ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 2, February 2017

Intrusion Detection System for MANET using Soft-Computing

[1] Namita Parati [2] Sumalatha Poteti
[1][2] Assistant Professor, Department of Computer Science and Engineering,
Bhoj Reddy Engineering College for Women, Hyderabad.

Abstract: **-- Due to the advancement in wireless technologies, many of new paradigms have opened for communications. Among these technologies, mobile ad hoc networks play a prominent role for providing communication in many areas because of its independent nature of predefined infrastructure. But in terms of security, these networks are more vulnerable than the conventional networks because firewall and gateway based security mechanisms cannot be applied on it. That's why intrusion detection systems are used as keystone in these networks. Many number of intrusion detection systems have been discovered to handle the uncertain activity in mobile ad hoc networks. This paper proposed a novel intrusion detection system based on soft computing techniques for mobile ad hoc networks. The proposed system is based on neuro-fuzzy classifier in binary form to detect, one of vey possible attack, i.e. packet dropping attack in mobile ad hoc networks**

Keywords:— **IDS, MANET, neuro-fuzzy, Security issues, Detection Methods,**

I. INTRODUCTION

Mobile ad hoc networks (MANETs) do not have any pre- existing infrastructure or administrative point as like conventional networks. In MANETs, mobile nodes can communicate freely to each other without the need of predefined infrastructure. This effectiveness and flexibility makes these types of networks attractive for many applications such as military operations, rescue operations, neighborhood area networks, education applications and virtual conferences. Mobile nodes play the role of host as well as routers and also support the multihop communication between the nodes. By the help of routing protocols, mobile nodes can send the data packets to each other in mobile ad hoc networks. 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 Manet's characteristics, Prevention based techniques such as authentication and encryption are not good solution for ad hoc networks to eliminate security threats because prevention based techniques cannot protect against mobile nodes which contain the private keys. So that Intrusion detection system is an essential part of security for MANETs. It is very effective for detecting the intrusions and usually used to complement for other security mechanism. That's why Intrusion detection system (IDS) is known as the second wall of defense for any survivable network security [3]. There are some groups which works together to enhance the functioning of mobile ad hoc networks (MANETs). IETF constituted the mobile ad hoc networks working group in 1997. Soft computing is viewed as an emerging method for computing which present the notable potentiality of human mind to understand and learn in the situation of imprecision and uncertainty [25]. Generally, soft computing admits three main components such as neural networks, fuzzy logic and genetic algorithms.

Many of the soft computing techniques have proved their applicability in the field of intrusion detection in wired networks. Recently, many of the researchers are emphasizing on soft computing techniques for intrusion detection in MANETs so that some of the IDSs based on soft computing techniques have been developed for MANETs .

II. INTRUSION DETECTION SYSTEM

IDS is the most used and developed system that can detect attack. Intellectual IDS can perform as a dynamic defensive system which is capable of adapting dynamically changing traffic pattern. Many researchers have worked on Intrusion Detection System to give the preeminent output through their system. It can be more categorized where researchers have mentioned the IDS

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 2, February 2017

system with the merging of the artificial neural network and clustering techniques [1, 11, 12]. They showed the performance with other well-known methods such as decision tree, naïve byes, in terms of detection precision and detection stability. They mainly used the clustering techniques to generate different training subsets. And based on these subsets, different ANN modules are trained to formulate different base models. Finally they used an aggregation model to aggregate the result. They reduced the complexity of each of the sub training set and correspondingly they increase the performance of the detection. Moreover, many of them proposed a survey report on where they have cited the detection of accuracy from IDS using only the artificial neural network classifier [13]. Using different ANN functions they disclosed the accuracy system for the intrusion detection system that will detect on which technique of the ANN function will give the highest accuracy rate.

The basic functionality of IDS depends only on three main modules such as data collection, detection and response modules. The data collection module is responsible for collecting data from various data sources such as system audit data, network traffic data, etc. Detection module is responsible for analysis of collected data. While detecting intrusions if detection module detects any suspicious activity in the network then it initiates response by the response module. There are three main detection techniques presented in the literature such as misuse based, anomaly based and specification based techniques. The first technique, misuse- based detection systems such as IDIOT [6] and STAT [7] detect the intrusions on the behalf of predefined attack signature. The disadvantage of this technique is that it cannot detect new attacks but has low false positive rate so that it is generally used by the commercial purpose based IDSs. Second intrusion detection technique is anomaly-based detection technique e.g. IDES [8]. It detects the intrusion on bases of normal behaviour of the system. Defining the normal behavior of the system is a very challenging task because behavior of system can be changed time to time. This technique can detect the new or unknown attacks but with high false positive rates. The third technique is specification - based intrusion detection [9]. In this detection method, first specified the set of constraints on a particular protocol or program and then detect the intrusions at run time violation of these specifications. The main problem with this technique is that it takes more time for defining the specification that's why it is a time consuming technique [10]. On the bases of the audit data, Intrusion detection system can be host based and network based. Host based IDS collect the audit data from operating system at a particular host and network based intrusion detection system collects audit data from host as well as trace the network traffic for any type of suspicious activity.

Normally there are three basic types of IDS architecture in literature: Stand-alone intrusion detection systems - In this type of intrusion detection system architecture, an IDS run independently on each node in the network; Distributed and Cooperative intrusion detection systems - In this architecture all nodes have IDS agents so that each node can take part in intrusion detection locally and depend on cooperativeness between the nodes it can be made decision globally. This architecture dependent IDS are able to make two types of decision i.e. collaborative and independent. In collaborative decision, all nodes take part actively to make decision but in case of independent decision some particular nodes are responsible for making decision. Hierarchical Intrusion Detection Systems - This type of IDS architecture is an extended form of distributed and cooperative IDS architecture in which whole network is divided into clusters. Each cluster has cluster head which has more responsibility than the other node members in the cluster [10] [11]. There are many number of IDSs have been proposed in MANETs.

III. MANET

A mobile ad hoc network [1, 2, 3, 4, 5] is a self-configuring infrastructureless network consisting of mobile nodes (Laptop, Personal Digital Assistants (PDAs) and wireless phones) with routing capabilities where each node operate both as host as well as router to forward the packets to each other, with the characteristics of self-organization and self-configuration which enable it to form a new network quickly as shown in fig.1. MANET has following distinct characteristics:

- Weaker in Security
- Device size limitation

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 2, February 2017

- Battery life
- Dynamic topology
- Bandwidth and slower data transfer rate

Apart from these limitation MANETs has many extensive application like: Military communication and operations, Automated battlefields, Search and rescue operations, Disaster recovery, Policing and firefighting.

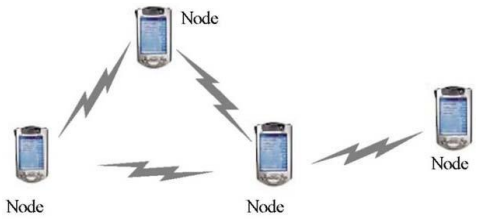

Fig. 1: Mobile Ad Hoc Network.

MANETs are highly vulnerable to several types of attacks, due to its characteristics: dynamic topology, infrastructure less, vulnerable of channels, vulnerable of Nodes and lack of strong line of defense. These mobile nodes can be malicious or selfish. Therefore, deploying security in mobile ad hoc networks is important [6].

IV. ATTACKES IN MANET

In MANETs, one of very commonly used routing protocol is ad hoc on demand distance vector (AODV) (Perkins and Royer, 1999). As an exemplar, AODV protocol is used in this research. This section discussed attacks on AODV that is considered in this research. A detailed description of threats on MANETs is given in Sen et al. (2010).

A. Packet Dropping Attack:

In PDA scenario, malicious nodes drop all the incoming data packets for disrupting the network services (Sen et al., 2010). For dropping the data packets, malicious nodes need to be a part of routing path so malicious nodes have little reason to drop control packets such as RREQ, RREP and RERR that are used in route discovery and route maintenance phases of AODV. In this research, control packets are not dropped by the malicious nodes. Dropping data packets can be prevented the end to end communication between the mobile nodes and also reduced the network performance due to the retransmission of data packets or discovery of new routes. During the simulation of PDA, malicious nodes continuously drop the data packets at each 1 sec interval. As in MANETs, mobility is the major cause to lose the data packet on AODV (Lu et al., 2003). That is why this research concentrates to differentiate the packet dropping due to the mobility from the packet dropping due to malicious nodes in MANETs.

B. Sleep deprivation attack through malicious RREQ flooding (SDMF)

The sleep deprivation attack (Pirrete and Brooks, 2006) is a kind of denial of service attack. During this attack, in the route discovery phase of AODV an attacker node broadcasts the route request (RREQ) packets to their neighbor with a destination IP address that exists in the network address range but is actually not present in network. Thus, all presented nodes in the network will compel to forward these RREQ packets because no one is having the route for this fake destination address in the network. The main aim of SDMF attack is to consume the battery power of nodes and discard them to perform the network operations.

C. Fuzzy and Neuro-fuzzy

Fuzzy logic is one of very important component of soft computing that can able to deal with uncertainty and impreciseness derived from human logical thinking or reasoning. Fuzzy logic is able to handle the multi valued logic of fuzzy set theory between the ranges of 0 to 1 and it gives the decisions in degrees form rather than yes or no terms [23]. IF-then- else based fuzzy rules can specify the every situation in the network for detecting the intrusions or attacks. Fuzzy inference system (FIS) is based on fuzzy rules for taking the decisions towards fuzzy reason.

All Rights Reserved © 2016 IJERCSE

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 2, February 2017

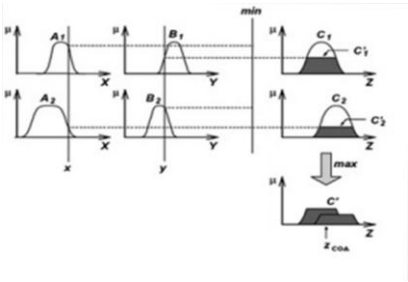

Fig. 2: The Mamdani fuzzy interference system (MFIS)

Mamdani FIS is shown in Fig 2. This is used de- fuzzification module that converts the fuzzy values to crisp values in terms of output. But, it is time consuming procedure. Takagi et al. suggested an approach to render the fuzzy rules from dataset [8] and is depicted in Fig 3(a). It is more efficient towards computation and also more suitable with adaptive techniques. Here, defuzzification is done by using weighted average.

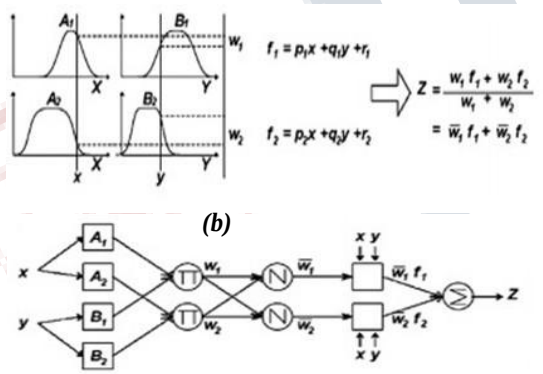

Fig. 3: (a) Presents the Sugeno model fuzzy reasoning (b) Equivalent ANFIS structure

There are several hybrids of soft computing approaches, where hybrid of neural and fuzzy has very popularity in many domains so that a very popular method has been proposed by Jang et al., which is known as ANFIS (Adaptive neuro-fuzzy inference system) [8].

In any modelling situation where nobody can't discover and recognize the membership functions and parameters linked with member functions for the large or vast data set. In this situation ANFIS is useful. It suggests a procedure for fuzzy modelling in respect of learning the information from a given dataset for computing the parameters of membership functions that permit the associated FIS to track or handle in best way of given input and output data. The membership functions related parameters will alter according to the procedure of learning. ANFIS can employ back propagation algorithm or aggregation of back propagation algorithm and least square estimation for the estimation of parameters related with membership functions. Fig 3(b) describes the ANFIS architecture [8]. This paper utilized the subtractive clustering method for determining the initial number of fuzzy rules and membership functions. However, ANFIS is applied for further fine tuning of these functions. Subtractive clustering [6] is quick, single pass algorithm for computing the clusters and cluster centers from a given dataset. Subtractive clustering is an extension of mountain clustering method that is indicated by Yager in [24]. According to the cluster information which is received by this algorithm is utilized to discover the initial rules and membership functions that are responsible to form the FIS.

V. NEED OF FUZZY BASED INTRUSION DETECTION SYSTEMS

Fuzzy logic is used in intrusion detection since 90's because it is able to deal with uncertainty and complexity which is derived from human reasoning [12]. By the help of fuzzy variables or linguistic terms, intrusion detection features can be viewed easily and decision of normal and abnormal activity in the network are based on its fuzziness nature that can identify the degree of maliciousness of a node instead of yes or no conditions [13] [14]. IF-then-else based fuzzy rules are used to define all situations in the network for identifying the attacks or intrusions. The fuzzy rule based system is known as fuzzy interference system (FIS) that is responsible to take decisions. Many types of fuzzy interference systems are proposed in the literature [15].

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 2, February 2017

Proposed Architecture

Data mining is frequently used to designate the process of extracting useful information from large databases. In this view, the term knowledge discovery in databases (KDD) is used to denote the process of extracting useful knowledge from large data sets using data mining as a particular step. Specifically, the data mining step applies so-called data mining techniques to extract patterns from the data. Additionally, it is preceded and followed by other KDD steps, which ensure that the extracted patterns actually correspond to Data Mining for Intrusion Detection useful knowledge. Here, we broadly outline some of the most basic KDD steps:

1. Understanding the application domain: First is developing an understanding of the application domain, the relevant background knowledge, and the specific goals of the KDD endeavor.
2. Data integration and selection: Second is the integration of multiple (potentially heterogeneous) data sources and the selection of the subset of data that is relevant to the analysis task.
3. Data mining: Third is the application of specific algorithms for extracting patterns from data.
4. Pattern evaluation: Fourth is the interpretation and validation of the discovered patterns. The goal of this step is to guarantee that actual knowledge is being discovered.
5. Knowledge representation: This step involves documenting and using the discovered knowledge.

Data mining techniques can be differentiated by their different model functions and representation, preference criterion, and algorithms [25].The main function of the model that we are interested in is classification, as normal, or malicious, or as a particular type of attack [26][27].

It is a fairly recent topic in computer science but utilizes many older computational techniques from statistics, information retrieval, machine learning and pattern recognition.

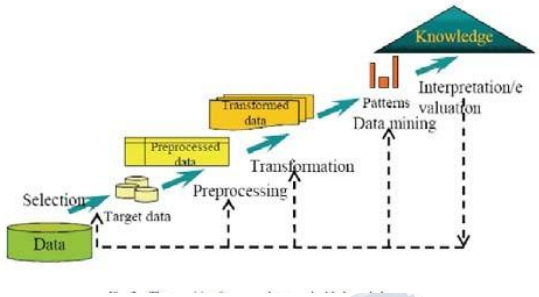

Fig.4: KDD Process [32].

Here are a few specific things that data mining might contribute to an intrusion detection project [22, 23]:

- Remove normal activity from alarm data to allow analysts to focus on real attacks
- Identify false alarm generators and ”bad” sensor signatures
- Find anomalous activity that uncovers a real attack
- Identify long, ongoing patterns (different IP address, same activity)

To accomplish these tasks, data miners employ one or more of the following techniques:

- Data summarization with statistics, including finding outliers
- Visualization: presenting a graphical summary of the data
- Clustering of the data into natural categories
- Association rule discovery: defining normal activity and enabling the discovery of anomalies
- Classification: predicting the category to which a particular record belongs

In our proposed Host based architecture we have added some additional modules (Expert System, Knowledge Expresser, Data Miner and Interference Engine) to enhance the capability of Classifier module as Data mining attempts to extract implicit, previously unknown, and potentially useful information from data, so that it can detect the attacks with minimal amount of time and provide useful information to the ADM and MDM module, to increase the effectiveness and scalability of this proposed architecture. There is one module previously mined data module in the architecture that access the previous stored signatures

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 2, February 2017

of different attacks and behavior of abnormal activities at the node, so that it can detect abnormal activity with minimum amount of time. The other modules Expert System, Knowledge Expresser, Data Miner and Interference Engine are used are to expert the system with proper information to classify the abnormal and normal activities with minimum amount of time. The graphical representation is given in Fig. 4.

The advantage of this approach is that it has expert system, Knowledge Expresser, Data Miner and Interference Engine. This means that the chances of one system catching intrusions missed by the other will increase. The below architecture takes care to ensure that the IDS running on each host does not drain resources more than necessary. Here all the modules work collectively at the same time to provide the necessary support for the intrusion detection in the network

We have divided our architecture into following three main modules:

- Audit Data Collection Module
- Intrusion Detection Module
- Response Module

Audit Data Collection Module: This module is to collect the audit records.

i. Host Audit Records Collection (HARC): In this sub module, each operation of a host should be recorded to check that whether an intrusion is taking place.

***Intrusion Detection Module*:** This module play very important role to analyze the activities to determine that any of the activity is violating the security rules on the host after taking the audit data record from Audit Data Collection Module. Once an IDS determines that an unusual activity or an activity that is known to be an attack occurs, it then generates an alert to the response module.

i. Audit Data Preprocessor (ADP): This refers to one or more individual preprocessors used by IDS to the collect audit data and to quantify and transform into the appropriate data format for the subsequent module.

ii. Classifier Module (CM): In this module we can employ classification algorithms in order to perform intrusion detection in MANETs by mapping a data item into one of several predefined categories.

iii. Data Miner (DM): Data Mining is a branch of computer science, is the process of extracting patterns from large data sets by combining methods from statistics and artificial intelligence with database management.

iv. Knowledge Expresser (KE): Knowledge Expresser from Classsifier Module, in its most fundamental form, is to extract interesting, nontrivial, implicit, previously unknown and potentially useful information from Classifier Module.

v. Expert Systems (ES): These systems are modeled in such a way as to separate the rule matching phase from the action phase.

vi. Inference Engine (IE): Inference engine is a computer program that attempt to infer or derive a deep insights or answers from the knowledge base.

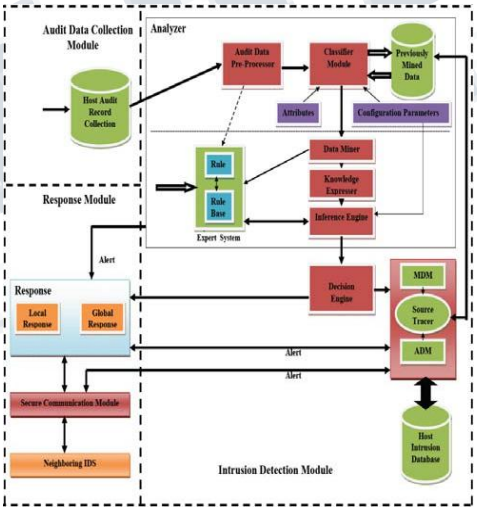

Fig. 5 : Intrusion Detection System for Mobile Ad Hoc Network: Proposed Architecture

Response Module: If an intrusion is detected by the Detection Engine then the Response Engine is activated by issuing the alerts from Intrusion Detection Module. The Response Engine is responsible for sending a local and a global alarm in order to notify the nodes of the mobile ad hoc network about the incident of intrusion.

This architecture is concerned with what activity is happening on each host. This architecture is ideal if it is able to detect actions and other activities with high confidence. In order to function properly, IDS has to be

installed on every node in the network to processes and perform analysis on the audit data gathered locally, at the expense of the already limited resources on the hosts.

VI. CONCLUSION

In this paper, we have analyzed fuzzy based intrusion detection systems which have been proposed in literature for Manets. We have analyzed the working style of proposed fuzzy based IDSs and reached on decision that still we do not have any promising solution for this dynamic environment because most of proposed fuzzy based IDSs emphasized on very limited features for data collection towards detection of very specific range of attacks. Hence, MANETs are required for more concentration of researchers. It can be a fastest growing area for future research in terms of detection techniques, response mechanism and selection of node features for data collection. In future, we are concentrating to develop a new intrusion detection system that can be used to classify the normal and malicious activities in the network.

REFERENCES

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

[2]. A. Hasti, "Study of Impact of Mobile AdHoc Networking and its Future Applications", BIJIT – 2012; January - June, 2012; Vol. 4 No. 1; ISSN 0973 – 5658.

[3]. Y. Zhang and W. Lee., " Intrusion detection in wireless ad hoc networks" , In Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom'00), pages 275-283, 2000.

[4]. IETF Mobile Ad-Hoc Networks Working Group (MANET), IETF

[5]. R. Heady, G. Luger, A. Maccabe, and M. Servilla, "The architecture of a network level intrusion detection system" Technical report, Computer Science Department, University of New Mexico, August 1990.

[6]. S. Kumar and E. H. Spafford, "A software architecture to support misuse intrusion detection" In Proceedings of the 18th national Information Security Conference, pages 194- 204, 1995.

[7]. K. Ilgun, R. A. Kemmerer, and P.A. Porras, "State transition Analysis: A rule- based intrusion detection approach", IEEE Transactions on software Engineering, Vol. 21 No. 3:181-199, March 1995.

[8]. T.Lunt, A. Tamaru, F. Gilham, R. Jagannathan, P.Neumann, H. Javitz, A. Valdes, and T.Garvey, "A real time intrusion detection expert system (IDES) final technical report.

[9]. Uppuluri P, Sekar R, "Experiences with Specification- based Intrusion Detection", In Proc of the 4th Int Symp on Recent Adv in Intrusion Detection , pp. 172-189.

[10]. S. Sen, J.A. Clark - Guide to Wireless Ad Hoc Networks; In: Chapter 17-Intrusion Detection in Mobile Ad Hoc Networks-Springer, 2008.

[11]. P. Brutch and C. Ko, "Challenges in Intrusion Detection for Wireless Ad-hoc Networks," In Proceedings of 2003 Symposium on Applications and the Internet Workshop, pp. 368-373, January 2003.

[12]. B. Shanmugam and N. B. Idris, "Anomaly Intrusion Detection based on Fuzzy Logic and Data Mining", In Proceedings of the Postgraduate Annual Research Seminar, Malaysia 2006.

[13]. M. Wahengbam and N. Marchang, "Intrusion detection in manet using fuzzy logic", 3rd IEEE National Conference on Emerging Trends and Applications in Computer Science (NCETACS), ISBN: 978-1-4577-0749-0, pp. 189 – 192, Shillong, 30-31 March 2012.

[14]. Verma, A. K., R. Anil, and Om Prakash Jain. "Fuzzy Logic Based Revised Defect Rating for

All Rights Reserved © 2016 IJERCSE

Software Lifecycle Performance Prediction Using GMR."Bharati Vidyapeeth's Institute of Computer Applications and Management, 2009.

[15]. J. S. R. Jang, C. T. Sun and E. Mizutani – Neuro-Fuzzy and Soft Computing - A computational Approach to Learning and Machine Intelligence; First Edition; Prentice Hall of India, 1997.

[16]. Watkins, Damian. "Tactical manet attack detection based on fuzzy sets using agent communication." In 24th Army Science Conference, Orlando, FL, 2005.

[17]. S. Sujatha, P. Vivekanandan, A. Kannan, "Fuzzy logic controller based intrusion handling system for mobile ad hoc networks", Asian Journal of Information Technology, ISSN: 1682- 3915, pp.175-182, 2008.

[18]. A. Visconti, H. Tahayori, " A Biologically – Inspired type-2 fuzzy set based algorithm for detecting misbehaving nodes in ad hoc networks" , International Journal for Infonomics, Vol.3, No.2, pp. 270-277, June 2010.

[19]. R. Vijayan V. Mareeswari and K. Ramakrishna, "Energy based trust solution for detecting selfish nodes in manet using fuzzy logic", International Journal of research and reviews in computer science , Vo. 2, No. 3, pp. 647-652, June 2011.

[20]. Kulbhushan and Jagpreet Singh, "Fuzzy logic based intrusion detection system against blackhole attack AODV in manet", IJCA Special issue on "Network Security and Cryptography" Vol. NSC, No. 2 pp. 28-35, December, 2011.

[21]. M. Wahengbam and N. Marchang, "Intrusion detection in manet using fuzzy logic", 3rd IEEE National Conference on Emerging Trends and Applications in Computer Science.

[23] W. Lee, S.J. Stolfo, K.W. Mok. "A Data Mining Framework for Building Intrusion Detection Models". IEEE Symposium on Security and Privacy (Oakland, California), 1999

[24] G. Florez, S.M. Bridges, and R.B. Vaughn, "An Improved Algorithm for Fuzzy Data Mining for Intrusion Detection". The North American Fuzzy Information Processing Society Conference, NewOrleans, LA, 2002.

[25] Fayyad, U. M., G. Piatetsky-Shapiro, and P. Smyth,"The KDD process for extracting useful knowledge from volumes of data,"

[26] Ghosh, A. K., A. Schwartzbard, and M. Schatz,"Learning program behavior profiles for intrusion detection.

[27] Kumar, S.,"Classification and Detection of Computer Intrusion", PhD. thesis, 1995, Purdue Univ., West Lafayette, IN.