose a new algorithm that is that will consider sufficient and reliable list of parameters for high security purpose. So a new approach is to be proposed that will increase the number of parameters along with the fuzzy system. The parameters that will be used in proposed works are as follows:

1. Packet Delivery Ratio
2. Average Delay
3. Direct Trust
4. Indirect Trust

PDR refers to the ratio or amount of packets that are delivered to the destination node. Average Delay refers to the amount of delay that has been occurred while data transmission from source node to destination node. Direct trust refers to the evaluation of trust value from a node to another node directly. For example, to calculate the trust value between node1 and node2. Indirect Trust refers to calculating the trust value from a node to another node via intermediate node. For example, to evaluate the trust value between node1 and node3 via node2.

The step wise processing or methodology of proposed work is given below.

1. Initialization of network by defining number of nodes in network, area covered by the network, location of the nodes that are going to deploy in the network. All these parameters are mandatory to create a network.
2. Next step is to deploy the nodes in the network as per values are given in previous step.
3. In this step the quality parameters such as PDR, DT, IT and delay will be evaluated.
4. Fuzzy logic system s initialized after declaring QoS parameters and these parameters are considered as an input to the fuzzy logics.
5. After initializing the fuzzy logics the next step is to define the set of rules in fuzzy that will help to generate the final output on the basis of received input parameters.
6. Now select source and destination node so that data transmission can done from source node to sink node in the network.
7. Elect the nodes for routing within the coverage area on the basis of evaluated parameters.
8. Now perform Deffuzification and after this step the overall rating of the nodes which relies within coverage area will be generated.
9. Now select the relay node from elected nodes on the basis of highest value of overall rating of the nodes.
10. Last step is to evaluate the results in the form of PDR, Delay and then perform the comparison of results with traditional mechanisms to prove the proficiency of proposed work.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Website: www.ijircce.com
Vol. 5, Issue 6, June 2017

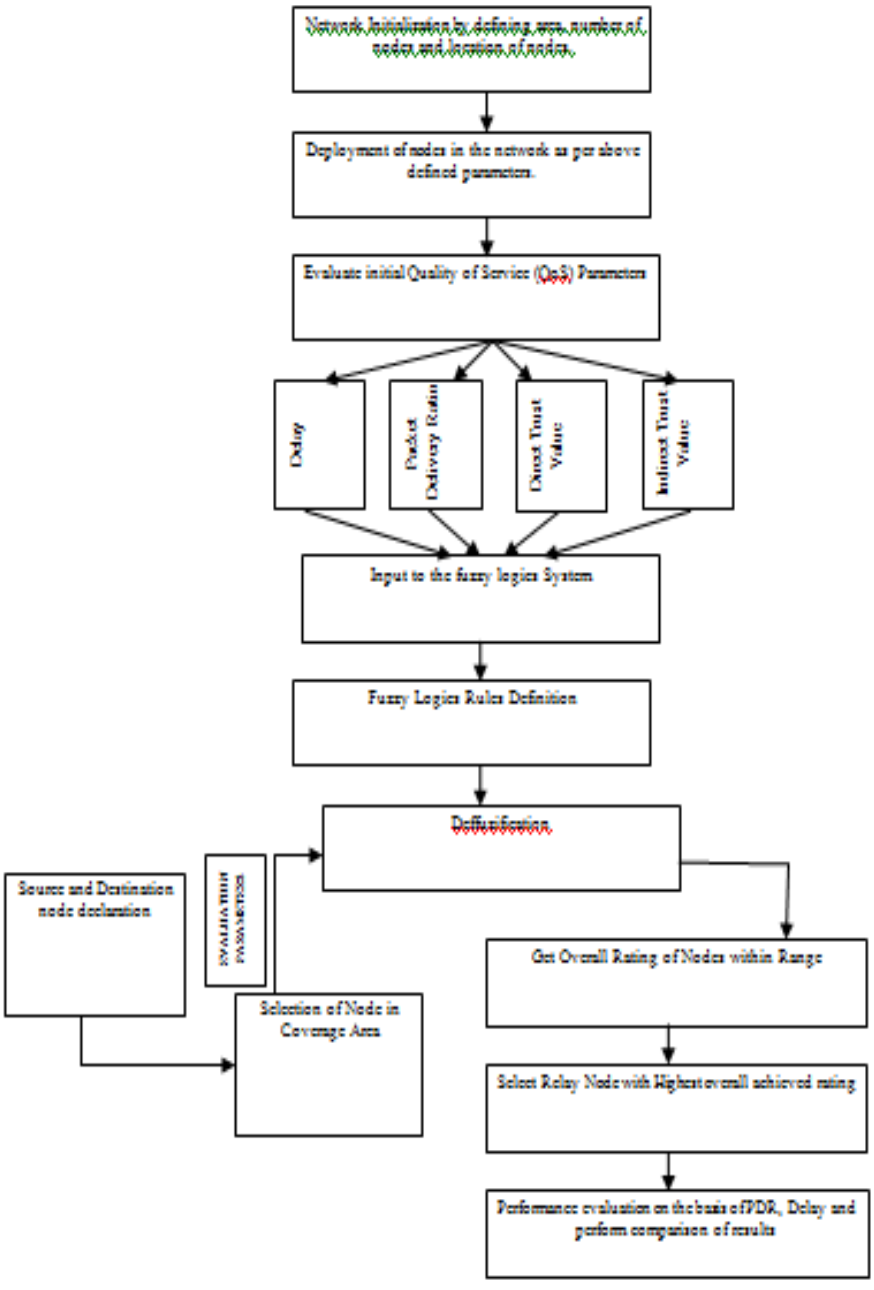

Figure 1 Block Diagram of proposed work

II. RESULTS AND EXPERIMENTS

This section represents the results of the proposed work in the form of graphs that are received after implementing the new work. The results proves the proficiency of proposed work over conventional work in the form of various performance parameters such as packet delivery ratio, delay etc. The figure below shows the fuzzy interference system of proposed work. Here we can see three membership functions as direct rust, packet delivery ratio, average delay and

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

indirect trust are input to the fuzzy logics which is comprises of total 81 set of rules and regulations and finally generates a overall rating as an output of the system.

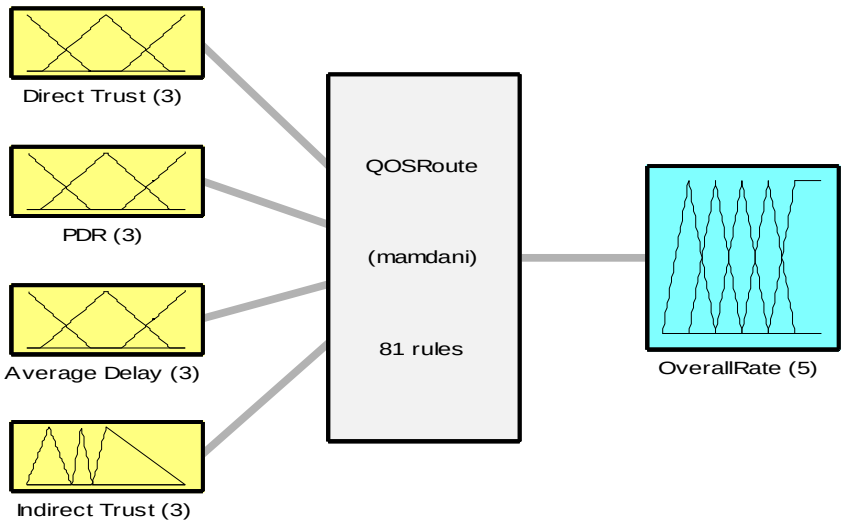

Figure2 proposed Fuzzy Interference Systems

Figure from 3 to 7 shows the graph of membership functions of direct trust in figure 3, packet delivery ration in figure 4, average delay in figure 5, indirect trust in figure 6.

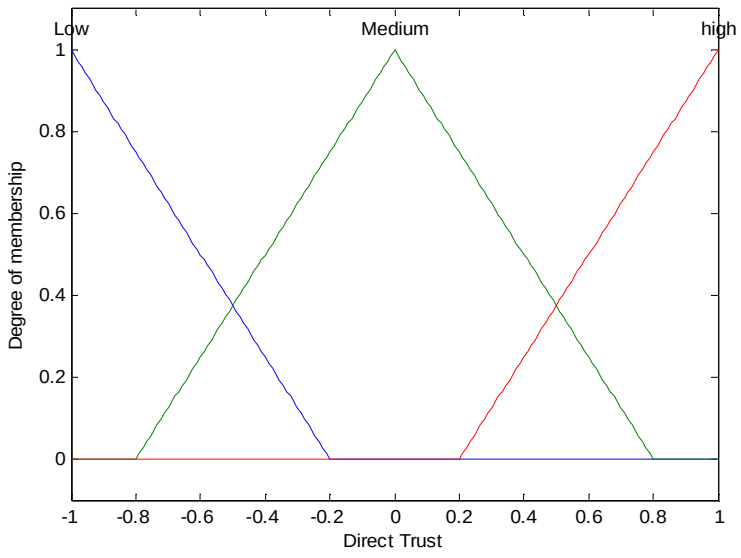

Figure 3 Membership function of Direct trust

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

The y axis in this graphs calibrates the data ranges from 0 to 1 in each and every membership function but the value of x axis varies as in figure 3 the value of x axis lies between -1 and 1, in figure 4 the value o0f x axis corresponding to PDR is between 0 to 100, the value of x axis in graph of average delay is calibrated from -1 to 1 and the value of x axis in indirect trust ranges from -40 to 100.

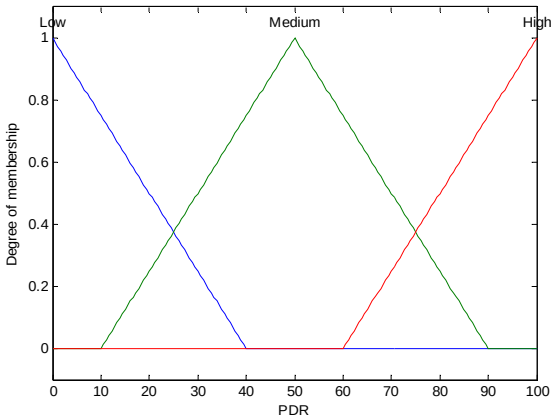

Figure 4 Membership function of PDR

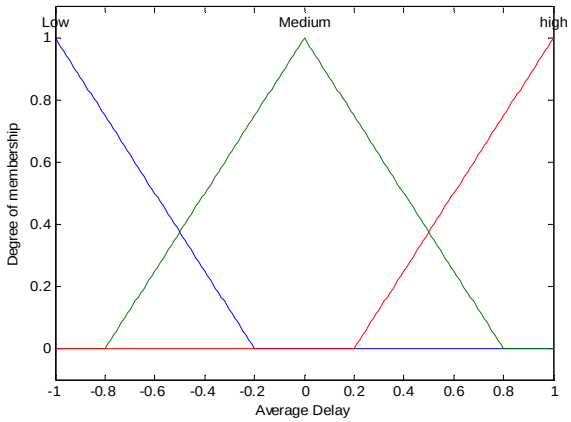

Figure 5 Membership function of Direct trust

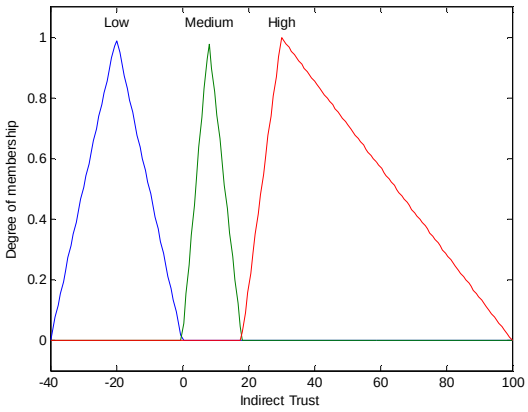

Figure 6 Membership function of Indirect Trust

The given figure 7 represent the overall rating of the nodes in the form of graph membership function. In this graph x axis ranges from 0 to 120 and y axis ranges from 0 to 1. The membership function has five stages as very low, low, medium, high and very high. This graph is generated after getting the output from fuzzy system on the basis of given inputs and defines set of rules and regulations.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

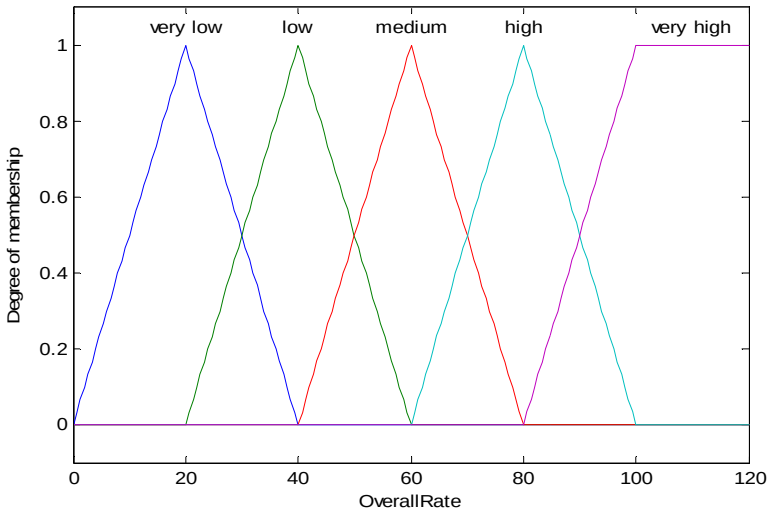

Figure 7 Membership function of overall rating of the nodes.

The graph given in figure 8, shows the values of overall rating, packet delivery ratio and direct trust value that is evaluated after implementing the proposed work. Here the y axis represents the values of overall rating that ranges from 25 to 60, y axis depicts the PDR that starts from 0 and end at 100 and z axis shows the value of direct 6trust which is calibrated from -1 to 1.

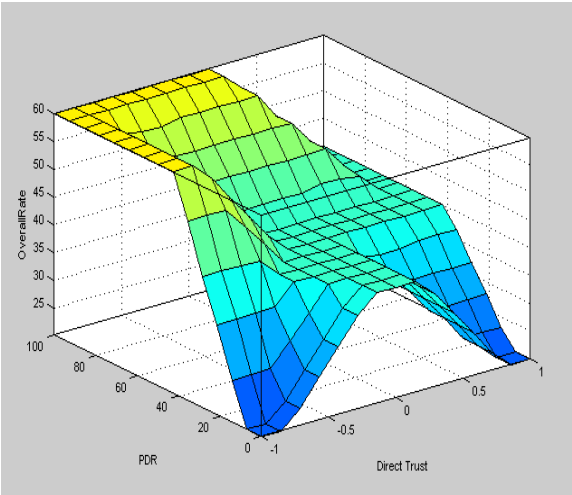

Figure 8 3D graph of overall rating, PDR and Direct Trust value of the proposed work.

The figure 9 represents the proposed network which comprises of nodes and it also depicts the source and destination nodes by highlighting them with red color. It also represents the elected path from source to destination node by adjoining the selected nodes for route creation. The nodes of the network are shown in round shape and the nodes that are used for route creation is shown by square marked with blue color.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

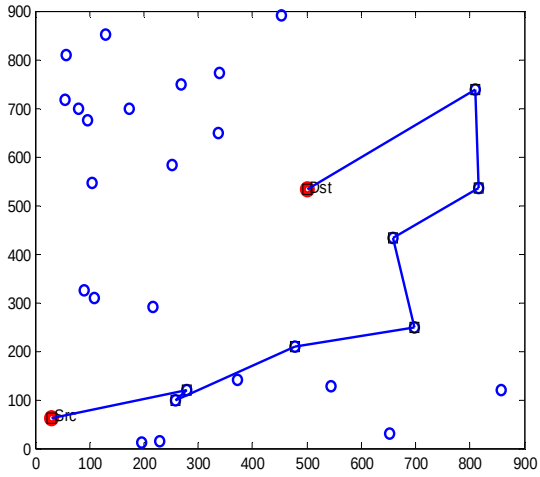

Figure 9 proposed network with created route from source to destinations

The graph below depicts the comparison of proposed work with existing work in the form of PDR. The proposed technique is named as DPDIT-OLSR i.e. Delay, PDR, Direct Trust and Indirect Trust-OLSR technique. The comparison is done between FGT-OLSR, MDI-OLSR and proposed work. From the graph below it is observed that the PDR of proposed work is higher as compare to rest f the techniques whereas the PDR of FGT-OLSR is quite closer to the PDR of proposed work.

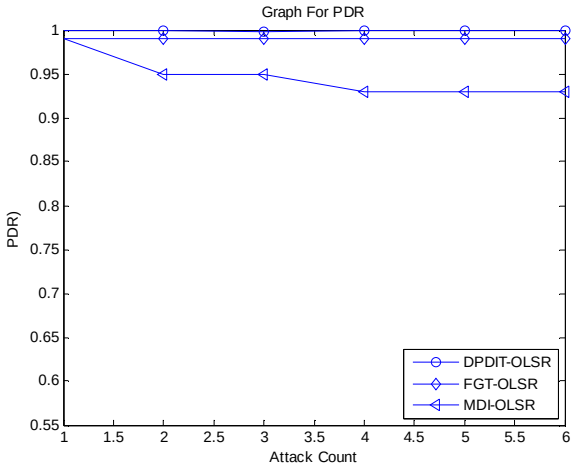

Figure 10 Comparison on the basis of packet delivery ratio

The figure 11 represents the comparison on the basis of end to end delay. The graph depicts that the value of end to end delay in case of proposed work starts from 0 and end at 0.01. The end to end delay is evaluated on the basis of attack counts in the network. The x axis comprised of attack counts and this values lies between 1 and 6. The value of end to end delay is notified to increasing with the increment in attack counts. The graph depict the difference that the delay of proposed work is lower as compare to other techniques which proves that the proposed work is better than other two methods because the end to end delay of an ideal network is always low.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

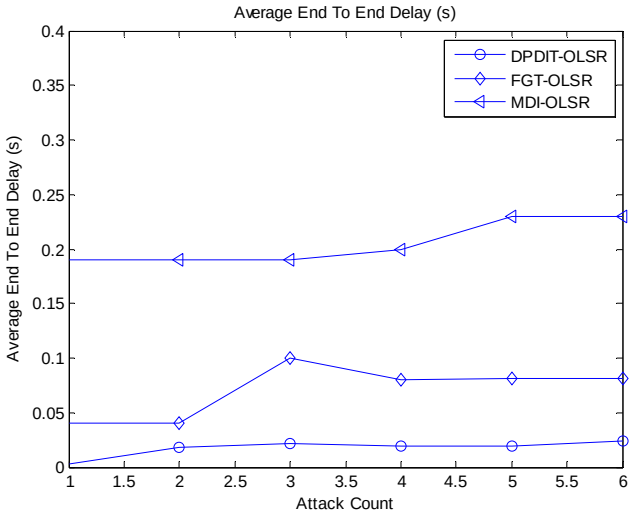

Figure 11 Comparison on the basis of end to end delay of data packet transmissions.

The figure 12 below compares the FGT-OLSR, MDI-OLSR and DPDIT-OLSR on the basis of control message overhead. Control message overhead is a term that is used to measure the amount of messages that is generated by an node per second. The control overhead in case of proposed work is evaluated to 0.86 whereas in case of FGT-OLSR it is measured to 0.8 and in case of MDI-OLSR it is notified at 0.82. Hence it is concluded that the control message overhead of proposed work is higher as compare to other two techniques.

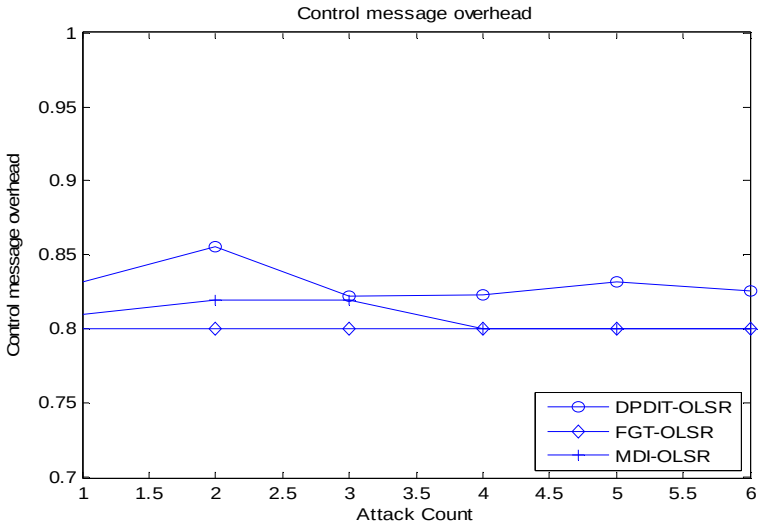

Figure 12 Comparison on the basis of control message overheads

III. CONCLUSION

On the basis of above defined section it is concluded at last that this study developed a novel trust based mechanism for providing high level security to the data plane in ad hoc network. The proposed is a collaboration of fuzzy logics, OLSR, PDR, Direct Rust, Indirect Trust and delay which works on the basis of logics, rules and regulations to derive an efficient decision at last. The proposed work is named as DPDIT-OLSR and the result section shows that it

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

outnumbers the FGT-OLSR and MDI-OLSR with respect to PDR, Delay and control message overheads. For further improvements, other routing protocols can be considered for implementations.

REFERENCES

[1] Shuaishuai Tan et al, "A Trust Management System for Securing Data Plane of Ad-Hoc Networks", IEEE, transactions on vehicular technology, vol. 65, no. 9, pp 7579- 7592, September 2016
[2] Sudha Dwivedi et al, "Review in Trust and Vehicle Scenario in VANET", IEEE, Future Generation Communication and Networking Vol. 9, No. 5, pp. 305-314, 2016
[3] Pooja Pilankar et al, "Trust based security in manet", IJRET: International Journal of Research in Engineering and Technology, 2319-1163, Volume: 05 Issue: 02 , Pp 12-19, Feb 2016
[4] Shuaishuai Tan et al, "Trust based routing mechanism for securing OSLR-based MANET ", ELSEVIER, Adhoc Networks, March 2015
[5] Shirina Samreen et al, "Trust based Data Plane Security Mechanism for a Mobile Ad hoc Network through Acknowledgement Reports", International Journal of Computer Applications (0975 – 8887), Volume 129 – No.6, pp 6-13, November2015
[6] Bijender Bansa et al, "Attacks Finding and Prevention Techniques in MANET: A Survey", IEEE, Wired and Wireless Communications Vol.4, Issue 2, Pp 1-7, 2015
[7] Savitha. M et al, "A Study on Various Attacks in Wireless Ad hoc Sensor Network", International Journal of Computer Science and Mobile Computing, vol 3, issue 9, pp 231-243, September 2014
[8] Ranjitha.R et al, "Secure Wireless Ad-Hoc Sensor Network from Vampire Attack Using M-DSDV", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 5, pp 4081-4087, May 2014
[9] X. Anita, et al, "Fuzzy-Based Trust Prediction Model for Routing in WSNs", HINDAWI, Volume 2014 (2014), Pp 1-11, July 2014
[10] Z. Wei etal, "Security enhancements for mobile ad hoc networks with trust management using uncertain reasoning", IEEE Trans. Veh. Technol., vol. 63, no. 9, pp. 4647–4658, Nov. 2014
[11] H. Xia, et al., "Trust prediction and trust-based source routing in mobile ad hoc networks", IEEE, Ad Hoc Netw., vol. 11, no. 7, pp. 2096–2114, Sep. 2013.
[12] Vanita Rani et al, "A Study of Ad-Hoc Network: A Review", International Journal of Advanced Research in Computer Science and Software Engineering, vol 3, Issue 3, Pp 135-138, March 2013
[13] Ashish Kr. Shrivastava et al, "Study of Wormhole Attack in Mobile Ad-Hoc Network", International Journal of Computer Applications, vol 73, Issue 12, Pp 32-37, July 2013
[14] M. Marimuthu et al, "Enhanced OLSR for defence against DoS attack in ad hoc networks", J. Commun. Netw., vol. 15, no. 1, pp. 31–37, Feb. 2013.
[15] Kartheesan, L et al, "Trust Based Packet Forwarding Scheme for Data Security in Mobile Ad Hoc Networks", OSR Journal of Computer Engineering (IOSRJCE) 2278-0661 Volume 2, Issue 3, PP 40-48, July 2012
[16] D. Chasaki et al, "Attacks and defenses in the data plane of networks," IEEE Trans. Dependable Secure Comput., vol. 9, no. 6, pp. 798–810, Nov. 2012.
[17] P. F. Saverio, A. Detti, C. Pisa, and G. Bianchi, "A framework for packet droppers mitigation in OLSR wireless community networks," in Proc. IEEE ICC, pp. 1–6. 2011
[18] Tameem Eissa et al, "Trust-Based Routing Mechanism in MANET: Design and Implementation", SPRINGER, Mobile NetwAppl, Pp 1-12, June 2011
[19] Pushpita Chatterjee, "TRUST BASED CLUSTERING AND SECURE ROUTING SCHEME FOR MOBILE AD HOC NETWORKS", International Journal of Computer Networks & Communications (IJCNC), Vol.1, No.2, Pp 84-97, July 2009
[20] I. Aad, et al "Impact of denial of service attacks on ad hoc networks", IEEE/ACM Trans. Netw., vol. 16, no. 4, pp. 791–802, Aug. 2008.
[21] Bing Wu et al, "A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks", SPRINGER, In *Wireless network security*, pp. 103-135. Springer US, 2006.
[22] Lidong Zhou et al, "Securing Ad Hoc Networks", IEEE, Pp 1-12, November 1999
[23] Petteri Kuosmanen, "Classification of Ad Hoc Routing Protocols"
[24] Alex Hinds, "A Review of Routing Protocols for Mobile Ad-Hoc Networks (MANET)",IJIET, Vol 3, Pp 1-5, 2013
[25] Charu Wahi, "Mobile Ad Hoc Network Routing Protocols: A Comparative Study", IJASUC, Vol 3, Pp 21-31,2012
[26] Muhammad Imran, "Analysis of Detection Features for Wormhole Attacks in MANETs", Science Direct Procedia Computer Science, Pp: 384-390, 2015.
[27] Sayan Banerjee, "A Review on Different Intrusion Detection Systems for MANET and its Vulnerabilities", IEEE, 2015