ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 1, January 2017

Artificial Intelligence Technique Application Based Intrusion Detection System in MANET

Mahvish Jabeen, Anuradha Sharma

P.G. Student, Department of Computer Science, Amity University, Lucknow, India

Associate Professor, Department of Computer Science, Amity University, Lucknow, India

ABSTRACT*:* With late advances in system based innovation and expanded constancy of our regular life on this innovation, guaranteeing reliable operation of network based frameworks is critical. Amid late years, number of attacks on systems has drastically expanded and thusly enthusiasm for system interruption discovery has expanded among the researchers. Intrusion represents a genuine security hazard in system environment. The steadily rising new intrusion or attacks sort postures extreme challenges for their detection. The human marking of the available system review data examples is by and large dull, costly and in addition tedious. This paper concentrates on detecting malicious nodes in MANET (Mobile Adhoc Network) by using fuzzy logic and rules using efficient AODV protocol for routing of packets to increase the efficiency of the intrusion detection system from the existing.

KEYWORDS*:* MANET (mobile adhoc network), A.I. Techniques (fuzzy logic), Malicious Node, Network Attacks, Network Intrusion.

I. INTRODUCTION

Intrusion detection grew from the notion that computer misuse can be detected by analyzing audit data in a computer system or network [1]. Intrusion detection basically refers to the monitoring of network or system and the activities going on in them thus providing an important aid to the administrators about the various activities related to security. As networks are growing larger day by day, there must be some mechanism to detect intrusions. Organizations which are spreading their network across the world through internet that is E-Commerce need it the most. Nowadays, the intruders conceal their activities so as to extract maximum information and not only they are confined to information extraction but masquerading and misusing the extracted information for launching novel attacks on the target host for their benefit. Through intrusion detection it becomes possible to identify and recognize all such attacks and report them to the administrator. An Intrusion Detection System (IDS) is a combination of both hardware and software that makes it possible to detect malicious activities. It is able to monitor network traffic, analyses audit log files and match well known attack signatures already stored in knowledge base, etc. It inspects all outbound and inbound network action and find out the doubtful patterns that may point to a network or system intrusion or attack from someone trying to crack into or conciliation a system. IDS gathers and observed information from different areas inside a network of systems to find out probable safety breaches, which contain together called intrusions (attacks exterior from theassociation) and misuse (attacks from inside the association). IDS use susceptibility assessment, it is an expertise which is design and developed to appraise the security of a network [26]. That is it gathers information from various known sources and is able to decide whether intrusion has taken place. The functional components of an IDS are- information source, analysis and response [2]. The most widely used IDS are Host Based IDS and Network Based IDS. Host Based IDS are able to detect intrusions on hosts and perform complete analysis on the host machines while the Network Based IDS are busy in sensing and monitoring network traffic that is intruders who attack on network traffic. The focus of this paper is on Network Based IDS to detect malicious nodes in MANET's (Mobile Adhoc Network) using efficient AODV routing protocol and fuzzy logic.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 1, January 2017

II. RELATED WORK

- **Yogita Danane, and Thaksen Parvat**, (2015) [27] according to them PC security has turned into an imperative piece of the day today's life. Single PC frameworks as well as a broad system of the PC framework additionally requires security. In accomplishing the security of the frameworks, an Intrusion Detection System (IDS) assumes a huge part. This work shows a fluffy hereditary way to deal with distinguishing system interruption. Work displays the aftereffects of the proposed framework regarding precision, execution time, and memory designation. To execute and measure the execution of the framework the KDD99 benchmark dataset is utilized.
- **Salma Elhag, Alberto Fernández, Abdullah Bawakid, Saleh Alshomrani, and Francisco Herrera (2015**) [27], they worked on the security approaches of data frameworks and systems that are intended for keeping up the honesty of both the secrecy and accessibility of the information for their trusted clients. In this work, we consider the utilization of Genetic Fuzzy Systems inside of a pairwise learning structure for the advancement of such a framework.
- The work entitled "Fuzzy Logic based Intruder Detection System in Mobile Adhoc Network" by **Shadab Siddiqui, P. M. Khan and Muhammad Usman Khan** (2014) [27], is an approach to detect malicious nodes by applying fuzzy logic in Mobile ad-hoc networks. The objective of the work is to provide security in Mobile Adhoc Network. The proposed work uses AODV algorithm. This algorithm implies some fuzzy rules which is implemented on the nodes in the network. The if-then rules of fuzzy will identify the malicious node in the network. 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 malicious nodes
- The work proposed by **Zaheeruddin, Vinod K. Jain, and Guru V. Singh** (2006) [27], a novel methodology for demonstrating commotion prompted disturbance utilizing the fluffy system. The fluffy methodology offers an advantageous method for speaking to the connections between the inputs and yields of a framework as basic IF–THEN rules.
- **Sampada Chavan, Neha Dave and Sanghamitra Mukherjee (2004) [27],** according to them the Intrusion Detection System structural engineering generally utilized as a part of business and examination frameworks have various issues that farthest point their configurability, versatility or productivity. In this work, two machine-learning standards, Artificial Neural Networks and Fuzzy Inference System, are utilized to outline an Intrusion Detection System. Grunt is utilized to perform constant activity investigation and bundle signing on IP system amid the preparation period of the framework.

III. INTRUSION DETECTION SYSTEM:

Intrusion Detection System (IDS) has become a primary study area in Computer-based security. When a person tries to access an information structure in the system or does any illegal action, the action is known as an intrusion that further has two types, exterior, and interior. The exterior are those people who do not have authority to access the system information and still they try to obtain illegitimately with the help of different saturation techniques. While interior is those who have a legal permission to access system, but try to do illegal activities. Any information system should accomplish three main principles for guarantee a correct access to the data, namely confidentiality, integrity and availability. Unfortunately, all networks could be the object of unauthorized accesses so that a strong security policy must be established for avoiding this violation of the prior principles [9]. The technology developed for this aim is known as IDS, which dynamically monitors logs and network traffic, applying detection algorithms to identify these potential intrusions within a network [8]. In particular, IDS can be split into two categories according to the detection methods they employ, **including (1) misuse detection and (2) anomaly detection.**

- **Misuse detection systems** use an established set of known attack patterns, and then monitor the net trying to match incoming packets and/or command sequences to the signatures of known attacks [17]. Hence, decisions are made based on the prior knowledge acquired from the model.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 1, January 2017

- **Anomaly detection methods** seek to define a ‘‘normal’’ behavioral model, and assuming that any deviation from this profile is considered to be an attack [23]. Therefore, good detection results can be obtained from novel attacks.

IDS Terminology

- **Alert/Alarm-** It is a signal signifying that the system already been or is being attacked.
- **True Positive-** It is an applicable attack which initiates IDS to make an alarm.
- **False Positive-** It is an action signaling IDS to make an alarm when there is no attack taken place.
- **False Negative-** It is a breakdown an IDS to become aware of a real attack.
- **True Negative-** When no attack has taken place IDS does not make any alarm.
- **Noise-** It is Data or intrusion that can initiate a false positive.
- **Site policy-** Guiding principles of an institute those used to manage the system and configurations of IDS.
- **Site policy awareness-** It is the capability of an IDS to modify its policies and configurations vigorously according to the changing environmental activity.
- **Confidence value-** It is a value an institute gives to an IDS based on past presentation and study to help conclude its capability to recognize a threat efficiently.
- **Alarm filtering-** It is a method of sorting attack alerts available from an IDS to differentiate false positives from real attacks.

IV. AODV PROTOCOL

AODV combines some properties of both DSR and DSDV. It uses route discovery process to cope with routes on demand basis. It uses routing tables for maintaining route information.AODV handles route discovery process with Route Request (RREQ) messages. RREQ message is broadcasted to neighbour nodes. The message floods through the network until the desired destination or a node knowing fresh route is reached. Sequence numbers are used to guarantee loop freedom. RREQ message cause bypassed node to allocate route table entries for reverse route. The destination node unicasts a Route Reply (RREP) back to the source node. Node transmitting a RREP message creates routing table entries for forward route.

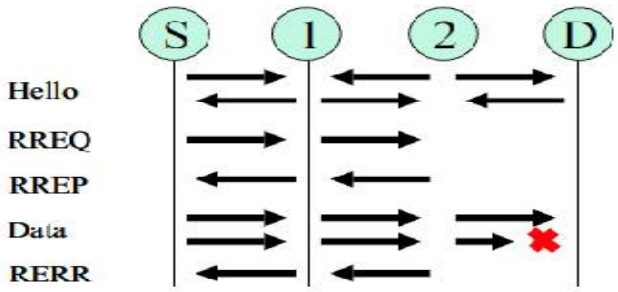

Fig. 1. AODV Protocol

For route maintenance nodes periodically send HELLO messages to neighbour nodes. If a node fails to receive three consecutive HELLO messages from a neighbour, it concludes that link to that specific node is down. A node that

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 1, January 2017

detects a broken link sends a Route Error (RERR) message to any upstream node. When a node receives a RERR message it will indicate a new source discovery process.

V. FUZZY LOGIC

Boole [22] introduced the beautiful notion of binary sets, which is the foundation of modern digital computer but Boolean logic is unable to model the human cognition and thinking process. Because of its rigid boundaries, the two valued logic is not so efficient in mapping real world situations. In order to handle real world problems Zadeh [23] introduced the concept of 'mathematics of fuzzy or cloudy quantities' followed by his seminal paper 'Fuzzy sets' [24]. Fuzzy logic is a superset of Boolean logic. Fuzzy logic uses fuzzy rules which are one of the important applications of fuzzy theory. Fuzzy logic is described as a mathematical system that uses analog input value between 0 and 1 in contrast to to digital logic.

Steps for fuzzy logic are:-

- **Fuzzification:**The aim of Fuzzification is to define input variable & input membership function for each input variable.
- **Knowledge base:** It classifies input according to membership values such as low, medium, high. The knowledge base consists of rules in the form of if-then rules.
- **Defuzzification (mapping):** In this two graphs are used.
  A. **Template Graph-** It contains all output membership function which are maximized when they have high fuzzy rules.
  B. **User Action Graph-** It includes audit log & user profiles.

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.

Fig. 2. Fuzzy Controller

VI. PROPOSED WORK

The proposed work consists of four phases namely Path generation using AODV algorithm, applying Fuzzy logic, verification and detection of malicious nodes.

A. *PHASE ONE: PATH GENERATION USING AODV ALGORITHM*

In this phase AODV algorithm is applied to generate path for route discovery. AODV uses all its features to generate the path from source to destination.

B. *PHASE TWO: APPLYING FUZZY LOGIC*

In this phase the generation of fuzzy rules takes place along with membership function. The fuzzy IF-THEN rules are applied in order to detect malicious node.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 1, January 2017

C. ***PHASE THREE: VERIFICATION***

In this phase verification of IF-THEN rules takes place. The condition of IF statement verified 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 .

D. ***PHASE FOUR: DETECTION OF MALICIOUS NODE***

In this phase we will be able to detect the malicious node by applying fuzzy rules.

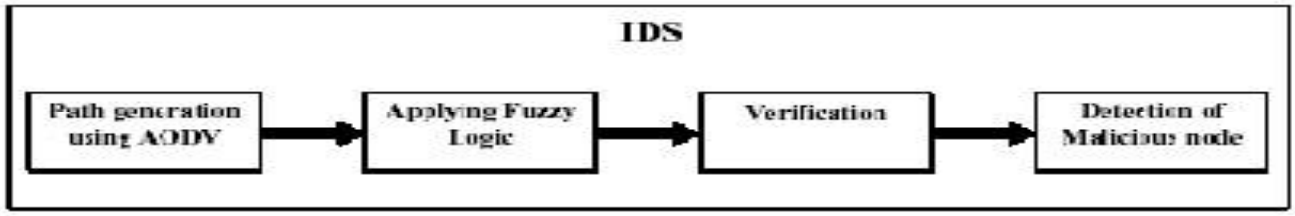

Fig. 3. Proposed Fuzzy based IDS model.

E. ***FUZZY RULES:***

- Rule 1) If (source sequence is low) OR (response time is high) then output is medium
- Rule 2) If (source sequence is low) AND (response time is medium) then output is high
- Rule 3) If (response time is medium) then output is low.
- Rule 4) If (source sequence is high) then output is low.

VII. EXPERIMENTAL RESULTS

Here we will evaluate our model Intruder Detection system in MANET using Fuzzy Logic. This system is developed to operate anywhere in any situation, therefore the experiment is carried out with same scenario with different experiments that shows the performance of system. The parameters used for simulation will be compared to the existing model. It is very important to choose suitable parameters for system evaluation. The performance parameters will describe the result of simulation. These parameters are important as they will be used to notify what will actually happen during simulation. Our choice is using MATLAB- 2010. MATLAB uses the hierarchical architecture in order to define components like nodes & network. The components are defined by text based language. The components can be nested to form complex module inside each other.
Every module can be accomplished by C++ file which describe its behaviour. MATLAB provides many modules such as queues, tools etc. by using C++ computation. MATLAB uses documentation & active discussion forums.

A. VALIDATION IN TERMS OF METRICS USED FOR COMPARISON.

The performance comparison is based on various metrics between existing AODV with proposed AODV using fuzzy logic.

B. THROUGHPUT

It is defined as total no of delivered packets divided by the total duration of simulation time.
Throughput = (Packets sent / Packet Total) *100

C. HOP COUNT

It is variation in time stuck between packets inward caused by network congestion & due to route changes.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 1, January 2017

D. EXECUTION TIME

It is the time used by algorithm for execution.

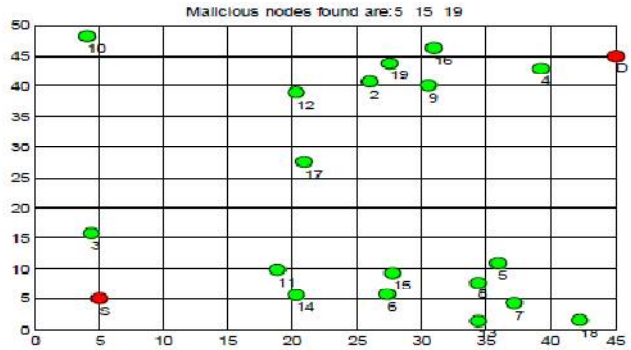

*Fig. 4. Displaying no of nodes in 50*50 area*

Nodes are displayed from source to destination and malicious nodes are found

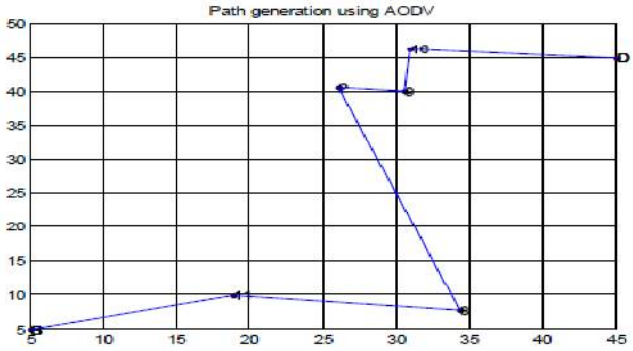

Fig. 5. Line showing path from source to destination

The figure shows the nodes selected and path formed from those nodes from source to destination.

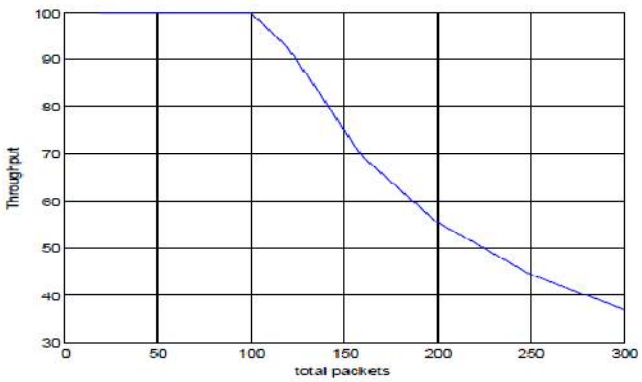

Fig. 6. Graph displaying throughput

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 1, January 2017

Throughput is calculated by taking different number of packets at a time and comparison is done as to what happens to the performance of the system after that.

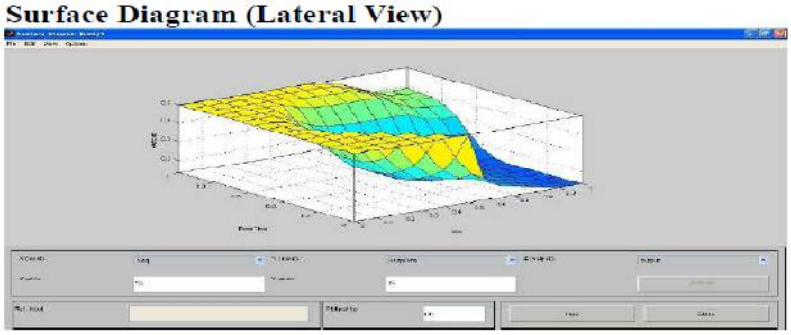

Fig. 7. Surface diagram displaying the no of malicious nodes (Lateral view)

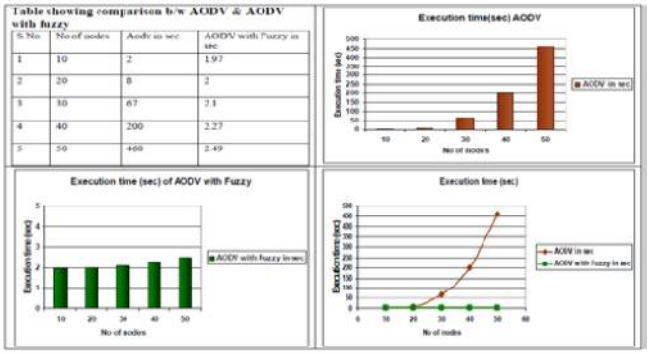

Fig. 8. Graph showing the execution time (sec) of AODV & AODV with fuzzy logic

VII. CONCLUSION

The security of MANET has picked up ubiquity among examination region. The security issues are examined and we have dissected the security framework with our proposed model Intruder Detection System in MANET utilizing Fuzzy Logic. This model is extremely effective for securing against assaults. Our proposed model can locate the protected course and offers in identifying so as to keep some assistance with attacking in MANET. The hub with succession no and limit esteem.

Our proposed calculation has demonstrated awesome change in Hop tally, execution time and throughput. The proposed arrangement does not require any kind of overhead on destination hub or any transitional hub on AODV directing convention. We have likewise utilized fuzzy IF-THEN standards to distinguish and erase assaults. The fuzzy standard is actualized by utilizing reaction time from hub. The calculation will give better answer for lessening of information misfortune over system.

The future extent of work is that the proposed security system may be reached out to shield against different assaults like dim gap assault, bundle dropping assault, asset utilization assault. Keeping in mind the end goal to recognize assaults, different fuzzy principles can be created by applying neuron fuzzy application.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 1, January 2017

REFERENCES

[1] J.P. Anderson, " Computer Security Threat Monitoring and Surveillance," James P. Anderson Co., Tech. Rep., 26 Feb 1980.
[2] Chang-Tien Lu, Arnold P. Boedihardjo, Prajwal Manalwar, "Exploiting Efficient Data Mining Techniques to Enhance Intrusion Detection Systems." in Proceedings of the 2005 IEEE International Conference on Information Reuse and Integration, pp. 512-517.
[3] Anuradha Sharma, Praveen Kumar Misra and Puneet Misra "A Security Measure for Electronic Business Applications" published in International Journal of Computer Applications (0975 – 8887) Volume 102– No.7, September 2014 .
[4] Atul kahate, "Cryptography and Network Security", TMH, New Delhi, 2006, pp. 4-10.
[5] Anuradha Sharma, Puneet Misra, "E-Business Transaction Security: Changing Trends in Database Security- Critical Review", International Journal of Computer Engineering and Technology(IJCET), IAEME, Vol.4, Issue 6, Nov-Dec(2013), pp. 175-180.
[6] Sampada Chavan, Neha Dave and Sanghamitra Mukherjee "Adaptive Neuro-Fuzzy Intrusion Detection Systems" Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04) 0-7695-2108-8/04 $ 20.00 © 2004 IEEE.
[7] Jakob Jonsson and Burton S. Kaliski Jr., " On the Security of RSA Encryption in TLS" published in 2002.
[8] Scott Fluhrer et. al. , " Weaknesses in the Key Scheduling Algorithm of RC4", Springer-Verlag Berlin Heidelberg 2001.
[9] Axelsson, S. (1998). Research in intrusion-detection systems: A survey. Technical Report 98–17, Department of Computer Engineering, Chalmers University of Technology, Goteborg.
[10] Chebrolu, S., Abraham, A., & Thomas, J. P. (2005). Feature deduction and ensemble design of intrusion detection systems. Computers and Security, 24(4), 295–307.
[11] Sourav Sen Gupta et. al., "Dependence in IV-related bytes of RC4 key enhances vulnerabilities in WP" IACR 2014.
[12] Sourav Sen Gupta et. al., " Proof of Empirical RC4 Biases and New Key Correlations", Published in 2012.
[13] Nidhi Singhal, and J.P.S.Raina, " Comparative Analysis of AES and RC4 Algorithms for Better Utilization", International Journal of Computer Trends and Technology- July to Aug Issue 2011.
[14] Pouyan Sepehrdad et. al., " Discovery and Exploitation of New Biases in RC4", Published in 2011.
[15] Souradyuti Paul and Bart Preneel, "A New Weakness in the RC4 Keystream Generator and an Approach to Improve the Security of the Cipher", Published in 2008.
[16] Mykola Karpinskyy et. al., "Reliability of RSA Algorithm And Its Computational Complexity", International Scientific Journal of Computing, 2003, Vol. 2, Issue 3, 119-122.
[17] Priteshkumar Prajapati et. al., " Comparative Analysis of DES, AES, RSA Encryption Algorithms", International Journal of Engineering and Management Research, Volume-4, Issue-1, February-2014.
[18] Lee, W., & Stolfo, S. (2000). A framework for constructing features and models for intrusion detection systems. ACM Transactions on Information Systems and Security, 3(4), 227–261.
[19] Patcha, A., & Park, J.-M. (2007). An overview of anomaly detection techniques: Existing solutions and latest technological trends. Computer Networks, 51(12), 3448–3470.
[20] H. Deng, H. Li, and D. Agrawal, "Routing security in wireless ad hoc networks", IEEE Communications Magazine, Vol. 40, No. 10, Oct 2002.
[21] S. Ki, P. Naldurg and R. Kravets, "Security aware ad hoc routing for wireless networks", in Proceedings of the 2nd ACM Symposium on Mobile Ad Hoc Networking and Computing, Poster Session, pp 299- 302, Long Beach, California, October 2001.
[22]. Boole G., "The Laws of Thought", New York: Dover Books (Reprinted), 1958.
[23]. Zadeh, L. A., "From Circuit Theory To Systems Theory", Proceedings of the Institute of Radio Engineering, Vol.50, 1962.
[24]. Zadeh, L. A., "Fuzzy Sets", Information and Control, Vol. 8, 1965.
[25]. Anuradha Sharma, Puneet Misra "A Security Framework for E-Business Applications "International Journal of Computer Applications (0975 – 8887) Volume 102– No.7, September 2014.
[26] E. J. Derrick, R. W. Tibbs and L. L. Reynolds, "Investigating New Approaches to Data Collection, Management and Analysis for Network Intrusion Detection", ACMSE, Winston-Salem, N. Carolina, USA, (2007) March 23-24, pp. 283-287.
[27]Mahvish Jabeen, Anuradha Sharma," Artificial intelligence Technique Application based Review for Intruder Detection System in MANET", International Journal of Research and Development in Applied Science and Engineering (IJRDASE) ,Volume 9, Issue 2, April 2016