IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 11, November 2017

A Trust Oriented Next-Hop Selection in Ad Hoc Network by Using Multiple Fuzzy

Lovepreet Singh Dhillon

Dept. of Computer Science and Engg., Ramgarhia Institute of Engg and Tech, Phagwara, Punjab

Abstract: Security of data is the major concern now days due to the enhancements in the communication technology. The Ad hoc network also suffers from the various security attacks such as black hole attack, gray hole attack, worm hole, sink hole etc. variety of security based routing protocol has been developed by different authors in past and selection of next hop for communication is one the implemented idea but lacks at the point of parameter selection. This study provides an improved method for selecting the next hop selection by enhancing the number of parameters. The Multilevel Fuzzy inference system is applied in order to optimize route of communication. The results are evaluated in terms of throughput, Packet Delivery ratio and Packet Loss. After comparing the proposed and traditional scheme it is concluded that the present scheme is much effective and proficient than the traditional.

Keywords: Ad hoc Networks, Security, Multi-Level Fuzzy Inference System, Packet Loss, Throughput, Packet Delivery Ratio.

I. INTRODUCTION

Ad Hoc networks are kind of wireless networks that have the feature of self-organization and do not have any particular topology for network structure. The ad hoc networks are developed by using the gathered mobile devices specifically for military crisis, emergency etc because in these situations the no framework is not available [3]. Mainly ad hoc networks are of three types i.e. MANETS (Mobile Ad hoc Networks), FANETS (Flying Ad hoc Networks) and VANETS (Vehicular Ad hoc Networks). Ad hoc networks also follow the routing process for establishing the communication between source and destination. The ad hoc network suffers from the issue of data security due to the mobility of the nodes. In this the data plane is more prone to attacks such as black hole, gray hole etc. Various authors have been developed many security related routing protocols to secure the data plane from unwanted access and attacks. Security of data can be maintained by using a trustworthy strategy for selecting the next hop to continue the communication in a safe manner. After having a review to the previous work it is observed that, traditionally, only one parameter was considered for next hop selection, which did not have an impact on network in terms of generating the optimal path. In this the whole paper is organized as section II represents the problem that is a

Motivation for this study, section III depicts the framework and idea of proposed work that is comprised of multilevel fuzzy system for next hop selection. Various parameters such as average delay, packet delivery ratio, direct trust is considered for fuzzy system1 and set of parameters for fuzzy system2 is energy, distance and throughput. Section IV interprets the results that are observed from proposed implementation. And last section concludes the study along with the future work.

II. PROBLEM FORMULATION

Routing is the process of selecting best paths in a network. In the past, the term routing was also used to mean forwarding network traffic among networks. However this latter function is much better described as simply forwarding. Routing is performed for many kinds of networks, including the telephone network (circuit switching), electronic data networks (such as the Internet), and transportation networks. The routing can be achieved by using various routing techniques. There are many routing techniques developed that can help to generate the efficient path for communication. But all the traditional routing techniques select the route on the basis of shortest distance. Only single parameter is considered by the traditional routing techniques that is shortest path finding. In these techniques first of all the possible routes are generated from source node to sink node and then the path with the shortest distance is selected as an efficient path for routing. The lacking side of these techniques is that these algorithms are not that efficient. Hence there is a need to develop such a system or technique which can overcome the shortcomings of previous routing algorithms. In order to develop such a system some other parameters can also be taken into consideration for the optimized route selection.

III. PROPOSED WORK

As routing differs from conventional routing in wireless sensor networks so an approach needs to be introduced which will be better than the earlier routing algorithms. The problem which occurs due to traditional routing algorithms is that

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 11, November 2017

they were not capable to generate the optimized route to any destination. So in this work we developed a new approach which has the capability to generate the optimal path for data transmission. In our work we have used multi level fuzzy logics in order to optimize and secure routing. Fuzzy 1 considers the parameters like Average delay (AD), Direct Trust (DT) and PDR (Packet Delivery Ratio) in order to generate a decision regarding the node selection on the basis of security of the route and fuzzy 2 will consider the parameters like Distance, Energy and throughput in order to select the nodes for route creation. Then the fusion will be implemented on the obtained results from the two layers of fuzzy network. On the basis of results of fusion the selection of next hop will be done to route the data from source node to destination node.

Proposed work has divided into two decision fuzzy systems. Both fuzzy systems have taken input parameters and produce a trust node as a output. The steps taken for the evaluation has described below.

1. Initially two different fuzzy systems termed as fuzzy 1 and fuzzy 2 have designed to take decision based on the input parameters.
2. Fuzzy decision system 1 takes three different inputs and produced one output. So in this step, different input and output variables will be defined. The three input parameters are Average Delay, Packet Delivery Ratio and Direct trust on the basis of which an output will be generated. Similarly for fuzzy decision system 2 whose inputs parameters are Energy, Distance and Throughput. Based upon these three input values, trust value 2 will be acquired.
3. In this step, two different trust values such as trust value 1 and trust value 2 are equipped.
4. Then fusion of both values trust value 1 and trust value 2 are performed in order to select a hop for the transmission of data from source to the destination node.
5. Lastly, hop will be selected using which data will be forwarded to the nest node in view of completion of transmission.

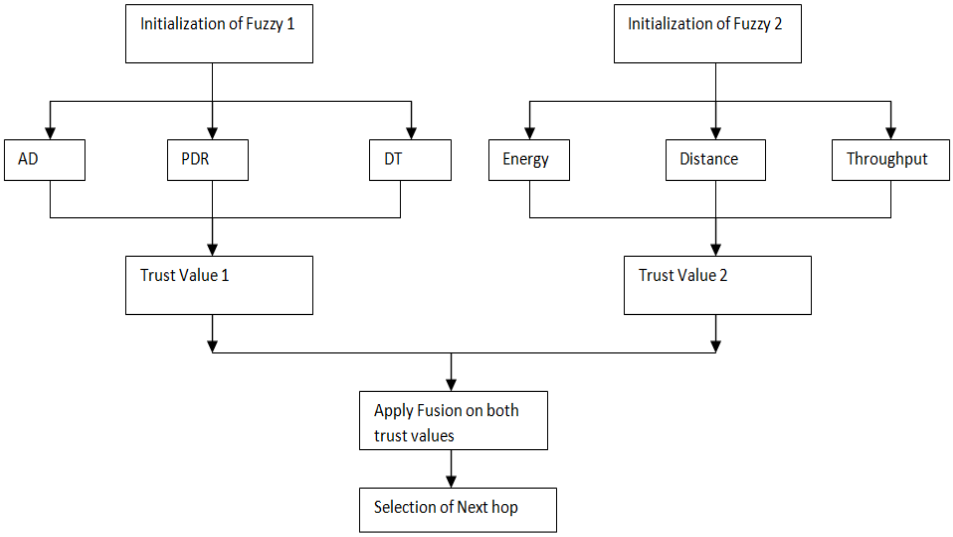


Figure 1 Block Diagram of Proposed Work

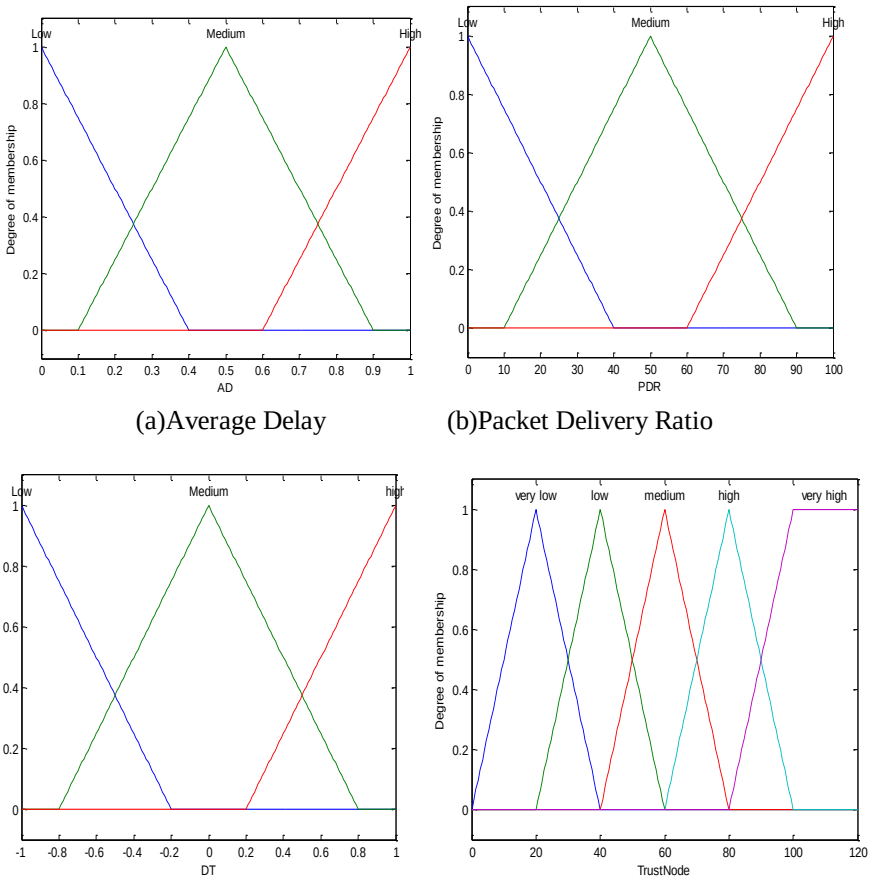
IV. RESULTS

This section describes the experimental analysis acquired from the proposed technique. The proposed technique employed two fizzy decision support systems where different inputs have given to the system. Fuzzy system takes membership functions of the input and output variables which are described as:

The figure 2(a) depicts the membership function of average delay parameter which is first and foremost input variable of the first decision support system. Average Delay is the parameter whose membership functions are divided into three sections such as “Low”, “Medium” and “High”. The range varies from 0 to 1 and each function is varying accordingly.

The figure 2(b) evaluates the membership function of Packet Delivery Ratio variable. The variable defined for fuzzy system is PDR whose membership functions are “Low”, “Medium” and “High”. The range is same for all the membership functions with varied range of different membership functions. Figure 2(c) represents the third input variable of fuzzy decision system 1 termed as Direct Trust and figure 2 (d) shows the trust node membership function. Based on these three membership functions, an output trust node will be acquired which membership function is shown in the above figure. The output variable has five different membership functions such as “Very Low”, “Low”, “Medium”, “High” and “Very High”. These values allow system to select next hop in the communication.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 11, November 2017



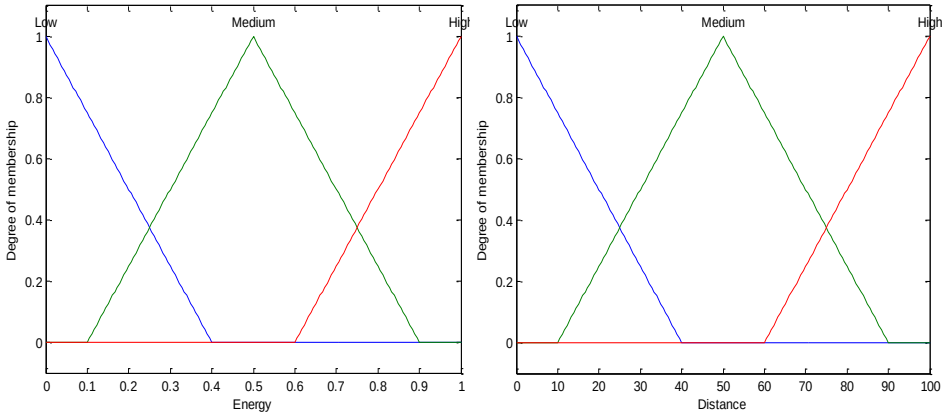
(a)Average Delay (b)Packet Delivery Ratio

(c)Direct Trust (d) Trust Node

Figure 2 Membership functions of fuzzy System 1

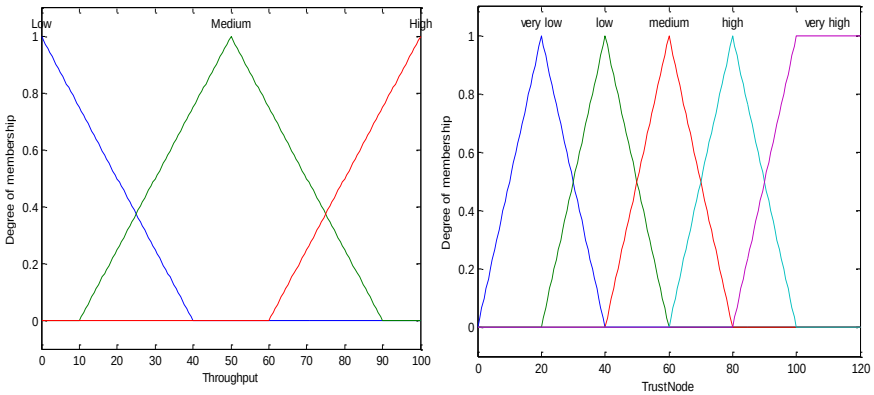
Now figure 3(a),(b),(c) and (d), depicts the input and output membership function for fuzzy system 2 which takes three input variables and produces trust node output. All the input variables have three membership functions such as “Low”, “Medium” and “High” ranges from 0 to 1. The three parameters taken by fuzzy system 2 are Energy, Distance and throughput.

The figure 3(d) depicts the output variable Trust node whose membership functions are “Very Low”, “Low”, “Medium”, “High” and “Very High”. The range varies from 0 to 1. Each membership function is specified within a range and if any node’s value lies in that range then the trust value of that node will be evaluated and shown accordingly.



(a)Energy (b) Distance

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 11, November 2017



(c)Throughput (d) Trust node

Figure 3 Membership functions of fuzzy System 1

Figure 4 shows deployment of nodes in the network. There are total 60 nodes in the network deployed in the area. The area defined for the deployment is 100 by 100. All the nodes are deployed in that region only. The symbols are shown in red color and text has written with the symbol shows the node number in the network.

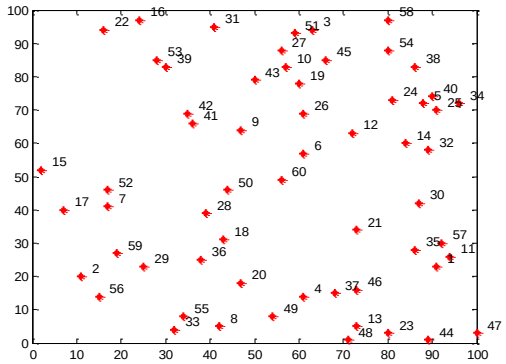


Figure 4 Nodes Deployment

The figure 5 depicts the route establishment between the numbers of nodes deployed in the network. Node number 32 is considered as a source node and 31 node no. is considered as a destination node. Node with green color is source and destination for the transmission. The packet has been transmitted from the respective source through another nodes i.e. relay nodes and reached to the destination node.

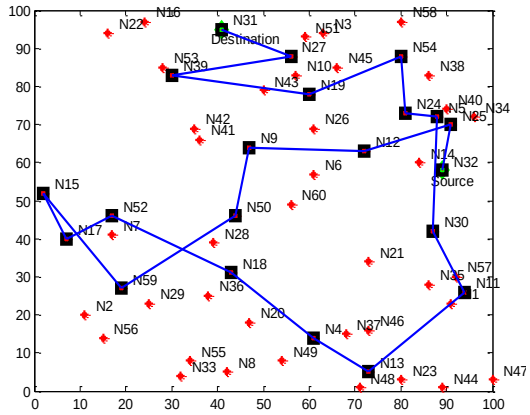


Figure 5 Route establishments between nodes

Figure 6 and 7 shows the comparison between traditional and proposed approach in view of different performance parameters such as Throughput, Packet Loss and Packet Delivery Ratio. From the results evaluated, it has been shown that proposed technique outperforms the traditional technique where high throughput, high packet delivery ratio, less packet loss and less delay has achieved.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 11, November 2017

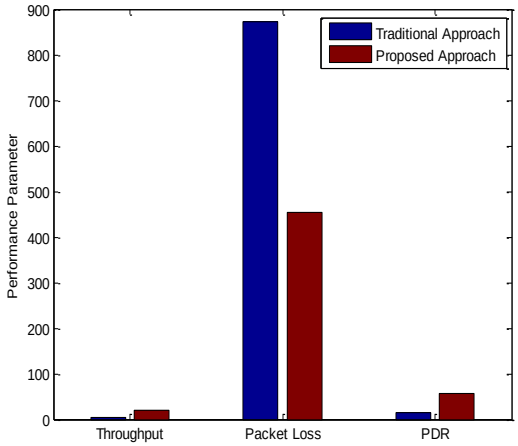


Figure 6 comparisons between traditional and proposed techniques in terms of performance parameters

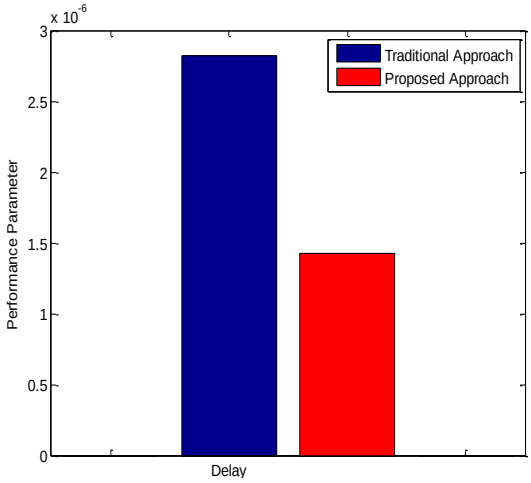


Figure 7 comparisons between traditional and proposed techniques in terms of delay

V. CONCLUSION

The transmission of packets has done using the intermediate node and which node has to be selected for the transmission is dependent on the trust of that particular node. The proposed technique extended this work by introducing multi-level fuzzy logics. In this parameters have divided into two fuzzy systems and then output has produced. The experimental analysis has performed in order to evaluate the performance of the proposed technique. Furthermore, proposed technique is compared with the traditional technique for the efficiency evaluation. From the results acquired, it has been concluded that proposed technique outperforms the traditional technique in terms of individual performance parameters such as PDR, Packet loss and Throughput. The proposed technique achieved high throughput i.e. 19.033 whereas traditional technique achieved 5.0667 throughout i.e. less than proposed approach. High Packet delivery ratio has achieved using both techniques are 55.7617 and 14.8438 for traditional and proposed technique respectively. Consequently, high packets have delivered at the destination using proposed technique. Moreover, Less Delay as well as packet loss is acquired in the proposed technique in comparison with traditional technique. On the whole proposed technique is effective, efficient and secure.

In future, the proposed technique can be improved by extending the number of performance parameters and complexity of the proposed technique can be reduced. Moreover, soft computing methods can be introduced in the proposed method for the evolution of trust node and chosen as a next hop for the transmission.

REFERENCES

[1] Alex Hinds, "A Review of Routing Protocols for Mobile Ad-Hoc Networks (MANET)",IJIET, Vol 3, Pp 1-5, 2013
[2] 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
[3] 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
[4] 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
[5] Charu Wahi, "Mobile Ad Hoc Network Routing Protocols: A Comparative Study", IJASUC, Vol 3, Pp 21-31,2012
[6] Dan-Yang Qin ,"An Effective Survivable Routing Strategy for MANET", 2011

[7] D. Chasaki et al, "Attacks and defences in the data plane of networks," IEEE Trans. Dependable Secure Comput., vol. 9, no. 6, pp. 798–810, Nov. 2012.
[8] 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.
[9] 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.
[10] 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
[11] Lidong Zhou et al, "Securing Ad Hoc Networks", IEEE, Pp 1-12, November 1999
[12] Muhammad Imran, "Analysis of Detection Features for Wormhole Attacks in MANETs", Science Direct Procedia Computer Science, Pp: 384-390, 2015.
[13] 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.
[14] Petteri Kuosmanen, "Classification of Ad Hoc Routing Protocols"
[15] Pooja Pilankar et al, "Trust based security in manet", IJRET: International Journal of Research in Engineering and Technology, 2319-1163, Vol. 05, No. 02 , Pp. 12-19, Feb 2016
[16] Prosenjit Bose, "Routing with Guaranteed Delivery in Ad Hoc Wireless Networks", Wireless Network, Vol 7, Pp 609-616, 2001
[17] 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
[18] 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
[19] 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
[20] 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
[21] Sayan Banerjee, "A Review on Different Intrusion Detection Systems for MANET and its Vulnerabilities", IEEE, 2015
[22] 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
[23] 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
[24] Xiaocong Jin, "TIGHT: A Geographic Routing Protocol for Cognitive Radio Mobile Ad Hoc Networks", IEEE, Vol 13, Pp 4670-4681, 2014
[25] 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
[26] Shirina Samreen et al, "Trust based Data Plane Security Mechanism for a Mobile Ad hoc Network through Acknowledgement Reports", International Journal of Computer Applications, Vol. 129, No. 6, Pp. 6-13, November 2015.
[27] Shuaishuai Tan et al, "Trust based routing mechanism for securing OSLR-based MANET ", ELSEVIER, Adhoc Networks, March 2015
[28] Tameem Eissa et al, "Trust-Based Routing Mechanism in MANET: Design and Implementation", SPRINGER, Mobile Netw Appl, Pp 1-12, June 2011
[29] X. Anita, et al, "Fuzzy-Based Trust Prediction Model for Routing in WSNs", HINDAWI, Volume 2014 (2014), Pp 1-11, July 2014
[30] Z. Wei et al, "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