International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 12, December 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

AN EFFICIENT FUZZY BASED INTRUSION DETECTION SYSTEM IN MANET

D. Nethra Pingala Suthishni[1], Dr. G. P. Ramesh Kumar[2]

[1]*Department of Computer Science,Sri Ramakrishna College of Arts & Science, (India)*

[2]*Department of Computer Science, Government Arts College, Kulithalai,(India)*

ABSTRACT

Over the past few years due to the amelioration in wireless technology, Mobile Ad hoc Networks (MANETs) play a major role for communication in many aspects due to its infrastructure less, dynamic topologic, self-organised and open network. Speaking in terms of security in MANET, these networks are more vulnerable to attacks than the traditional methods. For this reason, Intrusion Detection Systems (IDS) are used as the foundation in these networks. Various IDSs have been evolved by different researchers to handle the uncertainty of MANETs. The proposed work insists on an efficient fuzzy based intrusion detection system in Mobile Ad hoc Networks. The investigations and assessments of the proposed IDS are performed with the diverse intrusion detection dataset. The system shows higher accuracy in detecting the packet dropping nodes and collaborative attacks in MANET using Dynamic Source Routing (DSR) protocol. The outcome of the proposed system enhances the various performance metrics such as throughput, packet delivery ratio, jitter, end to end delay, routing overload and control overhead. Simulation of this environment is done using Network Simulator (NS2).

Keywords:Attacks, DSR protocol, Fuzzy Algorithm, Intrusion Detection System (IDS), MANET.

I.INTRODUCTION

MANETs are dynamic in nature and hence the nodes communicate freely within the network without any centralized control. Due to this compliance, MANETs are used in military applications, business environments, game theory, crisis management and many more. With the help of routing protocols such as DSR, the mobile nodes communicate with each other among the network efficiently. Some characteristics of MANETs such as communication via wireless links, resource constraints (bandwidth and battery power), cooperativeness between the nodes and dynamic topology make it more vulnerable to attacks [1] [2]. Due to the various characteristics of MANET, IDSs becomes a vital part of security for MANETs. IDS is an automated system and can detect a computer system intrusion either by using the audit trail provided by an operating system or by using the network monitoring tools. It is considered to be the key part of system defence that is used to identify abnormal activities in a computer system. Nowadays, nodes in the network environment are turning out to be more and more susceptible to attack, due to its de-centralised extended network connectivity, flexibility, convenience and cost of MANETs. This paper discusses the fuzzy based network intrusion detection system that classifies and detects the attacks based on fuzzy classifier. To achieve better performance of the system, comparison of DSR with and without fuzzy is done. The overall system hence improves the performance of the network over MANET and achieves various performance metrics of the routing environment using DSR protocol.

II. INTRUSION DETECTION SYSTEM

When any set of actions attempt to compromise with the security attributes such as confidentiality, repudiation, availability and integrity of resources then these actions are said to be the intrusions and detection of such intrusions is known as intrusion detection system (IDS) [R.Heady et al,1990]. Intrusion Detection System is defined as the attempts to comprise the confidentiality, integrity, bypass the security mechanisms of a computer network, intrusion caused by attackers accessing the system from the Internet. The goal of intrusion detection is detecting unauthorized use, misuse and abuse of computers or nodes on the network. In other words, it is the demonstration of recognizing undesirable movement on a system or gadget. An IDS gives a layer of safeguard which screens system movement for predefined suspicious action or examples, and ready system directors when potential threatening activity is distinguished. An intrusion detection system can be a bit of introduced programming or a physical apparatus. IDS can be categorized as Host-based IDS and network- based IDS depending upon its monitoring scope and detection techniques. Host-based IDS can also be referred to as stand-alone intrusion detection systems because their monitoring scope is restricted to only a single host. In the form of a single host, the use of the network traffic information for security auditing is more effective. Network-based IDS monitors the network and detects the malicious activities destined for that network.

III. DSR PROTOCOL

The dynamic source routing (DSR) is a reactive routing protocol, which is suitable for multi-hop mobile ad hoc network [3] [4]. DSR is a simple and efficient routing protocol. It is designed in multi-hop wireless ad hoc networks of mobile nodes. DSR allows the network to be completely self-organizing and self-configuring, without the need for any existing network infrastructure or administration. The routing protocol uses two mechanisms. The mechanisms are Route Discovery and Route Maintenance. The protocol allows multiple routes to any destination and sender. The sender selects the control of routes used in routing its packets, for example, for use in load balancing or for increased robustness. The basic framework for DSR protocol is to stream the 'Route Request' (RREQ) packet in the network. When the destination node receives the RREQ packet, it replies back to the source by sending 'Route Reply'(RREP) packet which includes the route information from the source node. In DSR protocol, the source node first initiates the route discovery process by broadcasting the packet to all its neighbors. Each node after receiving the 'RREQ' packet rebroadcasts to its neighboring nodes besides, if the particular node is not the destination node or it has not passed on formerly.

IV. ATTACK CLASSIFICATION

Attacks in MANET are generally categorized into two types[Revathi et al, 2012]; they are external and internal attacks. The internal attack is caused by a compromised node that belongs to the same network. The external attack is initiated by an outside source through routing which produce false routing information to maximise the network overload. The proposed system is pertinent for two attacks such as packet dropper attack and collaborative attack.

4.1 Collaborative Attack

Collaborative attack is one of the various multiple node attacks found from MANET. Here, a collection of two or more malicious nodes functions together to drop and deplete the packet between the source and destination. The author investigates the performance impacts of a collaborative black hole attack on a mobile ad hoc network. A collusion attack model against Dynamic Source Routing (DSR) protocol is presented. The authors also design a technique to detect the attack by utilizing information of two hop neighbors. The authors assume a clique or a cluster network structure. An honesty-rate IDS makes collaborative decisions based on multiple threshold values including rewards and penalties for packet forwarding. Using the acknowledgements from the destination, the source can find changes in packet delivery. Then a binary search based query procedure is adopted to locate the faulty link in the path.

4.2 Packet Dropper Attack

Packet dropper attackis a type of denial-of-service attack. A router that is supposed to relay packets instead discards them. This usually occurs from a router becoming compromised for a number of different causes. The research is through a denial-of-service attack on the router using a known DDoS tool. Packets are dropped from a lossy network. This type of attack is usually hard to detect and prevent. The malicious router can also accomplish this attack selectively, e.g. by dropping packets for a particular network destination, at a certain time of the day, packets or every seconds, or a randomly selected portion of the packets. This is rather called a greyhound attack. The malicious router drops all the packets. The attack can be discovered fair quickly through common networking tools such astrace route. Other routers notice that thecompromised router is dropping all traffic, and generally begin to remove that router from their forwarding tables and eventually no traffic will flow to the attack.

V. SIMULATION ENVIRONMENT

The network is simulated in four scenarios in the proposed system. Scenario (1): The network is simulated without the presence of packet drop and collaborative attack. Scenario (2): The network is simulated with the presence of attack and without the presence of any IDS. Scenario (3): The network is simulated with the presence of attack and the presence of normal non-optimized intrusion detection system. Scenario (4): The network is simulated with the presence of attack and the presence of optimized intrusion detection system. In each situation, the number of source nodes varies from two nodes to twelve nodes. In addition, each situation has two scenarios, with 1m/s mobility and with 20m/s mobility. The aim of these scenarios is to monitor the performance of the network in case of low mobility and high mobility.

5.1 Threshold Limit

Threshold is a limit value set by the user. The user can set the value for the best or worst case. The best and worst case value ranges from 0.3-0.6. If the threshold value set by the user is above 0.6, then it is called worst value and the value below 0.6 is called best value of the system. When a packet reaches the threshold value 0.6, the packet is considered as a normal packet; otherwise, the packet is considered to be malicious.

5.2 Fuzzy Measures

The proposed system automatically finds the fuzzy rules based on mined 1-length frequent items. The fuzzy rules are generated from definite rules, where the IF part of the rule is a numerical variable and THEN part is a class label related to an attack or a normal node. The membership is rather than crisp set membership or non-membership. It provides a very valuable flexibility for reasoning that takes inaccuracies and uncertainties into account. It provides a simple way of arriving to a definite conclusion based upon vague, ambiguous, noisy, imprecise or missing input information. The activated rules are combined in the rule base to compute the fuzzy output distribution. The fuzzy output distribution is defuzzified to obtain a crisp output value.

5.3 False Positive

False positive is obtaining a positive result for a condition. In this case, the output of the condition should be negative. This state is called a “false alarm” or “false positive error” state. IDS classifiesBENIGN packet as malicious and signals the nodes on the network.

False Positive Rate (FPR) = False Positive / False Positive + True Negative

5.4 False Negative

A false negative is obtaining a negative result for a condition. In this case, the output of the condition should be positive. This state is called a "false negative" state. IDS classifiesmalicious packet as benign.

False Negative Rate (FNR) = False Negative / False Negative+True Positive

5.5 Fuzzy Classification

Fuzzy classifiers are an application of fuzzy theory. The knowledge here is represented in a natural way using linguistic variables that are defined by the fuzzy sets. Fuzzy controllers are compared with classical controllers. Fuzzification is the first block controller. The controllers provide simplicity of control, low cost and the possibility to design without knowing the exact mathematical model of the process. Here, the variables are linguistic rather than numeric variables. Linguistic rules defining the control system consists of two parts: an antecedent block (IF…THEN) and a consequent block (following THEN). The rules are combined in a table called rule base. The values of natural language may be represented by fuzzy sets. Fuzzy set elements may partially belong to more than one set. The controller infuzzificationconverts each piece of input data to degrees of membership. There are many several membership functions thatmatch the input data with the conditions of the rules to determine. The condition is that each rule should match that particular input instance.

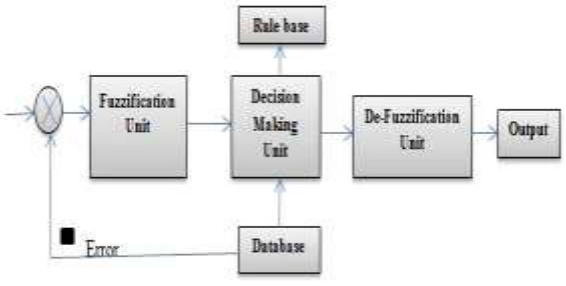


Fig. 1Fuzzy Classifier

The conclusion of the rule can be applied to both multi-input-multi-output problems and single-inputsingle-output problems. The output of the rule base is converted to a number that can be sent to the process as a control signal. This type of operation is called defuzzification that is done to obtain the crisp output.

VI.COMPARISON OF DSR PROTOCOL

6.1 Without Fuzzy Measures

Fuzzy system with minimum inference method is used in the system. That is called as the fuzzy inference method. The operation was set to minimum and defuzzification was carried out using centroid defuzzifier. The triangle membership functions were used to represent inputs and output with three linguistic variables inputs. The inputs are Low, Medium, and High.The outputs are Very Low, Low, Medium, High, and Very High. The proposed system measures that are given to the fuzzy logic are network size and hop count. The output that has been calculated dynamically is delay. It is found that theperformance of the DSR routing protocol without using fuzzy logic has been enhanced when compared to the original DSR protocol.

6.2 With Fuzzy Measures

Fuzzy systemsare based on set of rules. Theseare created by human logic. The rules are based on uncertainty and approximate reasoning. Fuzzy based methodology is applied in many automated machines like washing machine, refrigerator etc. There are two types of Fuzzy Logic Inference Systems (FIS). Mamdani FIS is taken with DSR in the proposed system. The system has five inputs and two outputs. The Inference System have inputs like Node Density(ND), Pause Time (PT), Node Mobility(NM), Number of Packets transferred(NP) and the Number of Connection(NC) and outputs Packet Delivery Fraction, Normalized Routing Load in the case of fuzzy classification.

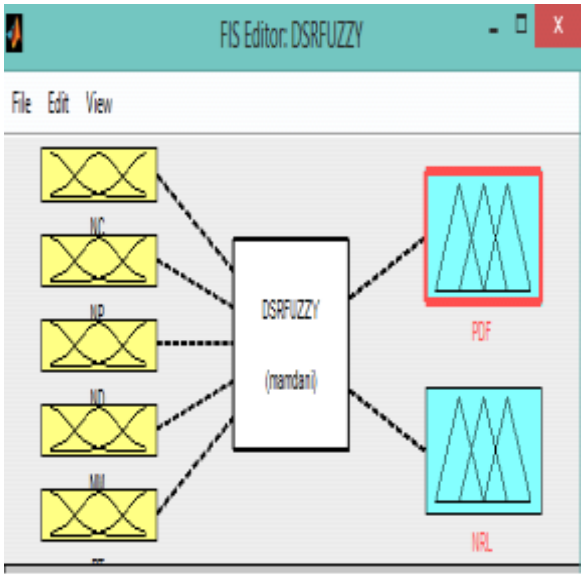


Fig.2 DSR with Fuzzy

VII. PROPOSED SYSTEM

The proposed system uses fuzzy algorithm to classify and detect attacks. The algorithm first discoversthe intrusions and monitors the nodes on MANET with the help of fuzzy measures. Initially, the algorithm defines a fuzzy classification. Randomly generated 100 nodes are deployed in the simulation environment. The source node sends a RREQ packet to the neighboring nodes. The source node broadcasts its packets to the neighboring nodes. Then the destination node identifies the availability of malicious nodes in the network. This monitoring process is called intrusion detection. The nodes in the network broadcasts and rebroadcasts the packets until the intended packet reaches the destination. Using DSR protocol, shortest path is recognised from source to destination. The routing process is finding at that time the node sends the data time to while occurring the "Packet drop attack". Withfuzzy algorithm, at the outset we first classify the attacks as either packet drop or collaborative and then based on threshold levels, malicious nodes are detected. Threshold is a limit set by the user. The user sets the valuesbetween 0.3 and 0.6. If the value set by the user is above 0.6, then the node is considered to be as malicious i.e., a packet dropper attack has been occurred. Otherwise, the nodes are normal. Suppose, if the nodes doesn't relay packets to the next node and discards them with the combination of two or more nodes, then the nodesare said to be collaborative attack. In this system, Fuzzy classification used to classify and prevent the packet drop and collaborative attacks. Finally, performance of the system is enhanced through various fuzzy performance metrics such as Throughput, Packet Delivery Ratio, End-To-EndDelay, Jitter, Packet Loss, Dropping Ratio, Control Overhead and Normal Overhead.

7.1 Algorithm for Proposed System

INPUT:Deployment of Nodes in MANET
Malicious Packets sent at irregular intervals
OUTPUT:Intrusion Detected (PacketDropper, Collaborative attack)
Begin no of nodes randomly generated
Creating a classified group using Fuzzy
Manage Route Stability
Packet Transmission Established
Malicious node sent with packet
Classify the attack with Threshold limit
Fuzzy measures the attack by support and belief of threshold value
Loop until end of the result
Store it asmalicious packet information
End loop
Close all connections
End

International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 12, December 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

VIII.RESULTS AND DISCUSSIONS

8.1 Packet Delivery Ratio

PDR is the ratio between the number of packets transmitted by a traffic source and the number of packets received by a traffic sink. It measures the loss rate as seen by transport protocols and as such, it characterizes both the correctness and efficiency of ad-hoc routing protocols.

8.2 End-to-End-Delay

End-to-end delay is how long it took for a packet travel from the source to destination. It is measured in seconds. The lower value of end to end delay means the better performance of the protocol. It is including all delays in the network such as buffer queues, transmission time and delays including routing activities and MAC control exchanges. It is a reliability routing protocol.

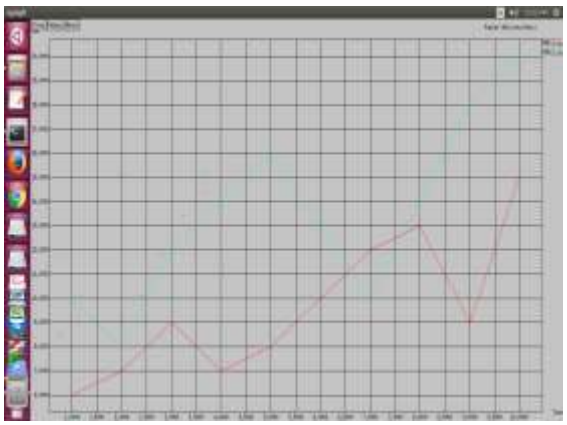


Fig.3 Packet Delivery Ratio

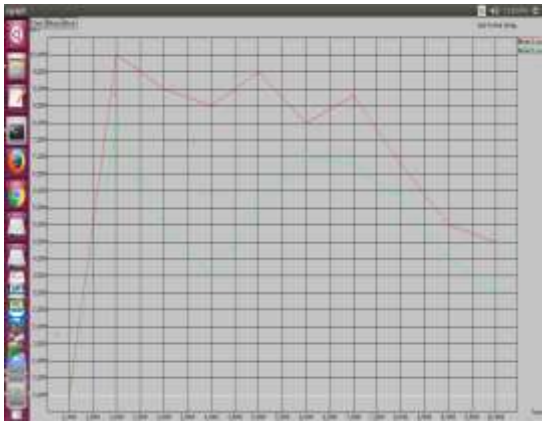


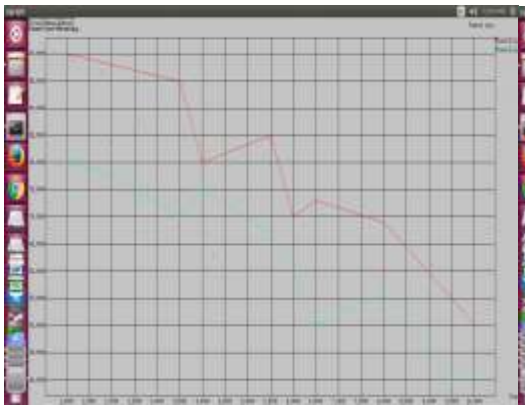
Fig. 5 End-to-End Delay

8.3 Packet Loss Ratio

Packet Loss Ratio is defined as the ratio of total number of data packets which fail to reach the destination node to the number of data packets sent by source node during the simulation process. Packet Loss Ratio is inversely proportional to the Packet Delivery Ratio.

8.4 Normalized Routing Load

Normalized Routing Load is defined as the ratio of total number of routing packets transmitted (including forwarded routing packets also) to the total number of data packets received at the destination nodes.



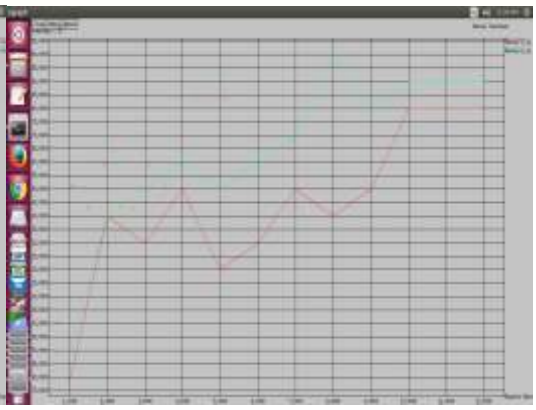


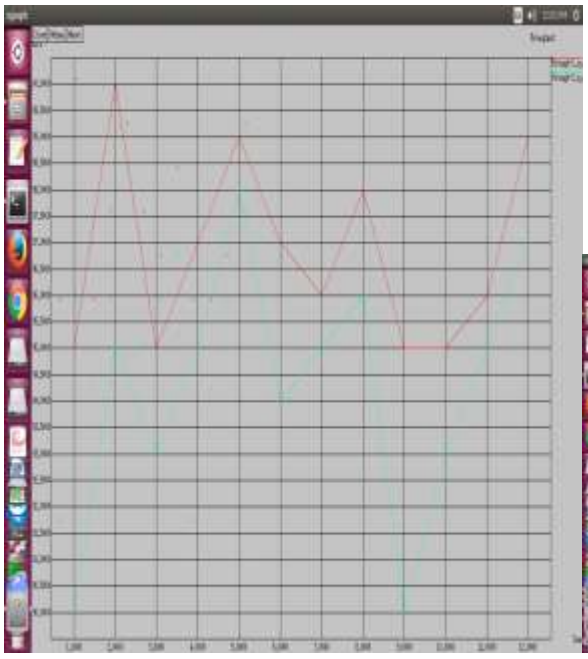
Fig. 6 Packet Loss Ratio **Fig. Normalized Routing Load**

8.5 Throughput

It is the ratio of total amount of data that reaches a receiver from a sender to the time it takes for the receiver to get the last packet. It is measured in bits per sec. which serve as the performance measure for the scheduler. Throughput is measured in bits per second(bit/s or bps).

8.6 Control Overhead

It is ratio of the control information sent to the actual data received at each node in MANET. It also refers to the processing time required to transmit a data by a node, which includes all the supporting functions like node discovery, link maintenance, network size, network latency and data transmission.



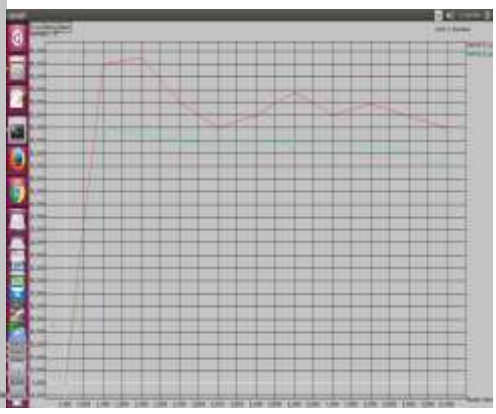


Fig. 8 Throughput **Fig. 9 Control Overhead**

IX.SIMULATION ENVIRONMENT

Table Simulation Parameters

Parameter	Value
Simulator	NS2
Nodes	100
Protocol	DSR
Simulation Area	1500*1500 m
Antenna	Omni-directional
Propagation Model	Two ray ground reflection
MAC	802.11
Power consumption for Transmission	1.6 W
Power consumption for Reception	1.2 W
Data rate	2Mbps
Traffic Source	Constant Bit Rate (CBR)
Battery Model	Linear
Speed of nodes	1 m/sec to 20 m/sec

X.CONCLUSION

The proposed method not only identifies the attack, it also identifies the range and extension of attack. The system provides a noble solution that classifies and identifies the attacker on the network by using fuzzy logic technique. The system also contains an IDS mechanism which gets input from fuzzy technique and provides secure data communication over the network. IDS also monitors for the traffic of black hole and gray hole attacks. The results clearly showthat this method detects attacks in an efficient manner when compared to existing method. The overall system thus enhances both qualitative and quantitative metrics. Future work includes the reduction of jitter value which is more in presence of IDS, which is because of route modification in presence of attacks.

REFERENCES

[1] Y. Li and J. Wei., "Guidelines on selecting intrusion detection methods in MANET", In Proceedings of the Information Systems Educators Conference, Commodore Perry, 2004, 1-13.

[2] A. Hasti, "Study of Impact of Mobile Ad – Hoc Networking and its Future Applications", BVICAM's International Journal of Information Technology, 4(1), 2012, 439-444.

[3] David B.Johnson, David A. Maltz, Josh Broch, "DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks", Carnegie Mellon University, Pittsburgh, 2001, 139-172.

[4] PrasantMohanpatra, SrikanthV.Krishnamurthy, "AD HOC NETWORKS: Technologies and Protocols", Springer Science and Business Media, USA, 2005, 1-22.

[5] Shailesh P. ThakareDr.M.S.Ali,"Introducing Fuzzy Logic in Network Intrusion Detection System",International Journal of Advanced Research in Computer Science,3(3), 2012, 810-815.

[6] DileepDhakadLaxmiShrivastava, "Comparitive Evaluation of DSR using Fuzzy Logic And Qualnet", InternationalJournal of Innovative Research in Science and Engineering,2(5), 2016, 40-47.

[7] S.Nithya, C.Gomathy, "Detection and Prevention of Collaborative Attack and Energy Efficient Routing in Wireless and Ad hoc Network",Indian Journal of Science and Technology, 9(1),1-6.

[8] Rohit Gupta, O.P.Sharma, "Performance Analysis for Various Mobility Nodes Using Fuzzy Schedule for DSR Protocol" International Journal of Science, Technology & Management, 4(1), 2015, 59-66.

[9] NenekaziNokuthala Penelope Mkuzangwe, Fulufhelo Vincent Nelwamondo, "A Fuzzy Logic Based Network Intrusion Detection System for Predicting the TCP SYN Flooding Attack", Intelligent Information and Database Systems, DOI: 10.1007/978-3-319-54430-4_2, 2017,14-22.

[10] Kulbhushan, Jagpreet Singh, "Fuzzy Logic based Intrusion Detection System against Blackhole Attack on AODV in MANET" IJCA Special Issue on "Network Security and Cryptography", NSC 2011,28-35.

[11] SapnaChoudhary, AlkaAgrawal, "Threshold Based Intrusion Detection System for MANET using Machine Learning Approach" International Journal of Advance Electrical and Electronics Engineering,3(1), 2014, 1-6.

[12] Vishnu Balan E, Priyan M K, Gokulnath C, Prof.Usha Devi G, "Fuzzy Based Intrusion Detection Systems in MANET" 2nd International Symposium on Big Data and Cloud Computing , 2015, 109-114.

[13] V. Jayalakshmi, IAENG T. Abdul Razak, "Trust Based Power Aware Secure Source Routing Protocol using Fuzzy Logic for Mobile Adhoc Networks" IAENG International Journal of Computer Science, 43:1, IJCS_43_1_12, 2016.

[14] Sonal, KiranNarang, "Black Hole Attack Detection using Fuzzy Logic" International Journal of Science and Research , 2(8),2013, 222-225.

[15] Mohammed Abdel-Azim, Hossam El-Din Salah, Menas Ibrahim, "Black Hole attack Detection using Fuzzy based IDS" International Journal of Communication Networks and Information Security, 9(2), 2017,187-195.

[16] G.Shilpa, N.Anjaneyulu, "A Novel Fuzzy Logic Analysis & Study on Intrusion Detection System" International Journal of Computer Science and Mobile Computing, 2(6), 2013, 110-115.