iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** VIII **Month of publication:** August 2017

DOI: http://doi.org/10.22214/ijraset.2017.8136

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VIII, August 2017- Available at www.ijraset.com

Improved Security Protocol Using Fuzzy Logic with Multi-parametres in Ad-hoc Networks

Arshpreet Singh[1], Harpreet Kaur[2]
[1] *Student,* [2] *Assistant Professor, ECE Department, BBSBEC Fatehgarh Sahib Punjab, India*

Abstract: ***wireless networking is one of the current attractive fields for researchers in current era. The ad hoc network is a separable part of wireless networking which facilitate the users to perform communication among mobile terminals with limited bandwidth. But as these networks did not follow any physical topology for installation therefore the risk of security attacks an threats are higher in ad hoc networks. Various attacks such a eavesdropping, spoofing, denial of service are difficult to detect in wireless ad hoc networks. So many researchers have been conducted in this field till now but most of them are not capable to achieve high level security of data plane in ad hoc wireless networks. A novel approach for securing data plane in AHNs has been developed under this study. The PRO-OLSR is a combination of fuzzy based system with OLSR routing protocol. The essential parameters like average delay, packet delivery ratio, direct trust and attack suspected ratio are used as an input membership function to fuzzy system. And on the Basis of the output of FIS the next hop for data delivery is elected. The simulation is done in MATLAB and results are generated to proves the proficiency of PRO-OLSR technique.***

Keywords: ***Wireless Ad hoc Networks, Security, Trust Evaluation, OLSR, Fuzzy Inference System, Average Delay, Packet Delivery Ratio and Attack Suspected Ratio.***

I. INTRODUCTION

Ad hoc networks are completely wireless networks which comprised of dynamic nodes which are interconnected to each other to create a communication network [1]. These nodes are dynamic in nature because they have dynamic layout and these nodes also have the feature of limited bandwidth to transmit the data. An ad hoc network is a kind of decentralized network because it did not follow any physical layout or topology for its structure [2]. AHNs are wireless networks which supports the transmission of multi-hop data packets. The ad hoc network is created by using various terminal nodes and these terminals are used to generate services to other terminals [3] because these terminal nodes also act as routers in the network. The advantages of ad hoc networks are that these networks are quite flexible , robust in nature and also support nodes mobility due to which all of the nodes in the network are dynamic [4]. MANETs and VANETs are most popular form of ad hoc communication networks. Following are some characteristics of ad hoc networks [5]

A. All the nodes in the AHNs are mobile therefore it follows a dynamic topology for network installation.
B. The operations in AHNs are energy constrained operations.
C. All the terminals in the ad hoc network have some limited bandwidth for data transmission [6].
D. AHNs are more prone to physical security threats such as eavesdropping, spoofing DOS attacks etc.

Ad hoc networks have been attaining the attention of lots of researchers due to their feature of self-configuration and self-maintenance [7].

The advantages and applications of ad hoc networks are as follows:

1) AHNs facilitate the users to have an access to the information and services of the network [8].
2) It did not stick to any specific geographical location.
3) This network can be installed at anywhere and anytime.
4) Applications of AHNs are [9]
a) Military exercises make use of ad hic networks to securely transmit their confidential data.
b) Disaster relief operations are also makes use of wireless ad hoc networks.

Most of the work focused on the concept of multi hop data delivery, network access and routing in AHNs [10]. But the issue security is also a primary concern because delivering the data securely over the network is one of the major goals of ad hoc networks [11]. The disadvantage of conventional work that had been done in this field to provide security to the data plane in the ad hoc network is that the main focus was on cryptography and encryption methods to secure the data which are quite old and weak methods of security as any person with the access of public or private key can easily decrypt the data and can misuse it or alter it

[12]. To solve this issue the concept of trust management comes to the existence but it also suffers from the problem of lack of vital parameters to maintain the confidentiality of data plane. In this work a novel approach for securing the data plane over the ad hic networks has been developed which utilizes the trust based security mechanism along with fuzzy inference system and OLSR protocol of data security [13]. In literature survey methods which are used worked on a less no of parameters. Due to the characteristics such as openness and dynamic topology, ad-hoc networks suffer from various attacks in the data plane [14]. Even worse, some attacks can subvert or bypass the frequently used identity-based security mechanism .In this paper Fuzzy logic is used with multi-parameters to overcome these problems.

II. WORK DONE

As security in ad hoc is one of the major factors that is considered while the data is sent in the Ad hoc network[15]. In literature many researchers have considered security issues. But the number of parameters that was considered was quite less and insufficient for achieving the high security[16]. So there is a need to propose a new algorithm that will consider sufficient and reliable list of parameters for more 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 used in are-Packet delivery ratio, Average delay, Direct trust and Attack suspected ratio(ASR=RSS/distance).

A. Packet Delivery Ratio

PDR is measurement of number of data packets that has been delivered to the destination node. It is the amount packets that are left when number of dropped packets is excluded from total number of transferred packets[17].It can be evaluated by using the following equation:

$$PDR = \frac{N}{seq_{curr} - seq_{prev}} \qquad (1)$$

In equation (1) seq_{curr} depicts to that packets that has been acknowledged currently and seq_{prev} refers to the previously acknowledged packets. And N represents the total number of transferred packets to the destination.

B. Average Delay

Average delay is the amount of time that is taken to deliver the data packets from source node to destination node[18]. It is calculated as below:

$$AD = \frac{\sum_{j=1}^{m} t_{S_{ack}} - \left(td_N - td_{n_j}\right) - ts_{h_j}}{m.\,AD_{max}} \qquad (2)$$

Here in above equation

AD_{max} Depicts the value of maximum acceptable delay.

C. Direct Trust

Trust management is a scheme that secures the data plane and initialized by evaluating trust factors. Trust can be of two types i.e. direct trust and indirect trust[19]. In this proposal we have considered the direct trust value as one of the parameters for securing the data plane in the AHNs[20]. Direct trust value divides the actions of a network in two categories as follows:

1) *Positive Events in Direct Trust Factor:* The network events such as route error, flow of data or data transmission, route request, route acknowledgment falls under the category of positive events[21].
2) *Negative Events in Direct Trust Factor:* Negative events are the events which has negative impact on network's performance. The events like, flooding, path detection, packet dropping are kind of negative events[22]. Following formula is used for evaluating direct trust factor:

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

$$DT^{A,B} = W_H^{DT} \times \left[\prod_{m=1\ to\ k} tm_m^{A,B}\right]^{1/k} + W_L^{DT} \times \frac{1}{l}\left[\sum_{n=1\ to\ l} tm_n^{a,b}\right] \qquad (3)$$

D. Attack Suspected Ratio

It is a parameter which is evaluated to check that whether the node elected for data transmission is suspicious or not. It is evaluated by considering received signal strength[23].

E. Fuzzy Inference System

Fuzzy Interference system is a rational system that is based on multi valued logics. These multiple values are in the form of membership functions[24] that are input to the fuzzy logic system . In completed work AD, PDR, DT and ASR are the parameters which are given as an input or membership function to proposed fuzzy system.

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[25].

III.METHODOLOGY

The methodology and block diagram of PRO-OLSR is defined in this section.

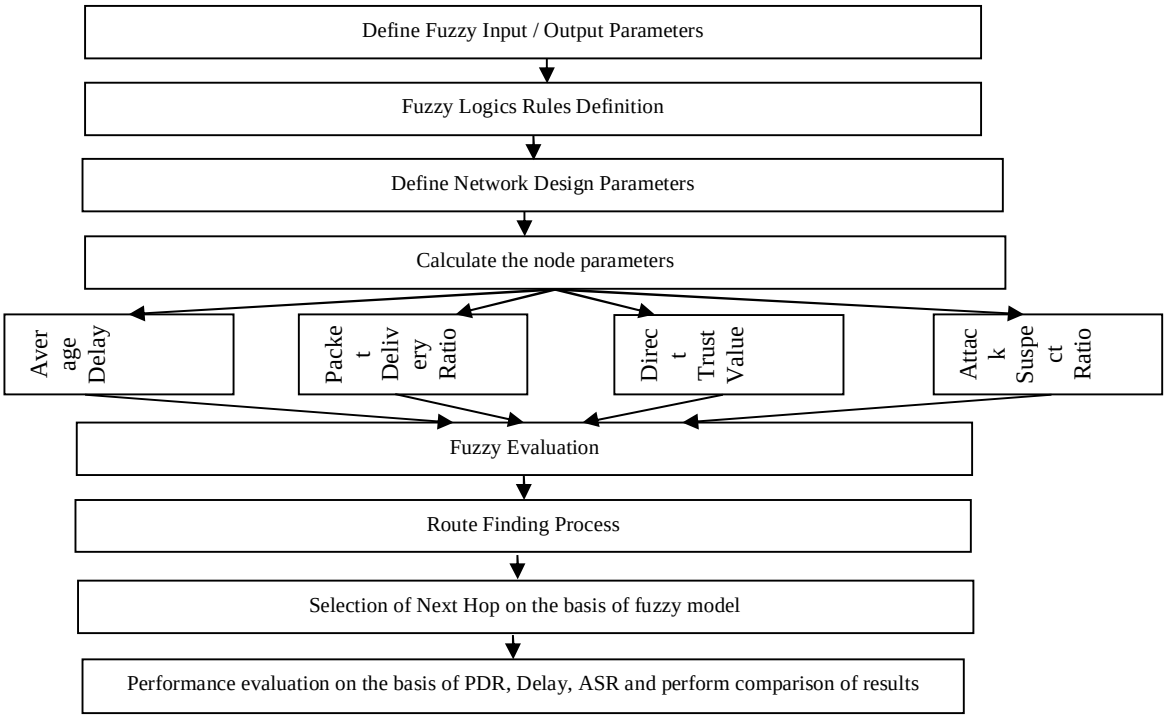


Figure 1 PRO-OLSR Framework

The step by step methodology of PRO-OLSR technique is as below:

A. Define Fuzzy

First step is to design a proposed fuzzy system. In this step the membership function in fuzzy system will be defined. In proposed work there are 4 membership functions i.e. Average Delay, Direct Trust, Packet Delivery Ratio and Attack Suspected Ratio.

B. Rules for Fuzzy System

This step mentions the list of rules for fuzzy inference system. The FIS works upon the basis of defined rules. Here rules are defines in the form If-THEN. For example,

$$IF\ Inp1\ is\ Low\ and\ Inp2\ is\ Low$$
$$THEN\ Output\ is\ Low$$

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VIII, August 2017- Available at www.ijraset.com

C. Define Network Design Parameters

After initialization of fuzzy, next step is to initialize the network. In this, user has to define the area for network deployment. The number of nodes in the network is also given by the users. Then on the basis of given parameters by the user the network will be created.

D. Calculate Node Parameters

After initializing the network, the next step is to calculate the node parameters or Quality of Service parameters. These parameters are Average Delay, Packet Delivery Ratio, Direct Trust Value and Attack Suspect Ratio. These parameters will be indulged in the process of fuzzy evaluation.

E. Fuzzy Evaluation

In this step the proposed fuzzy system will be evaluated. Here evaluation refers to generate the output after fuzzifying the input membership function of FIS by using defined set of rules. In this step the four of the membership functions or performance parameters will be evaluated to find a specific route to deliver the data to the destination terminal. Most of the suitable nodes will be considered to create a path between source and destination node.

F. Next Hop Selection

In this step the next hop for routing will be selected on the basis of proposed fuzzy inference system.

G. Performance Evaluation

Last step is to evaluate the performance of the proposed work by using various performance parameters. After calculating the performance parameters, a comparison is generated between proposed work and traditional mechanisms.

IV. RESULTS AND DISCUSSION

The proposed system is a combination of fuzzy logics, OLSR and trust evaluation mechanism to secure the data plane in ad hoc networks. This section implies the set of graphs that are obtained after implementing proposed work for the purpose of performance evaluation of the network.

As the proposed work is collaboration of fuzzy logics with trust evaluation, hence the figure below represents the membership functions and model for proposed fuzzy is as below. The figure 2 represents the fuzzy inference model for proposed work which is comprised of four input membership functions and output membership function. Mamdani FIS is used for fuzzy initialization.

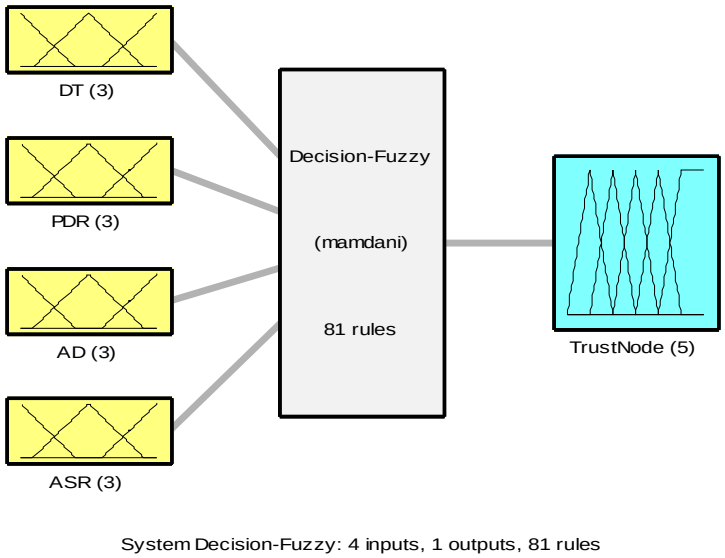


Figure 2 FIS model for PRO-OLSR Technique

The figure 3 depicts the graph for membership function to represent packet delivery ratio. The degree of all membership functions varies from 0 to 1 and poses three states i.e. low, medium and high. The value corresponding to PDR lies between 0 and 100.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VIII, August 2017- Available at www.ijraset.com

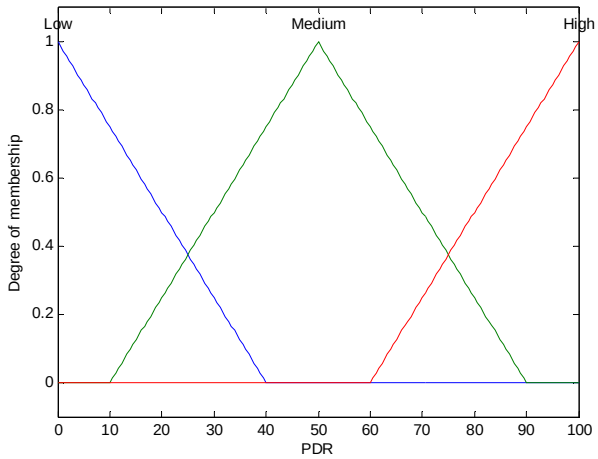


Figure 3 Membership function of Packet Delivery Ratio

Figure 4 represents the average delay as membership function in which the value of AD ranges from -1 to 1 and degree of membership function is 0 to 1.

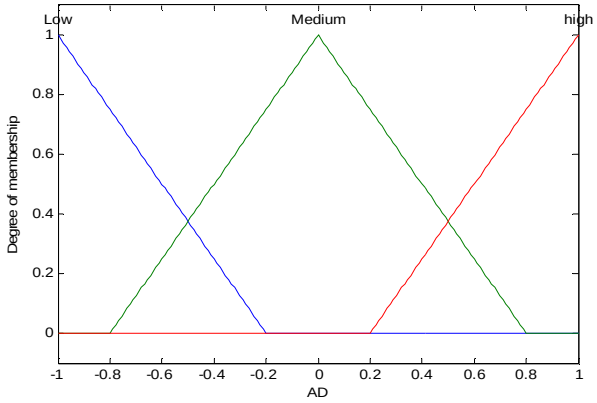


Figure 4 Membership function of Average Delay

Following is the representation of direct trust as membership function to the fuzzy inference system. In this the value of direct trust starts from -1 and ends at 1.

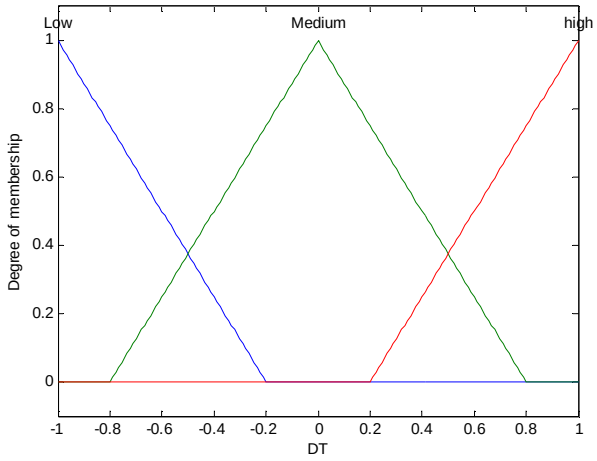


Figure 5 Membership function of Direct Trust

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VIII, August 2017- Available at www.ijraset.com

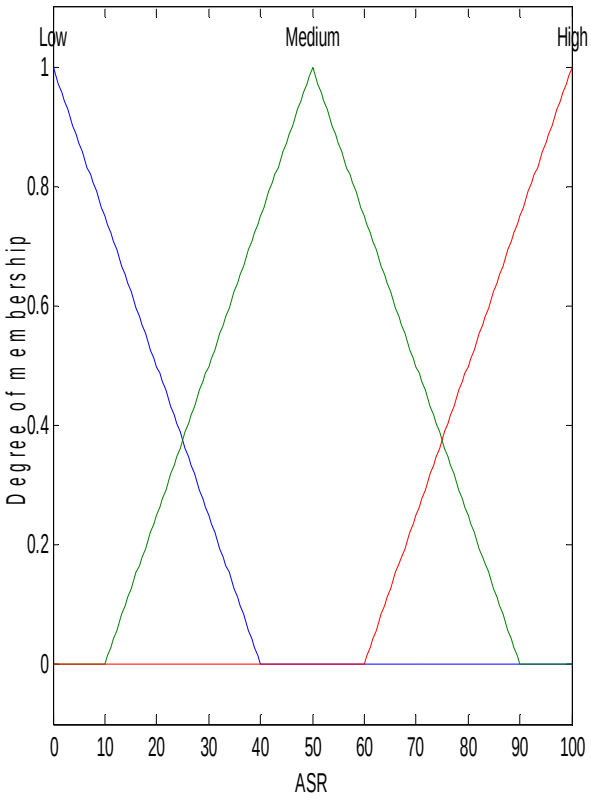


Figure 6 Membership function of Attack Suspected Ratio

Similarly the figure 6 shows the ASR as the membership function.
The figure7 below depicts the node deployment in the network. It is represented that in network there are total 100 nodes exists in the network.

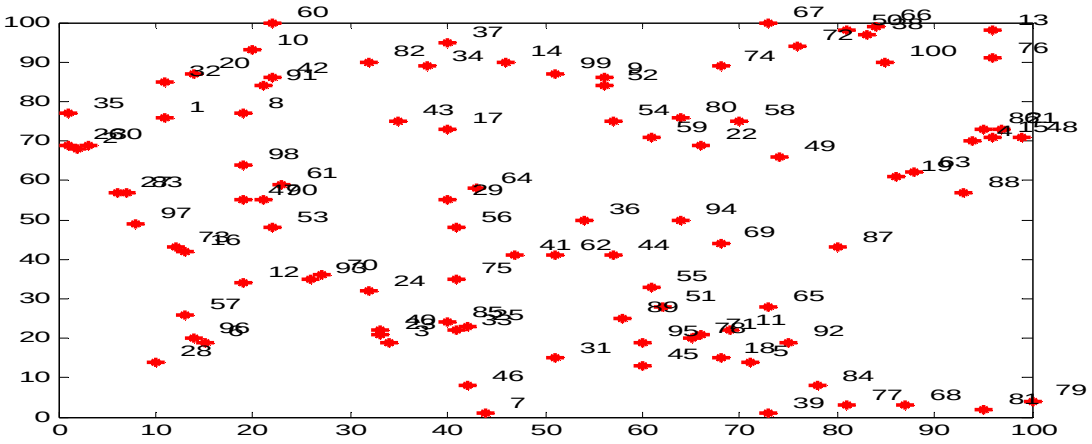


Figure 7 Node deployments in network

The figure 8 renders the route that is created between source and destination node. Here the node 94 is a source node and node 74 act as destination node.

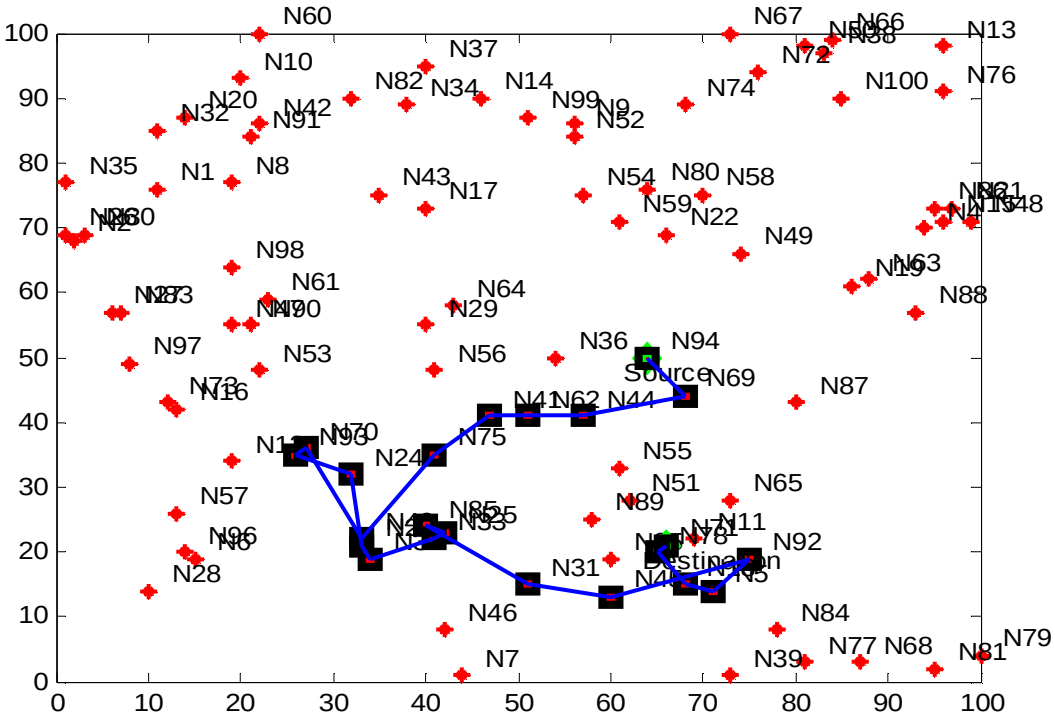


Figure 8 Path creation

The graph in figure 9 depicts the comparison of proposed work (Pro-OLSR) with conventional techniques with respect to PDR of the network. The comparison of proposed work is done with FGT-OLSR, TBS-OLSR, MDI-OLSR and OLSR. From the graph below it is obtained that the PDR of proposed work is evaluated to be 1 whereas the PDR of FGT-OLSR is quite closer to the PDR of proposed work. The value of PDR in case of proposed work remains constant even when the number attacks to the networks is increased. But in other cases the PDR gets declined with an increment in the number attacks to the network. Higher the PDR the more efficient the network.

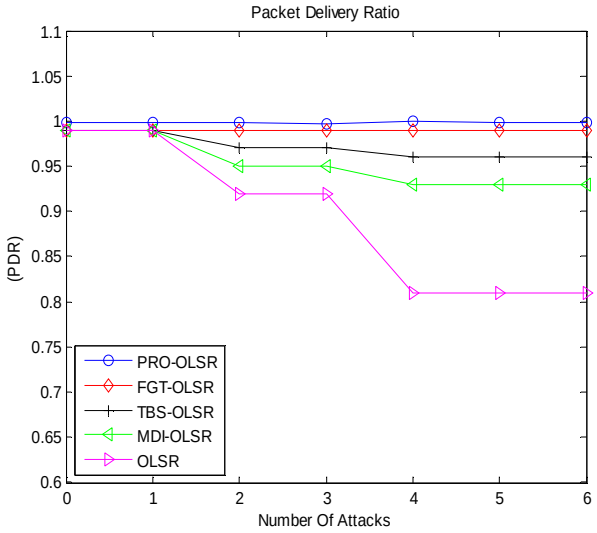


Figure 9 PDR of proposed and conventional mechanisms

The comparison graph of average delay is plotted in figure 10. As per graph the average delay of proposed work is lower as compare to other mechanisms. The average delay of proposed work is near by 0 whereas highest value of average delay is observed in case of FGT-OLSR which is approximately 0.8. The average delay is calculated corresponding to number of attacks in network.

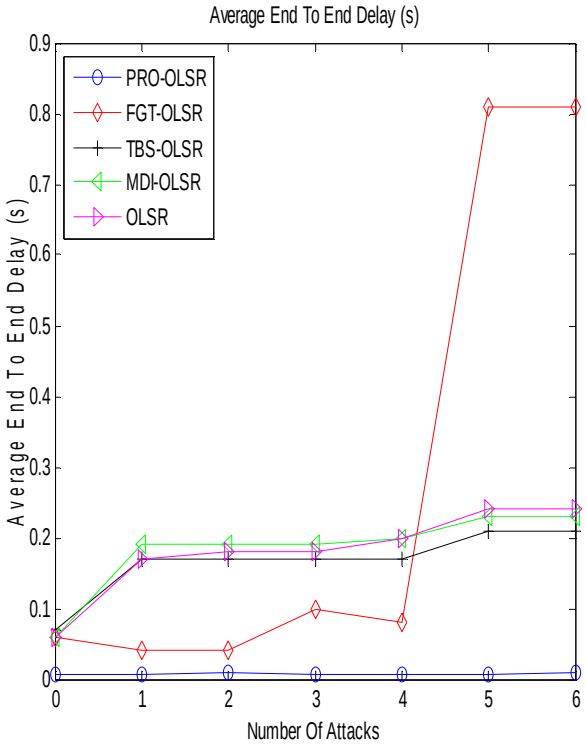


Figure 10 Average Delay of proposed and conventional mechanisms

Control message overhead refers to the measure the number of messages generated by a node with the interval of a second. The graph in figure 11 shows the comparison of control message overhead in case of PRO-OLSR, FGT-OLSR, MDI-OLSR, TBS-OLSR and OLSR. From the given graph it is concluded that the control message overhead of the proposed work is 0.84 which quite higher as compare to the value of message overhead in case of rest of the techniques.

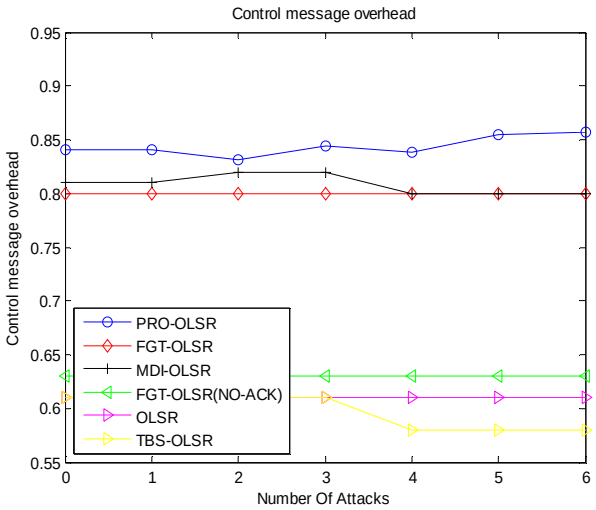


Figure 11 Control Message overhead in proposed and conventional mechanisms

The following figure 12 defines the graph of increased overhead in bytes with respect to proposed and other techniques. The comparison is done among PRO-OLSR, FGT-OLSR and FGT-OLSR (NO ACK). Here FGT-OLSR (NO ACK) refers to FGT based OLSR mechanism to secure data without acknowledgement. The increased overhead in bytes is higher in case of proposed work whereas the FGT-OLSR (NO ACK) suffers from lower value of increased overhead.

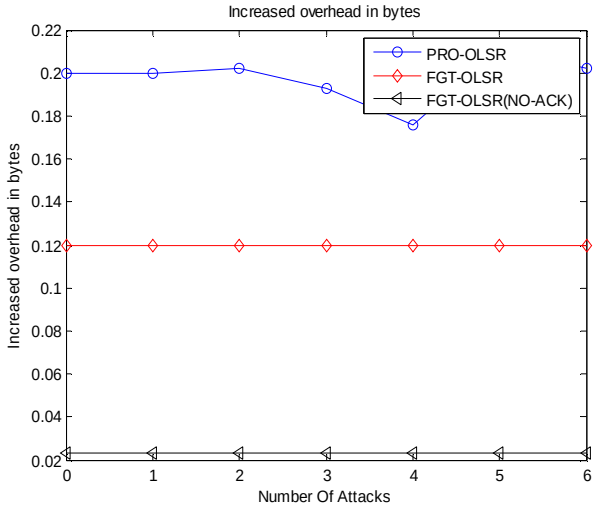


Figure 12 Increased overhead in bytes in proposed and conventional mechanisms

V. CONCLUSION AND FUTURESCOPE

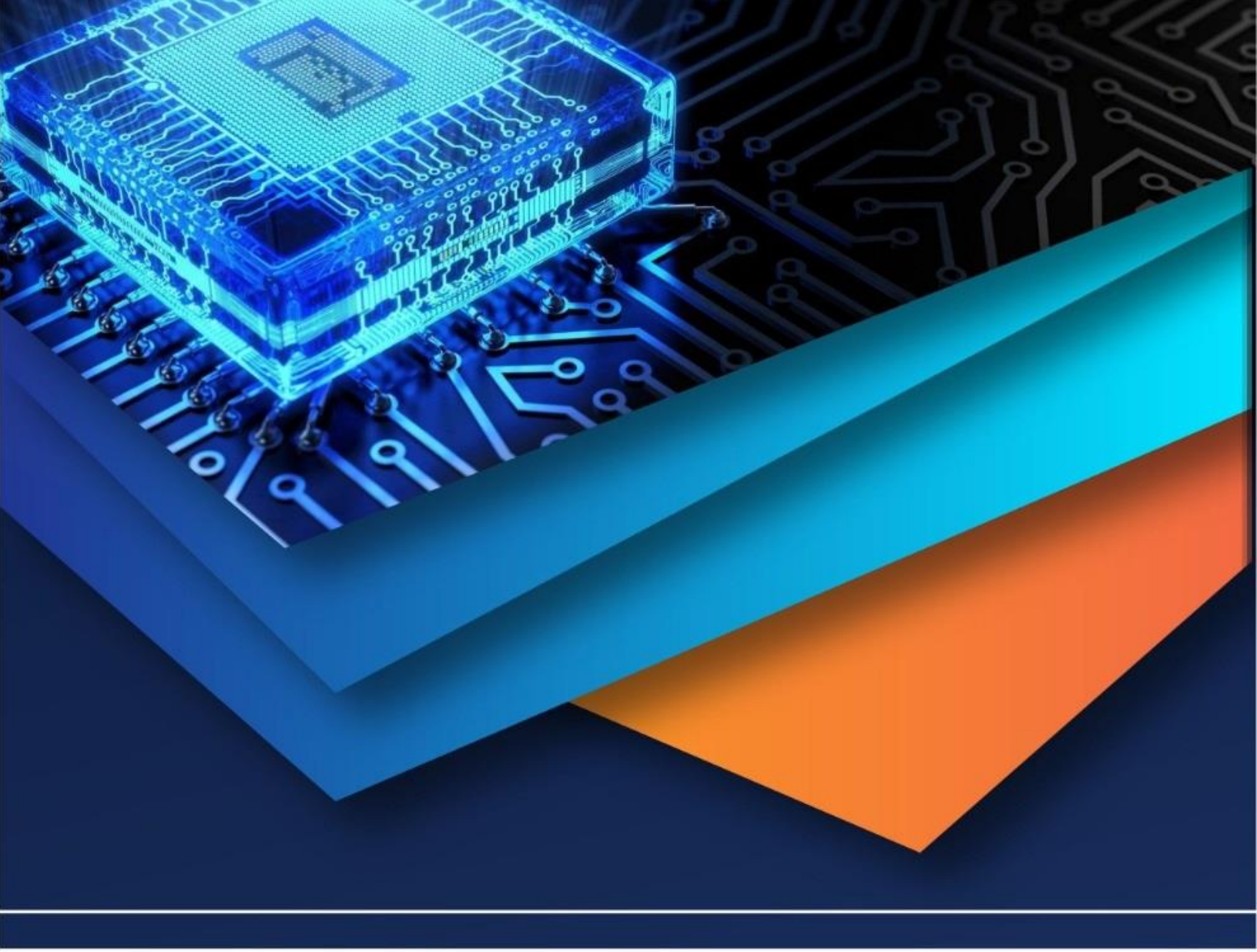
In this study a novel mechanism for securing data plane in ad hoc network is developed. The security is major concern nowadays as most of the data travels over the internet and wireless networks are more prone to security attacks and threats as compare to the wired networking. The proposed technique is a collaboration of Fuzzy Inference System with OLSR security protocol. The vital parameters such as Direct Trust, Packet Delivery Ratio, Average Delay and Attack Suspected ratio are considered for next hop selection and relay node selection. The result section concludes that the PRO-OLSR mechanism of security is more effective as compare to other techniques.

In future further enhancements can be done by increasing the number of parameters for trust evaluation and some advanced security routing protocols can also be considered.

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



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY