Volume 4, No. 2, Jan-Feb 2013

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Fuzzy Approach for Intrusion Detection System: A Survey

Partha Sarathi Bhattacharjee*, Dr. (Mrs.) Shahin Ara Begum
Department of Computer Science
Assam University, Silchar
Assam-788011, India
psbkls@gmail.com*, shahin.begum.ara@gmail.com

Abstract: Secured data communication over internet and any other network is always under threat of intrusions and misuses. Intrusions pose a serious security threat for the stability and the security of information in a network environment. An intrusion is defined as any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource. It includes attempting to destabilize the network, gaining unauthorized access to files with privileges, or mishandling and misusing of software. Intrusion Detection System (IDS) have become a needful component in terms of computer and network security. The goal of intrusion detection is to monitor network activities automatically, detect malicious attacks and to establish a proper architecture of the computer network security. Fuzzy logic dealing with vagueness and imprecision has a capability to represent imprecise forms of reasoning in areas where firm decisions have to be made in indefinite environments and is found to be appropriate for intrusion detection. This paper surveys the various IDS and the fuzzy approaches to IDS.

Keywords: Fuzzy Logic, malicious threats, networks security, intrusion detection

I. INTRODUCTION

The rapid development of information technology, network and computer attacks have stimulated wide concern worldwide. Not only has there been a marked increase in the number and kind of attacks, but the complexity and sophistication has also been increased. The potential harms of attacks are increasingly serious. As Internet security is a fast-moving field, the attacks that are catching the headlines can change significantly from one year to the next.

IDS which are increasingly a key part of system defence are used to identify abnormal activities in a computer system. Intrusion detection has emerged as a significant field of research, because it is not theoretically possible to set up a system with no vulnerabilities. One main confrontation in intrusion detection is that we have to find out the concealed attacks from a large quantity of routine communication activities.

Fuzzy logic is a form of many-valued logic or probabilistic logic; it deals with reasoning that is approximate rather than fixed and exact. In contrast with traditional logic they can have varying values, where binary sets have two-valued logic, true or false, fuzzy logic variables may have a truth value that ranges in degree between 0 and 1. Fuzzy logic has been extended to handle the concept of partial truth, where the truth value may range between completely true and completely false. Furthermore, when linguistic variables are used, these degrees may be managed by specific functions.

Fuzzy logic starts and builds on a set of user-supplied human language rules. The fuzzy systems convert these rules to their mathematical equivalents. This simplifies the job of the system designer and the computer, and results in much more accurate representations of the way systems behave in the real world. Additional benefits of fuzzy logic include its simplicity and its flexibility. Fuzzy logic can handle problems with imprecise and incomplete data, and it can model nonlinear functions of arbitrary complexity. Fuzzy logic techniques have been employed in the computer security field since the early 90's. Fuzzy logic has also demonstrated potential in the intrusion detection field when compared to systems using strict signature matching or classic pattern deviation detection. The concept of fuzziness helps to smooth out the abrupt separation of normal behaviour from abnormal behaviour. Fuzzy logic has a capability to represent imprecise forms of reasoning in areas where firm decisions have to be made in indefinite environments like intrusion detection.

In this paper we survey different IDS and fuzzy based approach for IDS. The remainder of the paper is organized as follows: Section II gives an overview of different types of network attacks. Section III describes the classification of Intrusion Detection System, Section IV describes the component of Intrusion Detection System, Section V describes the existing Intrusion Detection systems; Section VI explains the limitation of existing Intrusion Detection System , Section VII briefly explains the fuzzy approach for intrusion detection system., Section VIII measures the uncertainity of attack with respect to probability , Section IX concludes the paper and Section X lists the references.

II. NETWORK ATTACKS

There are four major categories of networking attacks. Every attack on a network can comfortably be placed into one of these groupings, [2].

a. ***Denial of Service (DoS):*** A DoS attack is a type of attack in which the hacker makes a computing or memory resources too busy or too full to serve legitimate networking requests and hence denying users access to a machine i.e. it blocks traffic, which results in a loss of access to network resources by authorized users. For example apache, smurf, ping of

death, neptune, mail bomb, UDP storm etc. are all DoS attacks.

b. ***Remote to User Attacks (R2L):*** A remote to user attack is an attack in which a user sends packets to a machine over the internet, which user does not have access to in order to expose the machines vulnerabilities and exploit privileges which a local user would have on the computer e.g. xlock, guest, xnsnoop, phf, sendmail dictionary etc.

c. ***User to Root Attacks (U2R):*** The User-to-Root attack is characterized by a process whereby any normal system user can illegally gain access to the super user's privileges. These attacks are exploitations in which the hacker starts off on the system with a normal user account and attempts to abuse vulnerabilities in the system in order to gain super user privileges e.g. perl, xterm etc.

d. ***Probing:*** Probing is an attack in which the hacker scans a machine or a networking device in order to determine weaknesses or vulnerabilities that may later be exploited so as to compromise the system. This technique is commonly used in data mining e.g. saint, portsweep, mscan, nmap etc.

III. CLASSIFICATION OF INTRUSION DETECTION SYSTEM

Intrusion detection refers to the detection of malicious activity (break-ins, penetrations, and other forms of computer abuse) in a computer related system. These malicious activities or intrusions are interesting from a computer security perspective. Intrusion Detection can be classified into two main categories. They are as follows [6,12]:

a. Host Based Intrusion Detection Systems:

System call intrusion detection systems deal with operating system call traces. The intrusions are in the form of anomalous sub-sequences of the traces. The anomalous sub-sequences translate to malicious programs, unauthorized behaviour and policy violations. They evaluate information found on a single or multiple host systems, including contents of operating systems, system and application files.

b. Network Intrusion Detection Systems:

These systems deal with detecting intrusions in network data. The intrusions typically occur as anomalous patterns though certain techniques model the data in a sequential fashion and detect anomalous sub-sequences. The primary reason for these anomalies is due to the attacks launched by outside hackers who want to gain unauthorized access to the network for information theft or to disrupt the network. They evaluate information captured from network communications, analysing the stream of packets which travel across the network.

IV. COMPONENTS OF INTRUSION DETECTION SYSTEM

There are normally three functional components of Intrusion Detection System [17]. The components are:

A. Data source*:* Data sources can be grouped into four categories namely Host-based monitors, Network-based monitors, Application-based monitors and Target-based monitors.

B. Analysis engine*:* This component takes information from the data source and examines the data for symptoms of attacks or other policy violations. The analysis engine can use one or both of the following analysis approaches:

- ***a. Misuse/Signature-Based Detection:*** This detection engine uses a database of known attack patterns. When they detect activity matching one of those patterns, an alert is triggered. Signature detection systems have an extremely low false alarm (or "false positive") rate but require constant updating in order to detect new types of attack.
- ***b. Anomaly/Statistical Detection:*** It develops a baseline (which may change over time) of "normal" activity on a system or network and then uses that baseline to detect when abnormal activity takes place. The major advantage to anomaly-detection systems is that they are often capable of detecting new types of malicious activity as soon as they occur. The downside is that systems can be "trained" to accept malicious activity as part of the baseline by slowly introducing it into the monitored environment until it is accepted as normal.

C. Response Manager*:* In basic terms, the response manager will only act when inaccuracies (possible intrusion attacks) are found on the system, by informing someone or something in the form of a response.

V. EXISTING INTRUSION DETECTION SYSTEMS

a. ***Snort:*** A free and open source network intrusion detection and prevention system, was created by Martin Roesch in 1998 and now developed by Sourcefire. Through protocol analysis, content searching, and various pre-processors, Snort detects thousands of worms, vulnerability exploit attempts, port scans, and other suspicious behaviour [23].

b. ***OSSEC:*** An open source host-based intrusion detection system performs log analysis, integrity checking, root kit detection, time-based alerting and active response [21].

c. ***Logsurfer****:* It is a tool for monitoring text log files for anomalous events in real-time. It can send messages when a rule is matched so that an administrator can react quickly to an event. [5].

d. ***OSSIM:*** The goal of Open Source Security Information Management, OSSIM is to provide a

comprehensive compilation of tools which, when working together, grant network/security administrators with a detailed view over each and every aspect of networks, hosts, physical access devices, and servers [21].

e. ***SHADOW****:* It is an open source intrusion detection system. SHADOW is perfectly usable by itself or the scripts can be modified to drive another IDS [22].

f. ***Suricata:*** An open source-based intrusion detection system, was developed by the OISF [24].

g. ***Bro****:* An open-source, Unix-based network intrusion detection system. Bro detects intrusions by first parsing network traffic to extract its application-level semantics and then executing event-oriented analyzers that compare the activity with patterns deemed troublesome [25].

h. ***Fragroute/Fragrouter:*** A network intrusion detection evasion toolkit. Fragrouter helps an attacker launch IP-based attacks while avoiding detection. It is part of the NIDS bench suite of tools by Dug Song [21] .

i. ***BASE:*** The Basic Analysis and Security Engine, BASE is a PHP-based analysis engine to search and process a database of security events generated by various IDSs, firewalls and network monitoring tools [21].

j. ***Sguil:*** Sguil is built by network security analysts for network security analysts. Its main component is an intuitive GUI that provides real-time events from Snort/barnyard. It also includes other components which facilitate the practice of network security monitoring and event driven analysis of IDS alerts [20].

VI. LIMITATIONS OF EXISTING INTRUSION DETECTION SYSTEM

Intrusion Detection System suffers from the following limitations [15] :

A. Limitation of Anomaly Detection:

Although anomaly detection can accommodate unknown patterns of attacks, it also suffers from several drawbacks. A common problem of all anomaly detection approaches, with the exception of the specification-based approach, is that the subject's normal behaviour is modelled on the basis of the audit data collected over a period of normal operation. If undiscovered intrusive activities occur during this period, they will be considered normal activities. In addition, because a subject's normal behaviour usually changes over time. The IDSs that use the above approaches usually allow the subject's profile to gradually change. This gives an intruder the chance to gradually train the IDS and trick it into accepting intrusive activities as normal. Further, the current anomaly detection approaches usually suffer from a high false-alarm rate.

B. Limitation of Misuse Detection:

Current misuse detection systems usually work better than anomaly detection systems for known attacks. That is, misuse detection systems detect patterns of known attacks more accurately and generate much fewer false alarms. This better performance occurs because misuse detection systems take advantage of explicit knowledge of the attacks. The limitation of misuse detection is that it cannot detect novel or unknown attacks. As a result, the computer systems protected solely by misuse detection systems face the risk of being comprised without detecting the attacks.

In addition, explicit representation of attacks, misuse detection requires the nature of the attacks to be well understood. Hence, it requires that human experts must work on the analysis and representation of attacks, which is usually time consuming and error prone.

VII. FUZZY APPROACH TO NETWORK INTRUSION DETECTION SYSTEM

With computers increasingly getting connected to public accessible networks it is not feasible for several computer systems to affirm security to network intrusions. In view of the fact that there is no ideal solution to avoid intrusions from event, it is very significant to detect them at the initial moment of happening and take necessary actions for reducing the likely damage. For intrusion detection, a wide variety of techniques have been applied specifically, data mining techniques, artificial intelligence technique and soft computing techniques. Most of the data mining techniques like association rule mining, clustering and classification have been applied on intrusion detection, where classification and pattern mining is an important technique. Similar way, AI techniques such as decision trees, neural networks and fuzzy logic are applied for detecting suspicious activities in a network, in which fuzzy based system provides significant advantages over other AI techniques. Recently, several researchers focused on fuzzy rule learning for effective intrusion detection using data mining techniques [18].

Universal access to computers has enabled hackers and would-be terrorists to attack information systems and critical infrastructures worldwide [8] explained that practically. Fuzzy preference relation, based on fuzzy satisfaction function is applied to comparison of attack signatures. Fuzzy signatures (their gamma resolution sets) are combined by fuzzy operators. Therefore, qualitative, fuzzy decision system is achieved. Different fuzzy set operators used in construction fuzzy satisfaction function, as also as different fuzzy preference relations have been tested. The method provided smoother results than one obtained by traditional methods. Experiments demonstrated that final outcome dependence on correct determination of fuzzy values out of signature attacks, as also as on adequate choice of fuzzy set operator.

Network intrusion detection (NID) is essentially a pattern recognition problem in which network traffic patterns are classified as either 'normal' or 'abnormal' [4]. The incorporation of computational intelligence in network intrusion detection systems (NIDS) presents the greatest potential for an acceptable solution. Computational intelligence has yielded successful solutions to similar

problems in other domains such as the highway incident detection problem.

Most current intrusion detection systems employ signature-based methods or data mining-based methods which rely on labelled training data [3]. However, in practice, this training data is typically expensive to produce. In contrast, unsupervised anomaly detection has great utility within the context of network intrusion detection system. Such a system can work without the need for massive sets of pre-labelled training data and has the added versatility of being free of the over specialization that comes with systems tailored for specific sets of attacks. Thus, with a system that seeks only to define and categorize normalcy, there is the potential to detect new types of network attacks without any prior knowledge of their existence. They discuss the creation of such a system that uses a fuzzy cluster algorithm to detect anomalies in network connections.

Artificial Intelligence plays a driving role in security services. The authors propose a dynamic Intelligent Intrusion Detection System model, based on specific AI approach for intrusion detection [13].

The use of fuzzy logic is described in the implementation of an intelligent intrusion detection system [1]. The system uses a data miner that integrates Apriori and Kuok's algorithms to produce fuzzy logic rules that capture features of interest in network traffic. Using an inference engine, implemented using FuzzyJess, the intrusion detection system evaluates these rules and gives network administrators indications of the firing strength of the rule set. The resulting system is capable of adapting to changes in attack signatures. In addition, by identifying relevant network traffic attributes, the system has the inherent ability to provide abstract views that support network security analysis.

A novel network intrusion detection framework for mining and detecting sequential intrusion patterns was proposed in the paper [7]. The framework of the paper consists of a Collateral Representative Subspace Projection Modeling (C-RSPM) component for supervised classification, and an inter-transactional association rule mining method based on Layer Divided Modeling (LDM) for temporal pattern analysis. Experiments on the KDD99 data set and the traffic data set generated by a private LAN tested show promising results with high detection rates, low processing time, and low false alarm rates in mining and detecting sequential intrusion detections.

A real-time NIDS with incremental mining for fuzzy association rules was explained in the paper [10]. By consistently comparing the two rule sets, one mined from online packets and the other mined from training attack-free packets, the system can render a decision every 2 seconds. Thus, compared with traditional static mining approaches, the system can greatly improve efficiency from offline detection to real-time online detection. Since the system derives features from packet headers only, like the previous works based on fuzzy association rules, large-scale attack types are focused. Many DoS attacks were experimented in this study. Experiments were performed to demonstrate the excellent effectiveness and efficiency of the proposed system. The system may not cause false alarms because normal programs supposedly would not generate enough mal-formatted packets, or packets that violate normal network protocols.

Network intrusion detection system (NIDS) based on genetic-fuzzy association rules was described in the paper[9], which mines rules in an incremental manner in order to meet the real time requirement of a NIDS.

An anomaly based intrusion detection system in detecting the intrusion behaviour within a network was developed in the paper[19]. A fuzzy decision-making module was designed to build the system more accurate for attack detection, using the fuzzy inference approach. An effective set of fuzzy rules for inference approach were identified automatically by making use of the fuzzy rule learning strategy, which are more effective for detecting intrusion in a computer network. At first, the definite rules were for attack data as well as normal data. Then, fuzzy rules were identified by fuzzifying the definite rules and these rules were given to fuzzy system, which classify the test data. Executing a fuzzy model involves defining the methods of fuzzification, aggregation, and defuzzification. KDD cup 99 dataset has been used for evaluating the performance of the system and experimentation results show that the method is effective in detecting various intrusions in computer networks.

The approach to use Genetic Algorithms and Fuzzy Logic in Intrusion Detection System is discussed in the paper [16]. With the increasing use of the internet, the security threats have multiplied many folds. Along with all other conventional method, Intrusion Detection System has come a long way in the fight against security vulnerabilities. The use of Genetic Algorithms in Intrusion Detection System is particularly useful as it considers both temporal and spatial information of the network connections. Moreover the use of fuzzy logic can help in detecting anomalies which cannot be discreetly deemed as normal or anomalous. This paper gives an overview of the Intrusion Detection System and looks at two major machine learning paradigms used in Intrusion Detection System, Genetic Algorithms and Fuzzy Logic and how to apply them for intrusion detection.

IDS by applying genetic algorithm (GA) to efficiently detect various types of network intrusions was explained in the paper[11]. Parameters and evolution processes for GA are discussed. This approach uses evolution theory to information evolution in order to filter the traffic data and thus reduce the complexity.

VIII. MEASUREMENT OF UNCERTAINITY OF ATTACK WITH RESPECT TO PROBABILITY [14]:

A False positive is where detection has been made. If this is a real attack then appropriate action must be taken. What if it isn't a real attack? This scenario is known as a false positive. A perfectly legitimate transaction could trigger IDS to believe that an attack was in progress. The solution is to investigate and review the IDS configuration to prevent the false positive from occurring again. The other

end of the spectrum is where an attack takes place and the IDS doesn't detect it—this is called a false negative. Here we analyse false positive test data which are collected from the report of PC Security Lab, China.

Table 1: PCSL Greater China Region False Positive Test (January, 2011)

Vendor	**x**	**Static FPs**	**$\mu_A(x)$**	**Dynamic FPs**	**$\mu_B(x)$**	**$\mu_c(x)=\mu_A(x)+\mu_B(x)$**
BitDefender	0	0	0	0	0	0
Microworld	1	0	0	0	0	0
F-secure	2	0	0	1	0.03125	0.03125
Jiangmin	3	2	0.009852	0	0	0.009852217
Kingsoft	4	2	0.009852	0	0	0.009852217
Microsoft	5	2	0.009852	0	0	0.009852217
NETGATE	6	3	0.014778	0	0	0.014778325
Qihoo	7	2	0.009852	2	0.0625	0.072352217
Rising	8	2	0.009852	2	0.0625	0.072352217
Trend Micro	9	4	0.019704	0	0	0.019704433
AVG	10	5	0.024631	0	0	0.024630542
Dr. Web	11	4	0.019704	1	0.03125	0.050954433
ESET	12	5	0.024631	0	0	0.024630542
G DATA	13	5	0.024631	0	0	0.024630542
Panda	14	4	0.019704	1	0.03125	0.050954433
TrustPort	15	5	0.024631	0	0	0.024630542
Zilya	16	4	0.019704	1	0.03125	0.050954433
ArcaBit	17	5	0.024631	1	0.03125	0.055880542
Avast	18	7	0.034483	0	0	0.034482759
Kaspersky	19	5	0.024631	2	0.0625	0.087130542
Filseclab	20	8	0.039409	0	0	0.039408867
IKARUS	21	7	0.034483	1	0.03125	0.065732759
QuickHeal	22	8	0.039409	0	0	0.039408867
SOPHOS	23	7	0.034483	1	0.03125	0.065732759
Symantec	24	8	0.039409	0	0	0.039408867
Antiy	25	9	0.044335	0	0	0.044334975
Emsisoft	26	4	0.019704	6	0.1875	0.207204433
McAfee	27	12	0.059113	0	0	0.0591133
Sunbelt	28	11	0.054187	1	0.03125	0.085437192
VBA32	29	11	0.054187	4	0.125	0.179187192
COMODO	30	13	0.064039	5	0.15625	0.220289409
Avira	31	21	0.103448	0	0	0.103448276
Coranti	32	18	0.08867	3	0.09375	0.182419951
Total :		**203**		**32**		

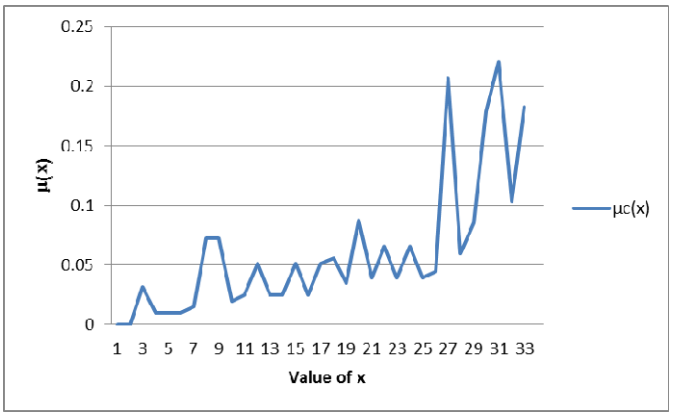

Figure.1: Total FPs test graph

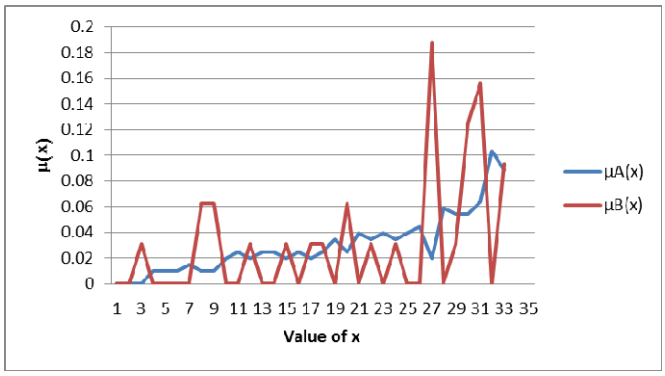

Figure.2: Static FPs and Dynamic FPs test graph

From Figure.1, we observe that the maximum False Positive Attack is detected by COMODO and from Figure.2, we observe that the maximum False Positive Attack is detected by Emsisoft with respect to dynamic False Positive attack. So the probability of false positive attack detection is very with respect to Anit Virus and it also varies from static FPs to dynamic FPs. So, uncertainity occurs and the membership function values vary in between 0 to 1. So, we can approach for fuzzy to define this uncertainity.

IX. CONCLUSION

Secured data communication over internet and any other network is always under threat of intrusions and misuses. It is important for maintaining a high level security to ensure safe and trusted communication of information between various organizations. So Intrusion Detection Systems have become a needful component in terms of computer and network security. There are various approaches being utilized in intrusion detections, but unfortunately any of the systems so far is not completely flawless. So, the quest of betterment continues.

Fuzzy approach to IDS is attracting considerable interest from research community. In this paper, we have surveyed different approach for network intrusion detection. From the research work survey in the paper, the popularity of the fuzzy logic clearly demonstrates the successfulness of the fuzzy approach to IDS. It is anticipated that fuzzy logic will continue to play an important role to stimulate the creation of efficient IDS.

X. REFERENCES

[1]. Aly El–Semary, Janica Edmonds, Jes´us Gonz´alez-Pino, Mauricio ,Papa, “Applying Data Mining of Fuzzy Association Rules to Network Intrusion Detection”, Proceedings of the IEEE Workshop on Information Assurance ,United States Military Academy, West Point, NY, 2006

[2]. A. Sung, S. Mukkamala, “Identifying important features for intrusion detection using support vector machines and neural networks” in Symposium on Applications and the Internet, 2003, pp. 209–216

[3]. Gao Xiang, Wang Min, Zhao Rongchun, “Applying Fuzzy Data Mining to Network Unsupervised Anomaly Detection”, ISCIT, 2005, IEEE Computer pp. 1249-1253

[4]. H. Adeli and A. Karim , “Wavelets in Intelligent Transportation Systems”, John Wiley & Sons UK , 2005

[5]. Logsurfer (software): http://www.cert.dfn.de/eng/logsurf/

[6]. Martuza Ahamed, Rima Pal, Md. Mojammel Hossain , Md. Abu Naser Bikas ,Md. Khalad Hasab, “A Comparative Study on the Currently Existing Intrusion Detection Systems”, Proceedings of the IACSIT,2009, Spring Conference, IEEE , pp.151-154

[7]. Mei-Ling Shyu, Zifang Huang, and Hongli Luo , “Efficient Mining and Detection of Sequential Intrusion Patterns for Network Intrusion Detection Systems”, Machine Learning in Cyber Trust, ISBN 978-0-387-88734-0. Springer-Verlag US, 2009, pp. 133-154

[8]. Milos Manic and Bogdan Wilamowski , “Fuzzy Preference Approach for Computer Network Attack Detection”, University of Idaho, College of Engineering, Center Boise, IEEE , 2001

[9]. Ming-Yang Su , Chun-Yuen Lin , Sheng-Wei Chien and Han-Chung Hsu, “Genetic-Fuzzy Association Rules for Network Intrusion Detection Systems”, IEEE International Conference on Fuzzy Systems, 2011, Taipei, Taiwan

[10]. Ming-Yang Su, Gwo-Jong Yu and Chun-Yuen Lin, “A real-time network intrusion detection system for large-scale attacks based on an incremental mining approach” ,Elsevier , computers & security , 2009, pp. 301 – 309

[11]. Mohammad Sazzadul Hoque, Md. Abdul Mukit and Md. Abu Naser Bikas , “An Implementation of Intrusion Detection System using Genetic Algorithm”, IJNSA, 2012, Vol.4, No.2

[12]. Mohammad Sazzadul Hoque, Md. Abdul Mukit and Md. Abu Naser Bikas, “An implementation of intrusion detection system using Genetic Algorithm”, International Journal of Network Security & Its Applications (IJNSA), 2012, Vol.4, No.2, pp. 109-120

[13]. Norbik Bashah Idris and Bharanidharan Shanmugam, "Novel Attack Detection Using Fuzzy Logic and Data Mining", Security and Management, CSREA Press,2006, pp.26-31

[14]. Nozer D. SINGPURWALLA and Jane M. BOOKER, "Membership Functions and Probability Measures of Fuzzy Sets", Journal of the American Statistical Association ,2004, Vol. 99, No. 467,pp.867-878

[15]. Peng Ning, Sushil Jajodia, "Intrusion Detection Techniques", The Internet Encyclopedia,Wiley Online Library,2004

[16]. Rajdeep Borgohain, " FuGeIDS: Fuzzy Genetic paradigms in Intrusion Detection Systems", IJANA, 2012, Volume: 03 Issue: 06, ISSN: 0975-0290, pp.1409-1415

[17]. R. G. Bace, "Intrusion Detection", Macmillan Technical Publishing, 2000

[18]. R. Shanmugavadivu and Dr. N. Nagarajan, "Network Intrusion Detection System using Fuzzy Logic", IJCSE, 2011, ISSN: 0976-5166 Vol. 2 No. 1

[19]. R. Shanmugavadivu and Dr.N.Nagarajan, "Learning of Intrusion Detector in Conceptual Approach of Fuzzy Towards Intrusion Methodology", IJARCSSE , 2012,Vol.2, Issue.5, ISSN: 2277 128X, pp.246-250

[20]. Sectools.Org: http://sectools.org/tools2006.html

[21]. SecTools.Org: http://sectools.org/tag/ids/

[22]. SHADOW (software): http://www.nswc.navy.mil/ISSEC/CID/step.tar.gz

[23]. Snort (software): http://www.snort.org/

[24]. Suricata (software): http://en.wikipedia.org/wiki/Suricata_(software)

[25]. The Bro Network Security Monitor: http://bro-ids.org/