International Journal of Research and Development in Applied Science and Engineering (IJRDASE)
ISSN: 2454-6844

Artificial intelligence Technique Application based Review for Intruder Detection System in MANET

Mahvish Jabeen
Computer Science & Engineering,
Amity University, Lucknow, India
jabeen.mahvish68@gmail.com

Anuradha Sharma
Computer Science & Engineering, ASET
Amity University, Lucknow, India
amisra@lko.amity.edu

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 investigation of existing intrusion detection task and gives a review on flow patterns in intrusion detection together with a study on technologies implemented by a few researchers in this research area.

Keywords: MANET, A.I. Techniques, Malicious Node, Network Attacks, Network Intrusion.

1. Introduction:

Intrusion detection System (IDS) is a type of security management system for computers and networks [11]. An intrusion detection system (IDS) 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 the association) 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 [12]. Data mining techniques can be used to detect intrusions. Applications of data mining have presented a collection of research efforts on the use of data mining in computer security. In the context of security of the data we are looking for the information whether an information security breach has been experienced [13]. This data could be collected in the perspective of discovering attacks or intrusions that aim to break the privacy and security of services, information in a system or alternatively, in the context of discovering evidence left in a computer system as part of criminal activity. There are four major categories of networking attacks: Denial of Service, Probing, User to Root and Remote to Local.

Intrusion detection system is the area where data mining concentrate heavily. There are two fold reasons for this first an IDS is very common and very popular and extremely critical activity. Second, large volume of the data on the network is dealing so this is an ideal condition for the data mining to use it. The data mining technology has the enormous benefits in the data extracting attributes and the rule, so it is significant to use data mining methods in the intrusion detection [14]. A significant problem of IDS is how to efficiently divide the normal behavior and the abnormal behavior from a huge number of raw information's attributes, and how to effectively generate automatic intrusion rules following composed raw data of the network. To accomplish this, different data mining methods must be studied, like classification, correlation analysis of data mining methods and so on [14]. The ever rising new intrusion or attacks type poses severe difficulties for their detection. The human labeling of the accessible network audit information instances is generally tedious, expensive as well as time consuming. This paper focuses on study of existing intrusion detection task.

2. MANET

A Mobile Ad hoc Network (MANET) is a collection of wireless mobile nodes forming a temporary network without any established infrastructure or centralized authority. In a MANET, the nodes are free to move about and organize themselves into a network. MANET does not require any fixed infrastructure such as base stations; therefore, it is an attractive networking option for connecting mobile devices quickly and spontaneously. The below figure shows a sample MANET [2]

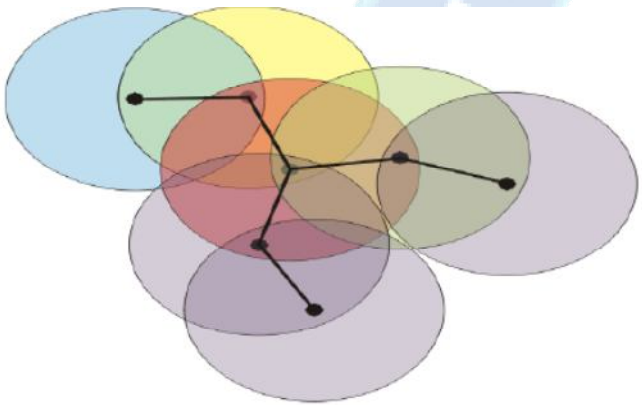

Fig. 1 Mobile Ad Hoc Networks

The characteristics of MANET are identified as follows [3]

Autonomous terminal: Each node in MANET is autonomous and acts both, as router and host.

Distributed: MANET is distributed in its operation and functionalities, such as routing, host configuration and security.

Multi-hop routing: If the source and destination of a message is out of the range of one node, a multi-hop routing is created.

Dynamic network topology: Nodes are mobile and can join or leave the network at any time; therefore, the topology is dynamic.

Fluctuating link bandwidth: The stability, capacity and reliability of a wireless link are always inferior to wired links.

Thin terminal: The mobile nodes are often light weight, with less powerful CPU, memory and power.

Spontaneous and mobile: Minimum intervention is needed in configuration of the network. The routing protocol should be an adapted one that allows users to communicate in the network. It should also support security. Some existing security technologies for wired network, such as encryption, can be utilized in MANET. However, because of the mobile and ad hoc nature of MANET, the applications of MANET are limited. Other technologies, such as firewall, do not apply to MANET, because of the lack of a centralized authority. Same as the wired network, MANET faces the security threat such as passive eavesdropping, spoofing, and denial of service. At the same time, because of its ad hoc nature, it suffers from more security threats. Threats to MANET can be classified into two groups:

Vulnerabilities accentuated by the ad hoc nature: The topology of MANET is mainly determined by geographical locations and by radio range of the nodes. Therefore, it does not have a clearly defined physical boundary. In wired network, a centralized firewall can implement the access-control. However, in MANET, access-control cannot be other attacks, such as denial of service (DOS) still threat MANET, even worse than for wired network, since the routing and auto configuration framework of MANET are more vulnerable to such attack.

Vulnerabilities specific to the ad hoc nature: The routing and auto configuration mechanism of MANET introduces opportunity for more attack because in both mechanisms, all nodes have full trust between each other

3. Related Work:

3.1 Intrusion Detection using Fuzzy:

Yogita Danane, and Thaksen Parvat, (2015) [1] 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. IDS is a product that screens the PC arrange and identifies the suspicious exercises that happen in the frameworks or system. The procedure of interruption identification incorporates recognizing interruption. Interruption is a suspicious action endeavored by the aggressor. 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. The KDD99 dataset is a benchmark dataset that analysts use in different system security explores. Hereditary calculation incorporates an advancement and gathering that uses a chromosome like information structure and add to the chromosomes utilizing determination, hybrid and change administrators. Fluffy guideline sorts system assault information.

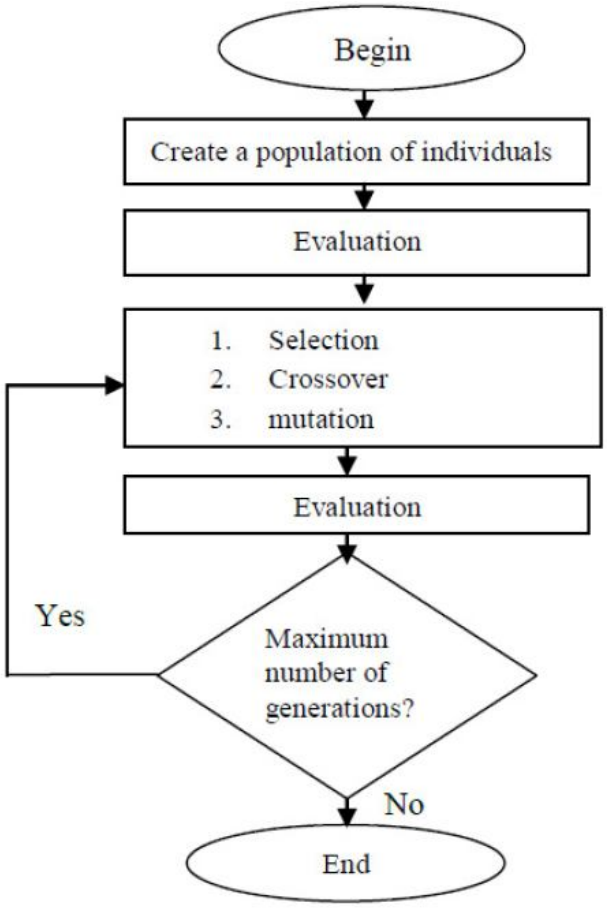

Fig. 2 Steps in Fuzzy Genetic algorithm

Salma Elhag, Alberto Fernández, Abdullah Bawakid, Saleh Alshomrani, and Francisco Herrera (2015) [2], 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. Then again, various malignant clients break down the vulnerabilities of these frameworks keeping in mind the end goal to increase unapproved access or to trade off the nature of administration. Thus, Intrusion Detection Systems have been outlined keeping in mind the end goal to screen the framework and trigger alarms at whatever point they discovered a suspicious occasion. Ideal Intrusion Detection Systems are those that accomplish a high assault discovery rate together with a little number of false cautions. Be that as it may, digital assaults present a wide range of qualities which make them difficult to be appropriately distinguished by straightforward factual systems. As indicated by this, Data Mining methods, and particularly those situated in Computational Intelligence, have been utilized for actualizing strong and exactness Intrusion Detection Systems. 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 benefits of utilizing this methodology are twofold: to start with, the utilization of fluffy sets, and particularly semantic marks, empowers a smoother fringe between the ideas, and permits a higher interpretability of the standard set. Second, the separation and-vanquish learning plan, in which we differentiate all conceivable pair of classes with points, enhances the accuracy for the uncommon assault occasions, as it gets a superior distinguishableness between an "ordinary movement" and the diverse assault sorts. The integrity of our technique is upheld by method for a complete trial study, in which we differentiate the nature of our outcomes versus the best in class of Genetic Fuzzy Systems for interruption location and the C4.5 choice tree.

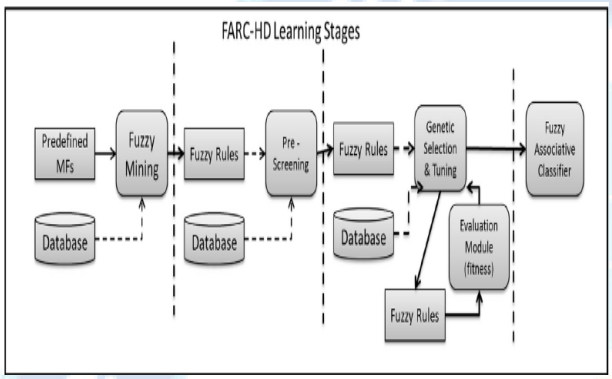

Fig. 3. Learning stages for the FARC-HD algorithm.

The work entitled "Fuzzy Logic based Intruder Detection System in Mobile Adhoc Network" by **Shadab Siddiqui, P. M. Khan and Muhammad Usman Khan (2014) [3],** is an approach to detect malicious nodes by applying fuzzy logic in Mobile ad-hoc networks. Security is a major concern in various scenarios of adhoc sensor network. Detection of malicious nodes forms an essential part of an approach to security. The proposed work uses fuzzy logic to identify the attack and malicious behavior of nodes. The proposed work will identify the attack over the network as well as provide the solution to reduce the execution time over the network. 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 results will show great improvement of AODV with fuzzy logic over the previous algorithm. The proposed scheme is implemented using Matlab & its results show its effectiveness.

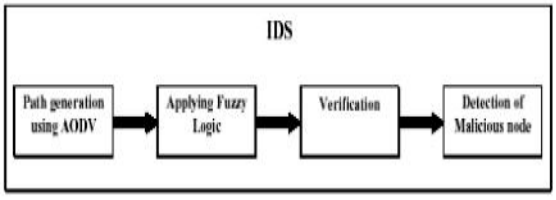

Fig. 4. Fuzzy based IDS

B.Ben Sujitha, R.Roja Ramani, and Parameswari (2012), [4] according to them system security is of essential concerned now days for huge associations. The interruption discovery frameworks (IDS) are getting to be vital for viable security against assaults that are continually changing in extent and multifaceted nature. With information trustworthiness, secrecy and accessibility, they must be solid, simple to oversee and with low support cost. Different adjustments are being connected to IDS frequently to distinguish new assaults and handle them. This work proposes a fluffy hereditary calculation (FGA) for interruption location. The FGA framework is a fluffy classifier, whose learning base is displayed as a fluffy govern, for example, "if-then" and enhanced by a hereditary calculation. The strategy is tried on the benchmark KDD'99 interruption dataset and contrasted and other existing strategies accessible in the writing. The outcomes are empowering and exhibit the advantages of the proposed approach.

Devendra K. Tayal, Amita Jain and Vinita Gupta (2010) [5], in their work an exertion has been made to add to a fluffy based model to think about the effect of different clamor components on Sleep unsettling influence and Health. We altogether overview the current writing and distinguish the inadequacies in the current models in this field. We then distinguish different commotion elements which can have the huge effect on Sleep and wellbeing. The MIMO Expert framework created in this work gives rest aggravation, wellbeing condition in the morning and wellbeing as yield variables and clamor level, short commotion span, long clamor length of time, age and Type of commotion as the data variables. Fitting fuzzification and defuzzification techniques have been utilized and the usage as a part of MATALAB 7.0.1 has been finished. It has been built up from work of different specialists that impact of important commotion like tunes and talks influence rest and wellbeing conditions severely than aimless clamor like railroad clamor, roadside commotion. Essentially other info variables influence rest and wellbeing condition. These variables have been concentrated on in this work. The commotion level and length of time of clamor, which are likewise the conspicuous components in choosing impact on listening to yield variable have been talked about, for e.g. a commotion of low level does not have noticeable influence on person starting abnormal state of clamors.

Bharanidharan Shanmugam and Norbik Bashah Idris, (2009) [6] according to them as of now accessible interruption identification frameworks concentrate mostly on deciding strange framework occasions in circulated systems utilizing mark based methodology. Because of its confinement of discovering novel assaults, we propose a mixture model in light of enhanced fluffy and information mining methods, which can recognize both abuse and peculiarity assaults. The point of our examination is to lessen the measure of information held for preparing i.e., property determination procedure furthermore to enhance the location rate of the current IDS utilizing information mining method. We then utilize enhanced Kuok fluffy information mining calculation, which thus an adjusted rendition of APRIORI calculation, for actualizing fluffy

standards, which permits us to develop if-then decides that reflect normal methods for depicting security assaults. We connected fluffy deduction motor utilizing mamdani derivation component with three variable inputs for quicker choice making. The proposed model has been tried and benchmarked against DARPA 1999 information set for its proficiency furthermore tried against the "live" systems administration environment inside the grounds and the outcomes has been talked about.

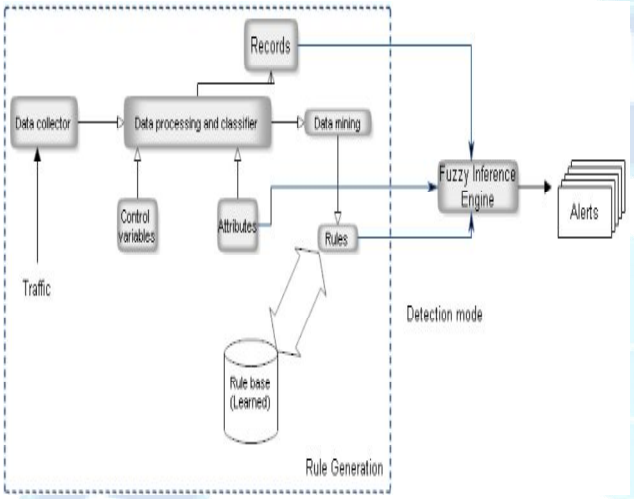

Fig. 5. IIDS framework.

3.2 Black Hole Attacks in MANET:

Elmar Gerhards-Padilla, et.al. (2007), [7], according to them Dark Hole Attacks are a genuine danger to correspondence in strategic MANETs. In this work we exhibit TOGBAD another brought together approach, utilizing topology charts to distinguish hubs endeavoring to make a dark gap. We utilize entrenched strategies to pick up learning about the system topology and utilize this information to perform credibility checks of the steering data spread by the hubs in the system. We consider a hub producing fake directing data as malignant. In this manner, we trigger an alert if the believability check comes up short. Moreover, we present promising first reproduction results. With our new approach, it is conceivable to as of now recognize the endeavor to make a dark opening before the real effect happens (Fig. 6).

This work proposed by **Zaheeruddin, Vinod K. Jain, and Guru V. Singh (2006)** [8], 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. Disturbance, in the present model, is considered as a component of clamor level, its length of time of event, and the financial status of a man. The model has been actualized on the Fuzzy Logic Toolbox of MATLAB, utilizing both Mamdani and Sugeno procedures. The consequences of the model are pertinent to the urban regions of India (Fig. 7).

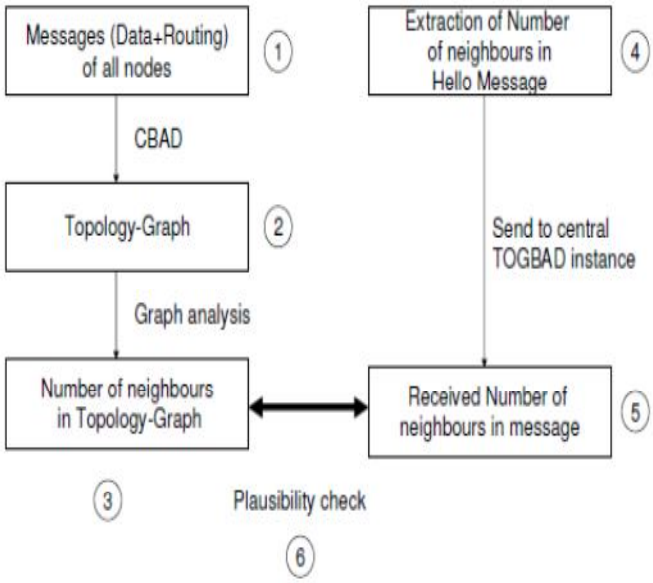

Fig. 6. Algorithm of TOGBAD

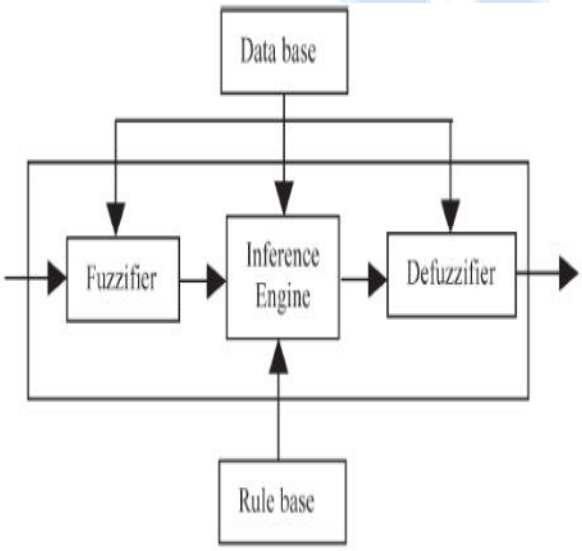

Fig 7. Structure of a fuzzy rule-based system.

3.3 Survivability Model for Wireless Sensor Network:

A Mobile specially appointed system (MANET) has turned into an imperative innovation the security issue, particularly, interruption discovery strategy examination has pulled in numerous individuals' exertion. MANET is more helpless than wired system and endures interruption like wired system. This work researched some interruption identification systems utilizing machine learning and proposed by **X. Wang, T. Lin and J. Wong, (2005) [9],** a profile based neighbor checking interruption location strategy. Further examination demonstrates that the elements gathered by every hub are an excess of for remote gadgets with constrained limit. We apply Markov Blanket calculation to the component determination of the interruption location technique. Exploratory studies have demonstrated that Markov Blanket calculation can diminish the quantity of components significantly with fundamentally the same location rate.

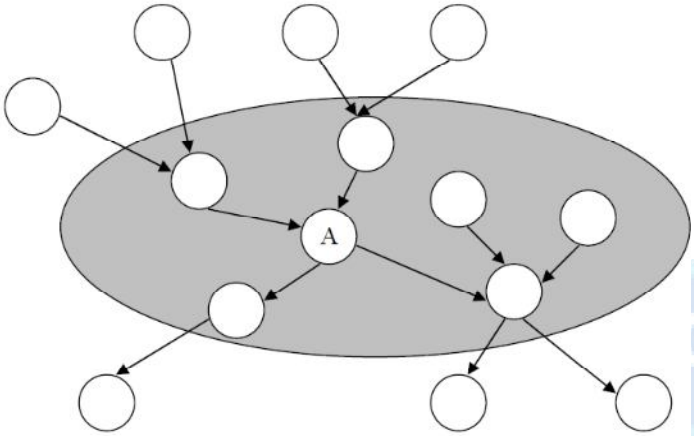

Fig. 8. the Markov Blanket of Node A

3.4 Intrusion Detection over MANET:

Sampada Chavan, Neha Dave and Sanghamitra Mukherjee (2004) [10], 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. At that point a mark design database is built utilizing convention investigation and Neuro-Fuzzy learning strategy. Utilizing 1998 DARPA Intrusion Detection Evaluation Data and TCP dump crude information, the investigations are sent and talked about.

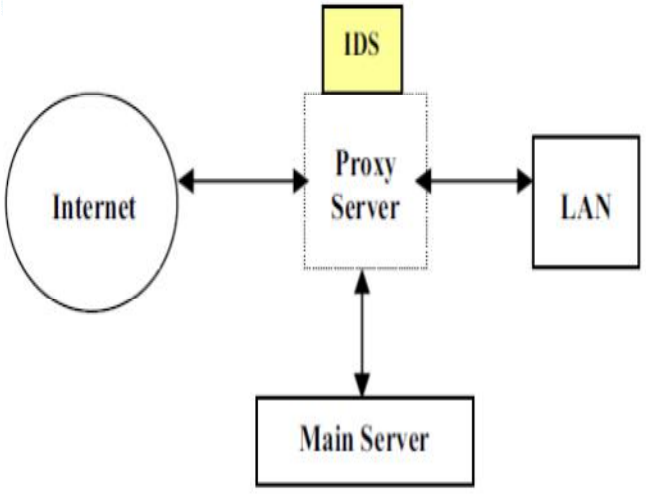

Fig. 9. Architecture of the proposed framework

4. Conclusion:

In this article a review on the recent developments is performed for the improvement of intrusion detection system by overcoming the network attacks due to the malicious activity of the nodes. We have discussed about various methodologies applied in last ten years in the research area of intrusion detection system to compare the performance and efficient usage of these technologies. It has been observed that the recent methodologies are incorporating latest A.I technique like fuzzy logic, neural network ,SVM etc. For full filing the growing demand of network detection speed and accuracy.Hybrid mechanism like neuro fuzzy methods proved to be outperforming in inteusion detection in the MANET systems.In future we can expect the involvement of optimization technique like GA and PSO based evolutionary algorithms in developing improved detection rules.

References:

[1] Yogita Danane, and Thaksen Parvat, "Intrusion Detection System using Fuzzy Genetic Algorithm", 2015 International Conference on Pervasive Computing (ICPC).

[2] Salma Elhag, Alberto Fernández, Abdullah Bawakid, Saleh Alshomrani, and Francisco Herrera, " On the combination of genetic fuzzy systems and pairwise learning for improving detection rates on Intrusion Detection Systems" Expert Systems with Applications 42 (2015) 193–202.

[3] Shadab Siddiqui, P. M. Khan and Muhammad Usman Khan, "Fuzzy Logic Based Intruder Detection System in Mobile Adhoc Network" BIJIT - BVICAM's International Journal of Information Technology Bharati Vidyapeeth's Institute of Computer Applications and Management (BVICAM), New Delhi (INDIA) (2014)

[4] B.Ben Sujitha1, R.Roja Ramani2, Parameswari: Intrusion Detection System using Fuzzy Genetic Approach; International Journal of Advanced Research in Computer and Communication Engineering, Vol. 1, Issue 10, December 2012.

[5] Devendra K. Tayal, Amita Jain and Vinita Gupta "Fuzzy Expert System for Noise Induced Sleep Disturbance and Health Effects" in BIJIT Issue3: (Jan-June 2010 Vol2 No1).

[6] Bharanidharan Shanmugam and Norbik Bashah Idris,"Improved Intrusion Detection System using Fuzzy Logic for Detecting Anamoly and Misuse type of Attacks" 2009 International Conference of Soft Computing and Pattern Recognition.

[7] Elmar Gerhards-Padilla, et.al." Detecting Black Hole Attacks in Tactical MANETs using Topology Graphs", 32nd IEEE Conference on Local Computer Networks 0742-1303/07© 2007 IEEE.

[8] Zaheeruddin, Vinod K. Jain, and Guru V. Singh , "A Fuzzy Model For Noise-Induced Annoyance", IEEE transactions on systems, man, and cybernetics –Part A: Systems and Humans, Vol. 36(No. 4), July 2006.

[9] X. Wang, T. Lin and J. Wong, "Feature selection in intrusion detection system over mobile ad-hoc network," Technical Report, Computer Science, Iowa State University, 2005.

[10] 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.

[11] K. Jungwon, J. B. Peter, A. Uwe, G. Julie, T. Gianni and T. Jamie, "Immune System Approaches to Intrusion Detection – A Review", Natural Computing: an international journal, vol. 6, Issue 4, (2007) December.

[12] 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.

[13] R. K. Bharti, S. Shukla and S. Jain, "Intrusion detection using clustering", Special Issue of IJCCT, International Conference [ACCTA-2010], vol. 1, Issue 2, **(2010)** August 3-5, pp. 3-4.

[14] M. Panda and M. R. Patra, "Ensembling Rule Based Classifiers for Detecting Network Intrusions", IEEE International Conference on Advances in Recent Technologies in Communication and Computing, **(2009)**, pp. 19-22.