ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

FUZZY BASED INTRUSION DETECTION SYSTEM FOR PREDICTION OF GRAY HOLE ATTACK IN MANET

V.Pagalnila*, M.Lalli

* Research Scholar School of Computer Science and Engineering, Bharathidasan University, Trichy.
Assistant Professor School of Computer Science and Engineering, Bharathidasan University, Trichy.

ABSTRACT

Mobile Ad hoc networks are collections of mobile nodes with links that are made or broken in an arbitrary way. No centralized controller and infrastructure. A major issue in Mobile ad-hoc network is security. This also aims of the work in MANET. To detection of malicious nodes forms a very essential one of the part an approach to security. The main objective of this work is to detect the intrusions through Fuzzy logic that prevents the network from denying the active session or extract the confidential information that is being shared. The proposed work uses fuzzy logic to identify the malicious nodes of capture the intrusion over MANET that networks as well as provide the best solution to reduce the execution time over the network.

The proposed work uses AODV algorithm and implies some fuzzy rules. In this paper a mechanism based on fuzzy logic is proposed to detect the gray hole attack in MANET with AODV protocol. An introduction of gray hole in MANET with NS2 (2.34) is done, after applying fuzzy if then rule to detection of gray hole node. The results showed to get better reflect of the performance rate over the AODV algorithm. The proposed system is implemented using NS2 & its results show its more effectiveness and compared the results with existing works.

KEYWORDS: MANET, Intrusion Detection System, Gray Hole Attack, AODV, Fuzzy Logic, and NS2.

INTRODUCTION

Since the knowledge is growing day by day the popularity of wireless technology is showing a marvelous grows and so opportunity a variety of application in the area of advanced networking. One of the most important fields in this is MANET in which the nodes do not depend on any pre-existing fewer infrastructures. MANET consists of group of nodes that are connected by wireless links & therefore the interconnection between nodes can change on arbitrary basis. No centralized controller and infrastructure and allows free mobility, node acts host and router to assist in transmitting data to other nodes in its range, that's can be quickly and inexpensively setup.

Nodes that are within the communication range of other nodes can communicate directly without the need of wireless links whereas nodes that are far away use intermediate nodes as relays. The eventual objective of MANETs is to offer dynamic, self-healing and self-constructing system for mobile devices .A dynamic network is constructed within the nodes of same radio frequency range of MANET to enable the communication among them. In the absence of fixed network routing equipment, every node in the network acts as host and a router. The self-organized dynamic constructions of MANETs are prone to various network attacks [2], which has been gained focus by many studies over security of MANET. These network attacks are highly challenging for data communication since, it requires total collaboration between the MANET nodes to forward messages an intrusion is a mischievous activity attempting to break the network into or compromise a system. IDS can be distinct as the tools, method, and resources to help classify, assess, and information of unauthorized or unapproved network activity. Intrusion detection is usually one of the parts of an overall security system that is installed around a system or device it is not a stand-alone shield measure. The Mobile Ad hoc Wireless Network is more exposed to be attacked than wired network.

Hence, MANETs need to have an Intrusion Detection System to monitor the fraudulent activities and to take necessary actions to prevent the network from attacks. Moreover, the intrusion detection system could easily identify the attempts

made by any outsiders who are intending to break the network and also prevents from users privileges violations [8]. [9] [10] and [11] says, MANET IDS inventions have been proposed.

AODV is an on-demand distance vector routing protocol [2]. The protocol is well known for the use in ad hoc networks. The use of multicasting with the network has many benefits. Multicasting reduces the communication cost for applications that sending the same data to many recipients [3, 5-8]. Instead of sending via, multicast reduces the channel bandwidth, sender and router processing and packet delivery delay. In addition, multicast source to destination within the wireless environment. Fuzzy is a set of various rules based on the vital features of AODV such as Request Forwarding Rate, Reply Receive Rate and so on. The exiting works where tested only with minimum number of nodes. Whereas, the proposed work is likely to be executed with large datasets. The proposed system is based on Fuzzy logic to detect the malicious node and analysis the delay of execution time and throughput of the rate and over all finding the malicious node of great performance of the result.

FUZZY LOGIC

Fuzzy logic based functions are approximate results rather than fixed and exact. Fuzzy logic variables may have rust values that range in degree between 0 and 1. In the proposed scheme [2] trust decision-making is based on fuzzy rules. If the evaluate expectation is greater than or equal to the threshold trust, and excluded from all future network operations. Depending upon the grade of trustworthiness the node can be included in the network operations and may be assigned unusual duties viz. send both the data and routing packets.

Fuzzy trust is represented [4] by the trust level that ranges over the set of values from very defective to very constant levels. It enables to specify a range for a given trust level instead of giving it a particular discrete value. Trust levels ranging from very not to be trusted, medium trustworthy, extremely trustworthy, unknown based on fuzzy logic.
Fuzzy logic is described as a mathematical system that uses analog input value between 0 and 1 in contrast to digital logic.

The fuzzy logic steps are described below: -

Fuzzification*:* The aim of Fuzzification is to characterize some input variable & input membership function for each input variable.

Knowledge base: It classifies input according to membership function values such as low, medium, high. The knowledge base consists of only rule based on some criteria in the form of if-then rules.

Defuzzification (mapping): In this two graphs are used for mapping.

- Template Graph- It contains all output membership function; which is maximized or minimized value when they have high fuzzy rules used.
- User Action Graph- It includes check log & user profiles.

Figure 1:

Fuzzy Controller

Fuzzy logic deals with reasoning which is approximate instead of fixed. The value in truth table of fuzzy logic ranges between 0-1. It is a problem solving methodology from simple microcontroller to large control systems. Fuzzy logic gives a simple way to arrive at definite conclusion based upon noisy, ambiguous or missing input information.

AODV ALGORITHM

The Ad hoc On Demand Distance Vector (AODV) routing protocol is a reactive routing protocol that uses some uniqueness of proactive routing protocols. Routes are recognized on-demand, as they are needed. However, once recognized a route is maintained as long as it is needed. Reactive (or on-demand) routing protocols find a path between

the source and the destination only when the path is needed and so data to be exchanged between the source to the destination, AODV algorithm is a routing protocol designed for only purpose of ad hoc mobile networks.

AODV is proficient to routing of both unicast and multicast routing protocol. It is an on AODV, meaning that it builds routes between nodes only as preferred by source nodes. It maintains these routes as protracted as they are needed by the source. Moreover, AODV forms routing trees that connect multicast collection of members. The Routing trees are composed of the group members and the nodes needed to connect the collection of members. AODV uses sequence numbers to ensure the novelty of routes. It is loop-free, self-starting, and self-configure scales to large numbers of mobile nodes.

AODV is used mostly to address routing problems in MANET& route to establish communication between nodes with minimum control overhead. AODV is a reactive protocol and it does not need the discovery & maintenance of routes which are not in communication instead it discovers the routes quickly to new destinations. AODV is loop free algorithm & operates in distributed manner. This selection of loop is acquired by using sequence number. Every node has a sequence number that increases monotonically every time there is a change in topology of the network. This sequence number also ensures that recent route is selected when a route discovery process initiates.
There are three types of messages in AODV Routing that are discussed bellow.

Route Request Message (RREQ): -
This is a message used by AODV for the purpose of discovering new routes to a destination node. Each node that receives the RREP packet updates its route destination is free and the packet is retransmitted. If there is more than one node with a valid data send to route path, however, multiple RREP packets will be sending to nodes on the reverse path.

There is a time to live (TTL) value in every RREQ message; the value of TTL states the number of hops the RREQ should be transmitted.

Route Reply Message (RREP): -A node is having a requested uniqueness or any intermediary node that has a route destination to the requested node create a route reply RREP message back to the discoverer node of the route to sender path.

Route Error Message (RERR): - Each node in the network maintains checking the link status to its send to Destination sequence number of nodes through active node routes. When the node identifies connect to break in an active route, (RERR) Message is generated by route path to the node in order to inform other nodes that the link is down.

RELATED WORK

In this section we will study various national and international research papers and about the proposed techniques for malicious node detection in Mobile Ad hoc Network. The research area related to this field is very large and complex. Here we will discuss some of them that are related to my proposed work.

Ireland, et al performed a work "Intrusion Detection and Defense Mechanism for Packet Replication Attack over MANET Using Swarm Intelligence" described an IDS approach based on fuzzy genetic algorithms. The algorithm designed by the author randomly generated improved fuzzy rules in the training phase. A record could either be an attack or normal activity was passed into a rule and was matched to one block of the rule. The parameters of each block measured the degree of certainty of an attack using the trapezoidal fuzzy rule shape. The sum of the degrees of certainty from each block was then compared with a threshold to determine if the record represented an attack or normal behavior. The detection rate of the proposed algorithm was up to 99%.

Y. Zhang, W. Lee, and Y. Huang, et al performed a work "Intrusion Detection Techniques for Mobile Wireless Networks,, designed a fuzzy genetic algorithm for Intrusion Detection to efficiently detect various types of intrusions within a network. The proposed fuzzy logic-based system was able to detect the intrusions in the networks as the rule base holds a better set of rules. The experiments and evaluations were performed with the KDD Cup 99 intrusion detection benchmark dataset. The experimental results highlighted that the achieved higher accuracy rate in identifying

Denial of service with 85.70% whether the records were normal or abnormal ones and obtained reasonable detection rate.

R. Shanmugavadivu, Dr.N.Nagarajan, et al performed a work "Network Intrusion Detection System Using Fuzzy Logic", designed a fuzzy logic-based system for effectively identifying the intrusions within a network. The author used an automated strategy for generation of fuzzy rules, which was obtained from the definite rules using frequent items. The experiments and evaluations of the system were experimented with the KDD Cup 99 intrusion detection dataset and the achieved results had higher precision of 90% in identifying all types of attacks.

Shadab Siddiqui, P. M. Khan,et al performed a work "Fuzzy Logic Based Intruder Detection System in Mobile Adhoc Network"" proposed fuzzy logic technique to identify network attacks and to find out the malicious behavior of nodes. The author provided security in Mobile Ad hoc Network. AODV algorithm was used.The proposed work will do comparison between the performance parameters obtained from AODV with priority based Intruder detection system with AODV implementing fuzzy logic to identify gray hole nodes. The outcome will show great improvement of AODV with fuzzy logic over the algorithm was implemented using Mat lab& its results show its effectiveness.

PROPOSED WORK

The proposed work consists of four steps namely route path creation using AODV algorithm in mobile ad hoc network, using Fuzzy logic. The proposed work is uses of IF THEN fuzzy rule applied in AODV and some implies rule based system followed in intruder detection and to identify the malicious nodes, named as gray hole attack. AODV algorithm is applied to generate path for route discovery and data forward. AODV uses all its features to create the path from source to destination.

The generation of fuzzy rules takes place along with membership function. The fuzzy IF-THEN rules are applied in order to detect malicious node. In this step verification of IF-THEN rules takes place. The condition of IF statement confirmed by checking if the destination sequence number is much greater than source sequence number and if response time of node is greater than set threshold value then malicious node is detected In this step we will be able to detect the malicious node and detect of the gray hole attack by applying fuzzy rules. The procedure can be understood by following algorithm.

Step 1 select sender and receiver node.
Step 2 selected _node =source
Step 3 while (selected node! =destination)
Step 4 Broadcast from Selected _node
Step 5 Select intermediate nodes by using AODV.
Step 6 Find the malicious node by using Fuzzy logic
Step 7 If intermediate node= =safe
{
Update present node=Intermediate node.
}
Else if (Destination sequence number of n type>source sequence number of n type) && (source node type>threshold)
{
Find gray hole attack
}
Else
{
Go to step 4
}
Step8. End while.

SIMULATION STUDY

Simulation Settings

A Mobile Ad-hoc network (MANET) that consists of node is created. The data packets are transmitted to destination node and received by the nodes using Ad-hoc On Demand Distance Vector (AODV) routing protocol. When an event is detected the nodes transmits more number of data packets up to destination. When more number of nodes to size, the equal wireless channel the malicious will occur. This is known as channel contention. Once the malicious is

detected the each intermediate node adjusts its transmission rate in order to throughput value. To detect and malicious node an effective and efficient technique is implemented in NS2.Simulations done with the help of using NS-2 simulation program that consists of the collection of all network protocols to simulate many of the accessible network topologies and event. Even though NS-2 contains wireless ad-hoc
Routing protocols, it does not have any modules to simulate number of malicious node. All routing protocols simulate in NS2 it's installed in the directory of "ns-2.34". The network performance is also evaluated by calculating delay and throughput value. A review of simulation parameters is given in Table.

Tables:

Table 1. SIMULATION PARAMETERS

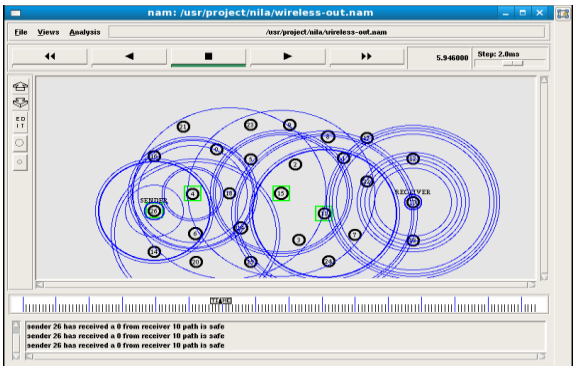
Channel Type	Channel/Wireless Channel
Radio-Propagation	Propagation/Two Ray Ground
Transmission range	250m
MAC Protocol	Mac/802_11
Interface Queue	Queue/Drop Tail/PriQueue
Antenna Model	Antenna/Omni Antenna
Routing Protocol	AODV (Ad-hoc On Demand Distance Vector)
Simulation time	16min
Traffic Type	TCP/FTP, UDP/CBR
Packet size	512 bytes
Number of nodes	0 to 27
Total area	700*510
Malicious nodes	1
Mobility Model	Random Waypoint
Packet rate	4paket/sec
Max Speed	0-05 m/sec

Simulation Scenario

The proposed work is detect the gray hole attack by using fuzzy logic that also used in AODV routing protocol is simulated using NS2 simulator. The aim of these simulation runs is to analyze the performance of the proposed work. Performance is compared in terms of average throughput ,delay time for malicious node occur and without malicious node and e, throughputs is defined as the ratio of number of packets received to that of the number of packets sent and the performance of the rate for malicious node is the overall average delay time by a packet from the source to that of the destination.

There are used 27 nodes placed randomly in the simulation environment use. Due to random dynamic topology, the source and destination are also selected randomly.

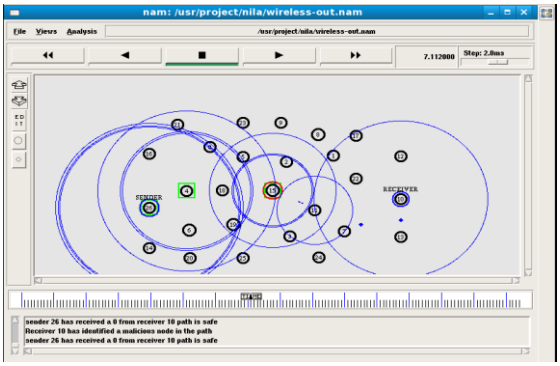
Figure: 1



PACKETS TRANSMISSION

This fig 1 showed the normal packet transmission using selected path and it shows the random packet transmission in wireless network topologies.

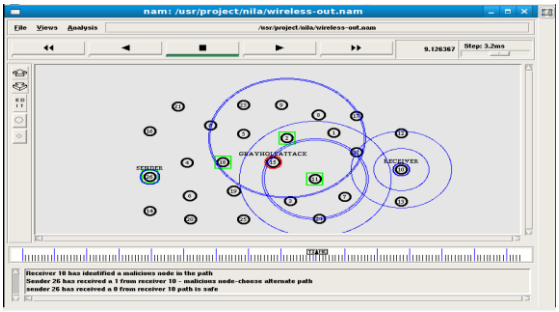
Figure: 2



PACKET DROP AND MALICIOUS NODE

This figure 2 show the malicious node occurs at same time showed packet dropping. Whenever detect the malicious node generate after then loss of packet transmission and if the destination sequence number is much greater than source sequence number and if response time of node is greater than set threshold value then malicious node is detected in red code that's intermediate node is detected is called malicious.

Figure: 3



PACKETS RETRANSMIT WITH ALTERNATE PATH

This fig 3 shows packet retransmit with taken alternate path. There are different kind of attack but my proposed work uses of gray hole attack because gray hole attack is also packet dropping attack whenever gray hole node is send to

packet random only from source to destination if packets not received acknowledgement with in threshold time then nodes select alternate path for retransmit packets. And therefore, the packet loss is very low due to it fast detect of malicious node and packets retransmit through new path every time.

Simulation Results

In this paper, an analysis is done for throughput value and Delay and the result is compared with AODV. The simulation result shows the effectiveness of the proposed technique. We are viewing results of our proposed system and existing system by using some different performance parameters.

A variety of parameters used for analysis are described below:

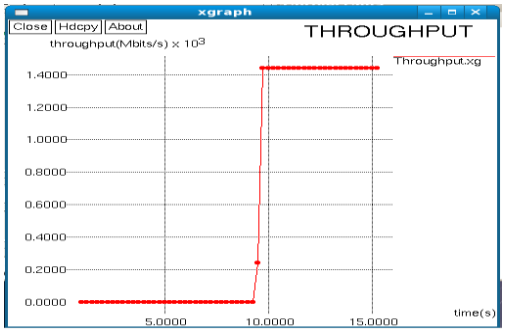
Packet Loss Ratio (PLR): It is the ratio of difference between the total number of generated packets and total number of received packets divided by the total number of generated packets.

PLR = (Generated packets- Received Packets)/ Generated packets Throughput value: It is also known as packet Delivery ratio of the amount of data packets delivered to the destination and total number of data packets sent by source.

PDF= (Received Packets / Packets Sent)*100 Delay Time: The interval time between sending by the source node and receiving by the destination node, which includes the processing time and queuing time.

EED= (Time packet received-Time packet sent)
Total number of packets received

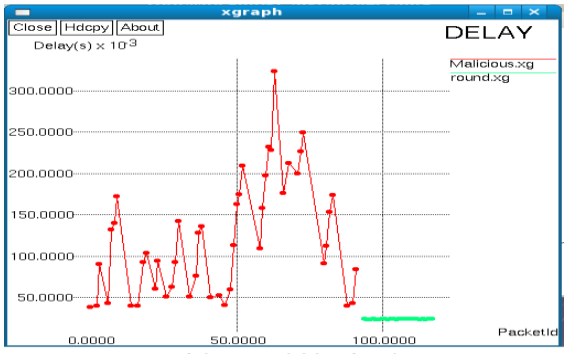
Figure: 4



PACKETS DELIVERY RATIO

The Figure 4 shows Packet delivery ratio. The proposed work is to increase the Packet delivery ratio before find the malicious node. The nodes are waiting for acknowledgement in threshold phase of time .If the Acknowledgement not received with in threshold phase means malicious node is occurs so to select the alternative path or retransmit the packets and after send to packet transmission in safe path.

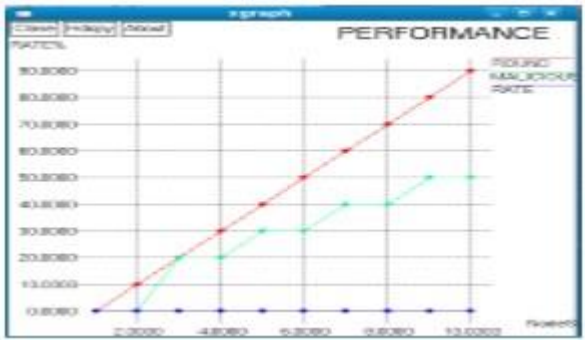
Figure: 5



PACKET LOSS RATIO

Figure 5 shows the Packet loss ratio. The Packet loss ratio is decreased in source to destination node.
The nodes are waiting for acknowledgement for threshold period of time if the Acknowledgement not received with in threshold period which shows detect the malicious node so again to select alternate path or retransmit the packets. So packet dropping is very low and select the all node send to source to destination and path also very safe node, so packet loss ratio is 100%.

Figure: 6



AVERAGE END-TO-END DELAY RATIO

Figure 6 depicts overall performance of ratio. In our proposed work is to decrease the average end-to-end delay. Because in this network nodes are waiting for acknowledgement for threshold phase of time, if the Acknowledgement not received with in threshold period that the time malicious node is occur and again selected the alternate path to send the packet in safe path so packet transmission time is delay and packet loss ratio decreased. The performance round rate is 100% so every node is safe path.

Table 2. Table showing performance analysis of proposed system

No. Of Nodes	Malicious Node	Send Packets	Received Packets	Packet Loss ratio	Average end to end delay
26	1	1005	1005	100	9615ms
100	3	850	850	100	11785ms
200	3	670	670	100	13578ms

CONCLUSION

The security MANET issues are discussed and analyzed the security system with our proposed model Intruder Detection System in MANET using Fuzzy Logic for predict gray hole attack. This model is organized for protecting against over attacks. Our proposed model can find the safe route and helps in preventing attack in MANET by identifying the node with sequence no & entry value no. The system will check for the crosses the threshold value then that node is said to be malicious node. Mostly the malicious node will give high-speed route reply with high destination sequence number Moreover on identifying the malicious node the routing table and messages from malicious node are not forwarded in network. The proposed result does not require any type of overhead on destination node or any intermediate node on AODV routing protocol. I have also used fuzzy IF-THEN rules to identify and detect attacks. This AODV algorithm with fuzzy logic will provide best solvable solution for reduction of data loss over network. The results have shown that proposed system has better performance than typical AODV in all its parameters like execution time, throughput, hop count etc. In addition, the results are also discussed and propose some new dimension for the future works on IDS in MANET using Neuron fuzzy logic .Because fuzzy logic is provided accuracy result and fixed of predictable decision-making rule.

REFFERENCES

[1] G. Indirani, Dr. K. Selvakumar, V. Sivagamasundari, "Intrusion Detection and Defense Mechanism forPacket Replication Attack over MANET UsingSwarm Intelligence", IEEE, 978-1-4673-5845-3, 2013.
[2] C. Perkins, E. Belding-Royer and S. Das, Ad Hoc On-Demand Distance Vector (AODV) Routing.IETF RFC 3561, July 2003.
[3] V. R. Ghorpade, (2008)" Fuzzy Logic based Trust Management Framework for MANET", DSP Journal, Volume 8, Issue 1.
[4] Ahmad Ridha, Ali Rizvi, FaragAzzedin, (2007) "Fuzzy Trust for Peer-to-Peer Based Systems", World Academy of Science, Engineering and Technology.
[5] MarjanKuchaki Rafsanjani, Ali AsgharKhavasi, Ali Movaghar,"An Efficient Method for Identifying IDS Agent Nodes by Discovering Compromised Nodes in MANET", IEEE, 978-0-7695-3925-6, 2009.
[6] A.Karygiannis and K.Robotis, E.Antonakakis," Creating Offline MANET IDS Network Traces ", IEEE, 1 - 4244-0992-6, 2007.
[7] YasirAbdelgadirMohame, Azween B. Abdullah "Implementation of IDS with Response for Securing MANETs "IEEE, 978-1-4244-6716-7110, 2010.
[8] Ricardo Puttini, Jean-Marc Percher, Ludovic MC, Rafael de Sousa,"A Fully Distributed IDS for MANET ", IEEE,0-7803-8623-W04.2004.
[9] HadiOtrok, Joey Paquet, **"**Testing Intrusion Detection Systems in MANET: A Comprehensive Study ", IEEE, 0-7695-2835-X, 2007.
[10] Ashraf Abu-Ein, Jihad Nader "An enhanced AODV routing protocol for MANETs" IJCSI International Journal of Computer Science Issues, Vol. 11, Issue 1, No 1, January 2014.
[11] K.S.Sujatha, VydekiDharmar, R.S.Bhuvaneswaran, "Design of Genetic Algorithm based IDS for MANET ", IEEE, ISBN: 978-1-4673-1601-9,2012 .
[12] Christoforos Panos1, Christos Xenakis2 and Ioannis Stavrakakis1, "A Novel Intrusion Detection System for MANET", IEEE,
[13] A. Mishra, K. Nadkarni, and A. Patcha, "Intrusion Detection in Wireless Ad Hoc Networks," IEEE Wireless Communications, Vol. 11, Issue1, pp. 48-60, February 2004.
[14] Y. Zhang, W. Lee, and Y. Huang, "Intrusion Detection Techniques forMobile Wireless Networks," ACM/Kluwer Wireless Networks Journal(ACM WINET), Vol. 9, No. 5, September 2003.
[15] Emma Ireland, "Intrusion Detection withGenetic Algorithms and Fuzzy Logic", UMM CSci Senior Seminar Conference, December 2013.
[16] P. Jongsuebsuk and N. Wattanapongsakorn, C. Charnsripinyo, "Network Intrusion Detection with FuzzyGenetic Algorithm for Unknown Attacks", IEEE, 2013.
[17] Mostaque Md. Morshedur Hassan, "Network Intrusion Detection System UsingGenetic Algorithm and Fuzzy Logic", International Journal of Innovative Research in Computerand Communication Engineering, 2013.
[18] R. Shanmugavadivu, Dr.N.Nagarajan, "Network Intrusion Detection System Using FuzzyLogic", Indian Journal of Computer Science and Engineering, 2011
[19] B.BenSujitha, R.RojaRamani, Parameswari, "Intrusion Detection System using Fuzzy GeneticApproach", International Journal of Advanced Research in Computer and Communication Engineering, 2012.
[20] ShadabSiddiqui, P. M. Khan, "Fuzzy Logic Based Intruder Detection System in Mobile Adhoc Network", BIJIT - BVICAM's International Journal of Information Technology, 2014.