Journal of Information Systems Engineering and Management
2025, 10(14s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Simulation Based Fuzzy Model for Mobile Ad-hoc Network Security

Ayesha Mujawar[1] ,Riyajuddin Mujawar[2], Pratibha Deshmukh[3] ,Shubhangi Mahadik[4] ,Jyoti Kharade[5] Santoshrao Arun Khawale[6]
[1,2]*Bharati Vidyapeeth, Institute of Management, Sangli , Maharashtra, India*
[3,4,5]*Bharati Vidyapeeth's, Institute of Management and Information Technology, Navi Mumbai, Maharashtra, India*
[6]*Bharati Vidyapeeth's, Bharati Kala Mahavidya. Pune, Maharashtra, India*
Email: ayeshamulla78@gmail.com, riyajuddin1676@gmail.com, pratibha.deshmukh@bharatividyapeeth.edu, shubhangipati@gmail.com Jyoti.kharade@bharatividyapeeth.edu, santoshraokhawale@gmail.com

ARTICLE INFO

Received: 18 Nov 2024
Revised: 05 Jan 2025
Accepted: 18 Jan 2025

ABSTRACT

Complex nature of an ad-hoc network due to mobile nodes creates different types of problems for security in such networks. It is very difficult task to analyze such type of network for proper decision making to work safely in such type of environment. Therefore, in this study, simulation has been carried out using Ns-2.34 simulator and the obtained result has been analyzed with and without using fuzzy approach for correct analysis. The designed simulated tool/model shows analysis of security parameters to obtain safe fuzzy speed and safe mediator for proper decision making while designing and working with such type of networks.

Keywords: ad-hoc, mobile nodes, simulation, fuzzy, security parameters.

INTRODUCTION

To monitor the working as well as functionality of both wired as well as wireless networks, varieties of tools are available nowadays. Few of them are traffic monitoring tools, bandwidth monitoring tools, scanners, sniffers, analyzers, password crackers etc. These all tools are designed for a specific (working) purpose only.

An ad-hoc network contains mobile nodes. Due to dynamic nature of such nodes, it is difficult to predict the working, state of such network easily. Therefore, huge complexity exists in an ad-hoc network due to dynamic nature of mobile nodes. So here research has been carried out by considering few important network security parameters. Along with it few network performance parameters are also analyzed. For simulation variety of simulators are available nowadays like Ns-2, Ns-3, OPNET etc. But Ns-2 is widely used simulator which works well for both wired as well as wireless networks. Here Ns-2 simulator has been used for simulation purpose.

It is very difficult to simulate the scenario for an ad-hoc network due to its complex structure. Therefore before moving towards the actual design, simulation for such type of network, the designed tool/model is helpful to decide safe or secure speed as well as mediator to maximize throughput of such type of network. This designed tool/model is very simple, easy to handle and understand.

ANALYSIS METHODOLOGY

The analysis has been done by considering few important network security parameters like speed, packet drop attack analysis, energy consumption analysis, transmission time analysis with network performance parameters.

The designed tool/model follows the following steps for an ad-hoc network analysis-

1. Start
2. Decide and Choose the parameter of Analysis
3. Select the node count for design and analysis
4. Get design of the network using (Ns-2) simulator
5. Display Ns-2 data without fuzzy approach
6. Apply Fuzzy approach for data through FIS and again obtain Ns-2 data with fuzzy approach.
7. Get Safe Fuzzy Mediator as well as Safe Fuzzy Speed for the selected scenario.
8. Stop

Developed Fuzzy Model For Network Security Parameter Analysis:

The model is developed using MATLAB. Here the data used for analysis is obtained by using Network Simulator i.e. Ns-2. This developed tool provides analysis of Packet Drop Attack, Processing Time, Energy Consumption and Bandwidth Utilization as important network security parameters.

i. Packet Drop Attack Analysis

Packet drop is one of the passive attacks which may occur with more frequency in wireless networks like ad-hoc network. It is very harmful for such type of network. The designed model/tool shows analysis of Packet drop attack with and without fuzzy approach using MATLAB and Ns-2 Simulator. Fig.1 shows designed tool/model for security parameter analysis.

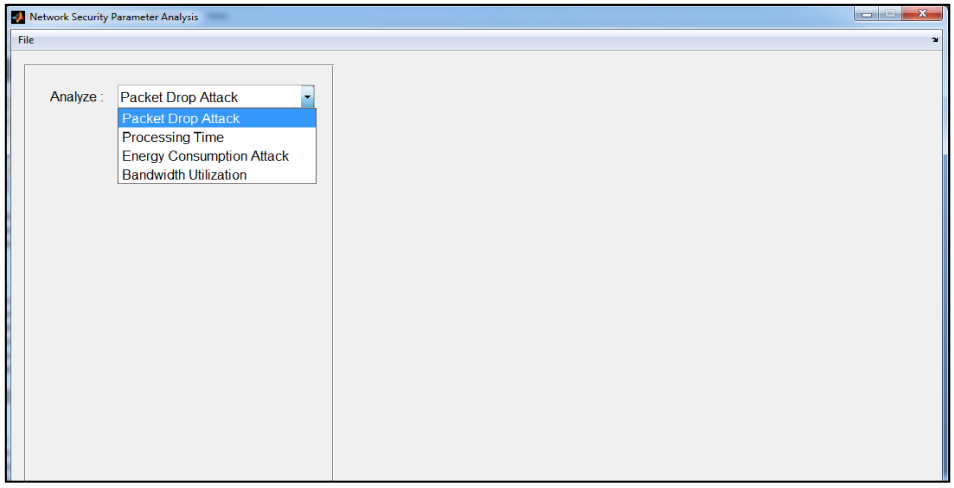

Figure 1. Fuzzy Security Tool

Following Fig.2 shows Ns-2 database of packet drop analysis for selected case without fuzzy approach. Here the user can choose any case for analysis. After that user can see its design along with the number of sources, mediators and destination count for. In right panel user can see the simulated analyzed data for different possibilities of mobility.

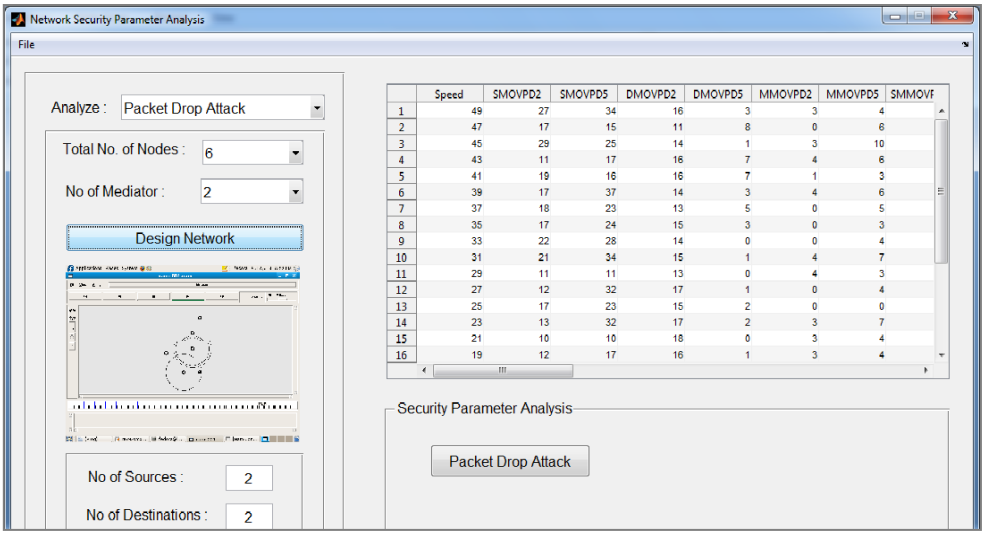

Figure 2. Packet Drop Analysis without fuzzy approach

In this analysis, speed and mobility are major factors under consideration. After clicking on Packet Drop Attack button, user gets the fuzzified output of Speed, Packet Drop and Safe mediator as shown in Fig. 3. Here throughput is considered as one of the network performance parameters.

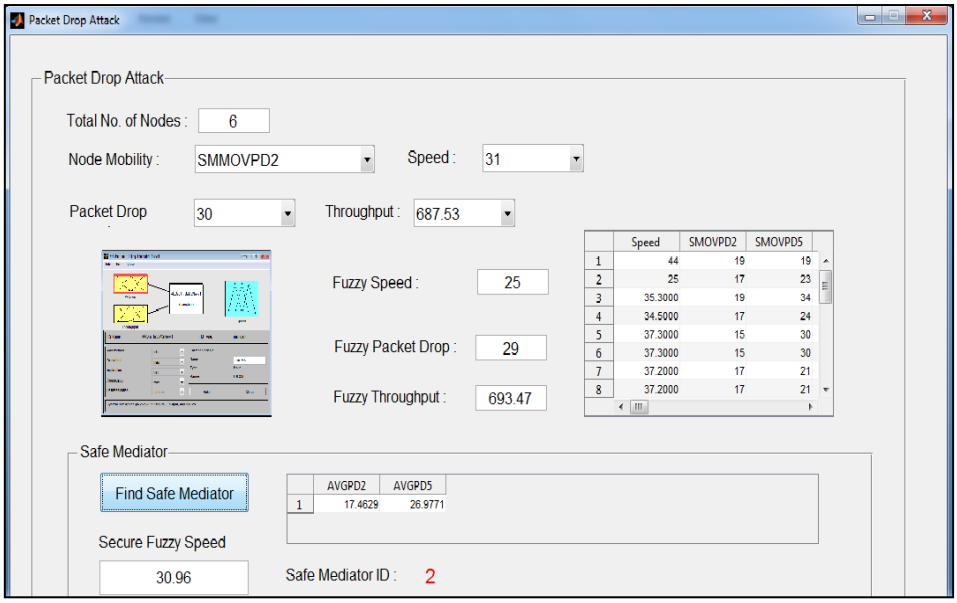

Figure 3 Packet Drop Analysis with Fuzzy approach

The flow of experiment is as shown in Figure 4 –

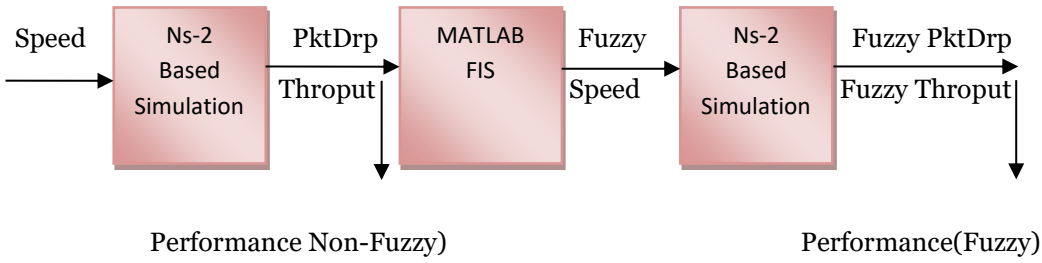

Figure 4. Experiment Flow

Following Table 1 shows the sample data analyzed by using Fuzzy Security Model or Tool for packet drop attack analysis.

Table 1: Sample Data For Packet Drop Attack Analysis

Total No. Of Nodes	Mobility	Speed	Packt Drop	Throughput	Fuzzy Speed	Fuzzy Packet Drop	Fuzzy Throughput
6	DMOVPD2	41	16	506.33	25	15	506.24
11	SMMOVPD5	47	97	680.25	37	60	681.25
14	SMMOVPD7	35	81	536.07	25	64	543.14
25	DMOVPD12	47	211	591	37.3	173	623.9

Figure 5 and 6 shows the graphical representation of sample data analyzed by using developed model with and without fuzzy approach for packet drop attack analysis.

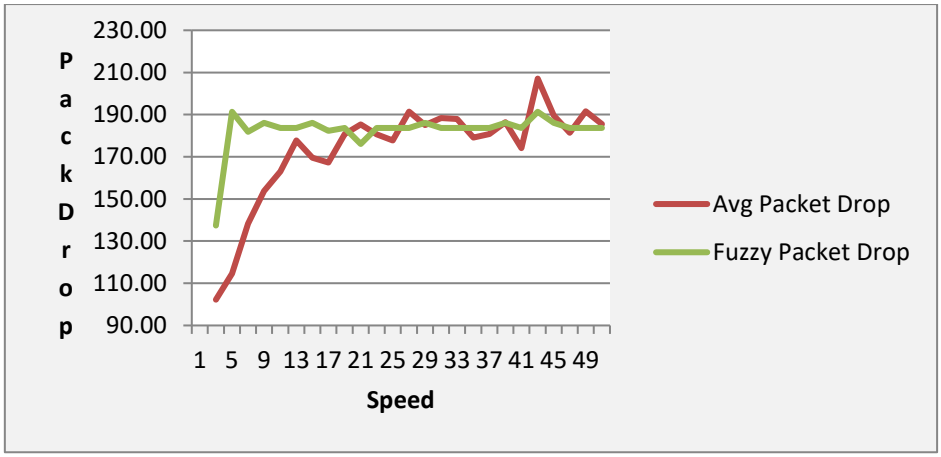

Figure 5. Speed And PackDrop Analysis

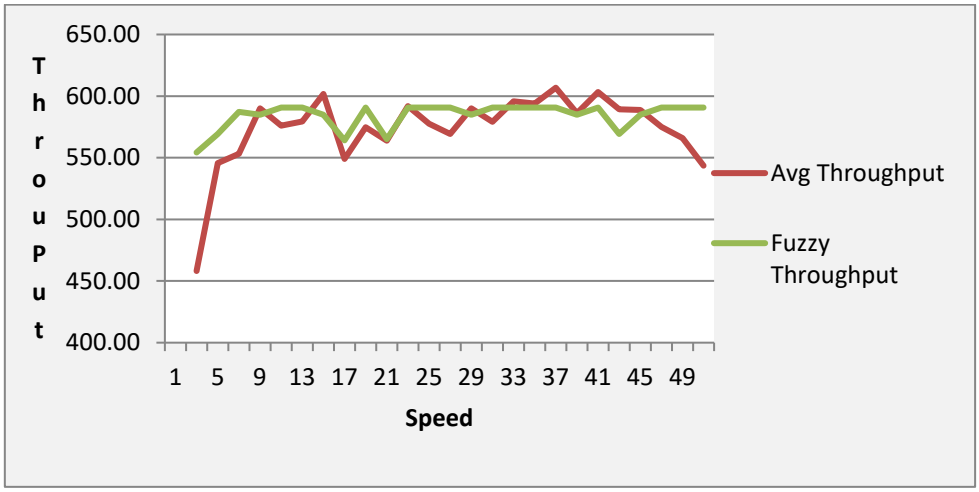

Figure 6. Speed And Throughput Analysis

ii. Processing Time

MANET's dynamic topology effect on processing time of a packet which results as either more or less delay which effects on the performance of the network. Therefore, it is important to maintain it properly. Here the analysis of processing time or transmission time required for a packet has been analyzed by using the same method as above. Here end to end delay is considered as one of the network performance parameters.

Fig. 7 and 8 shows sample output for processing time with and without fuzzy approach.

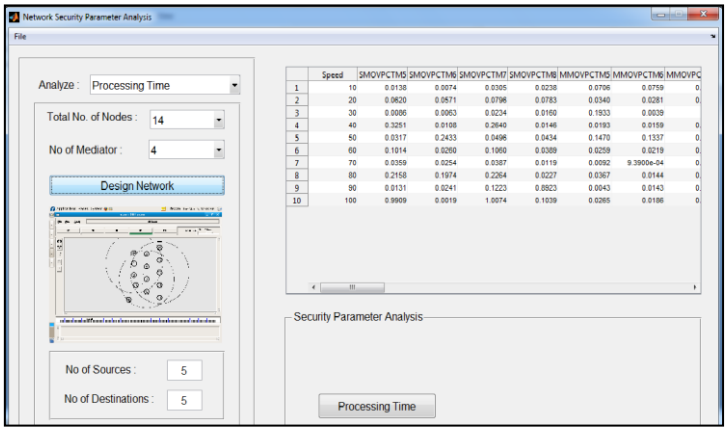

Figure.7 Processing Time Database without fuzzy approach

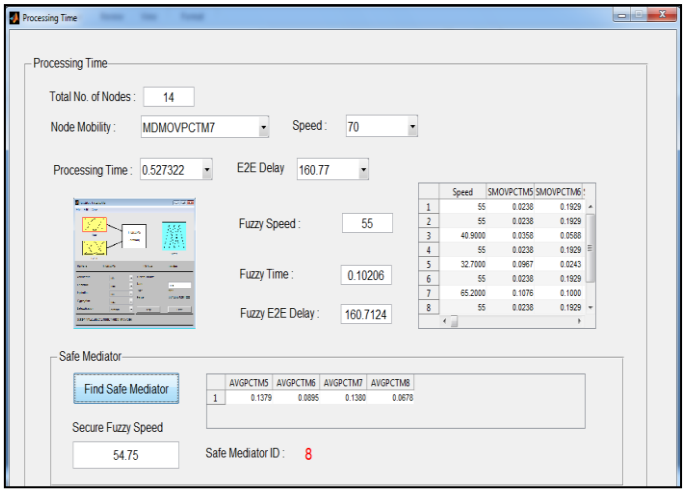

Figure.8 Processing Time Database with fuzzy approach

Similarly following Table 2 shows the sample data analyzed with and without fuzzy approach for processing time analysis.

Table 2: Sample Data For Processing Time Analysis

Total No. Of Nodes	Mobility	Speed	Proc. Time	End to End Delay	Fuzzy Speed	Fuzzy Proc Time	Fuzzy End to End Delay
11	SMMOVPCTM6	80	0.0721	232.86	55	0.03729	225.06
11	DMOVPCTM4	50	0.0271	230.93	32.68	0.0016	225.06
14	SMOVPCTM5	70	0.036	160.77	55	0.02375	160.71
25	SMOVPCTM10	50	0.4636	242.3	32.71	0.10363	240.13

iii. Energy Consumption Attack

Mobile nodes have limited resources like energy, bandwidth as they are battery powered nodes. Therefore, it leads to different types of vulnerabilities. An active attack may spend energy showing misbehavior in the network. Whereas to save energy showing lack of cooperation causes selfish attack. Therefore, maintaining proper energy to keep safe networking environment is one of the difficult tasks while working with such types of networks. Here Packet Delivery Ratio is considered as one of the network performance parameters.

Following Fig. 9 and 10 shows sample output for energy consumption attack analysis.

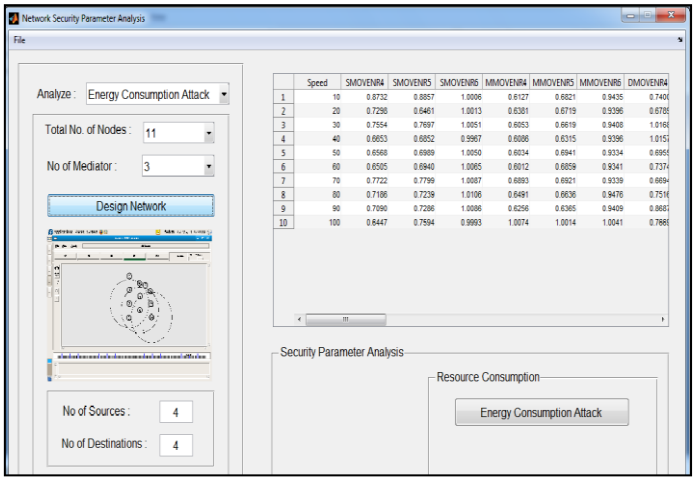

Figure 9 Energy Consumption Database without fuzzy

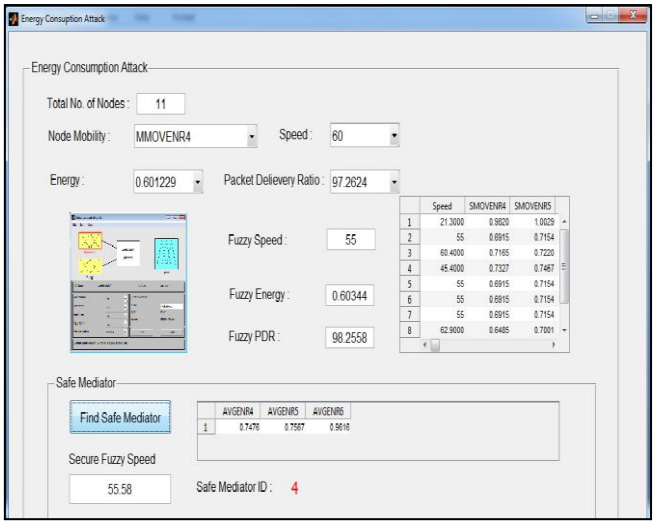

Figure 10 Energy Consumption Database with fuzzy approach

Table 3 shows sample data obtained For Energy Consumption Attack Analysis with and without fuzzy approach.

Table 3: Sample Data For Energy Consumption Attack Analysis

Total No. Of Nodes	Mobility	Speed	Energy	Packet Delivery Ratio	Fuzzy Speed	Fuzzy energy	Fuzzy Packet Delivery Ratio
11	MMOVENR6	90	0.9409	97.5979	55	0.9365	98.256
14	DMOVENR6	80	1.0332	98.969	55	1.0248	99.068

Similarly, Bandwidth Utilization parameter is analyzed. Here the simulator used for Analysis is Ns-2 (Network Simulator All-in-one 2.34). Variation in number of nodes as well as different possibilities of mobility are considered. Following fig. 11 shows sample scenario using Network Simulator (Ns-2).

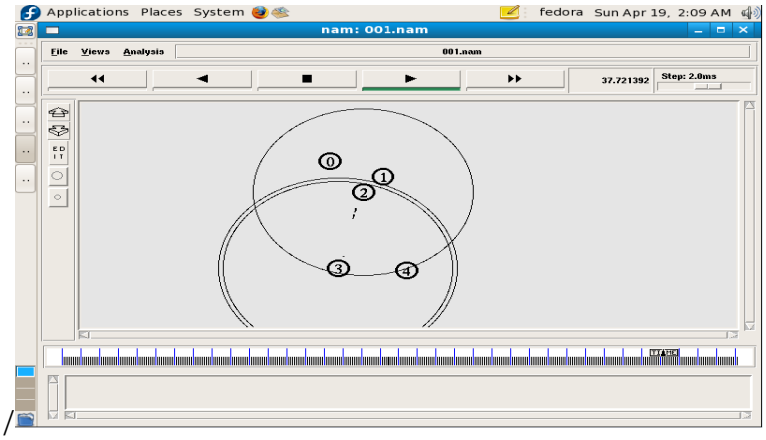

Figure 11. Ns-2 simulation Sample scenario

CONCLUSION

Fuzzy based Security model or tool designed for Ad-Hoc network is useful for security of network like ad-hoc network. The Developed model works as one of the decision-making systems for the network user. This Tool provides fuzzy based safe or good mediator as well as safe fuzzy speed for maintaining the security of the system.

The developed tool helps for a normal user to design its own network scenario for mobile ad-hoc network by following security principle. It helps the user during initial phase of actual network design and implementation.

REFERENCES

[1] Sanyog Dubey et. al, "Implementation of Matlab Simulink Approach in shunt active power filters to minimize the harmonics" International Journal of Advanced Engineering Research. Studies/III/II/Jan-March, 2014/28-35 e-ISSSN 2249-8974

[2] Kirtiwant Ghadle et. al. "Travelling Salesman problem with MATLAB programming" International Journal of Advances in Applied Mathematics and Mechanics 2(2) (2015) 258-266 (ISSN: 2347-2529)

[3] Varun Jadhav et. al, "Fault Simulations on Distribution Network through a GUI", International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering, ISSN (Online) 2321-2004, (Print) 2321-5526 Vol.4 Issue 2 April 2016, pp.-11-16.

[4] Lucass Krasusla "MATLAB based applications for Image Processing and Image Quality Assessment Part II Experimental Results

[5] Shailesh Thakare, "Introducing Fuzzy Logic in Network Intrusion Detection System" International Journal of Advanced Research in Computer Science, Volume 3, No.3, May-June 2012 ISSN No. 0976-5697 pp.810-815

[6] Raquib Buksh "MATLAB based Image Editing and Color Detection" International Journal of Scientific And Research Publications, Volume 4. Issue 1, January 2014 ISSN: 2250-3153

[7] Preeti Wadhwa, "A Survey on Co-Simulation Tools Based on MATLAB" International Journal of Innovative Research in Computer and Communication Engineering" Vol. 5, Issue 2, February 2017 ISSN(Online): 2320-9801 ISSN(Print) : 2320-9798 pp. 1682-1689

[8] Anjali Vasu, "Review of Digital System Access Remotely for FPGA Lab" International Journal of Advanced Research, Research Review Article (2015), Vol. 3, Issue 5 pp.575-579

[9] Gobithasan Rudrusamy, "Fuzzy Based Diagnostics System for Identifying Network Traffic Flow Anamalies" Network Research Group, School of Computer Sciences, Malaysia.

[10] A. Toraralba "A collection of Fuzzy Logic-Based Tools for the automated Design, Modelling and Test of Analog Circuits"

[11] Aiyeshabi S. Mulla (Ayesha Mujawar),"Design And Development Of Fuzzy Toolbox For Network Security", A Thesis Submitted to Shivaji University , Kolhapur in 2018.

[12] R. Padmalatha "A Novel Algorithm for Improving the End-to-End ActivePacket Loss Measurements in Computer Networks" International Journal of Computer Applications (0975 – 8887) Volume 6– No.1, September 2010

[13] A.T.I Fayeez, "Throughput Analysis Of Energy Aware Routing Protocol For Real-Time Load Distribution In Wireless Sensor Network (Wsn)" IJRET: International Journal of Research in Engineering and Technology eISSN: 2319-1163 | pISSN: 2321-7308 Volume: 02 Issue: 11 | Nov-2013

[14] G. Usha Devi, "Resource Reservation using PRTMAC Protocol in MANET" IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501 Vol.2, No.3, June 2012

[15] Sachin Kumar Gupta "Performance Metric Comparison Of Aodv And Dsdv Routing Protocols In Manets Using Ns-2" IJRRAS 7 (3) June 2011