ISSN: 2321-7782 (Online)

Volume 3, Issue 3, March 2015

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

Techniques and Counter Attack Methodologies used in Intrusion Detection System

Mohammad Abrahim Wani[1]
Research Scholar
MMICT&BM
Maharishi Markendeshwar university
Mullana Ambala Haryana, India

Rshma Chawla[2]
Assistant Professor
MMICT&BM
Maharishi Markendeshwar university
Mullana Ambala Haryana, India

Abstract: Securing the system is a major concern in the present digital era. The wide spread of networking has increased the necessity of protecting the system to a very high extent. Intrusion detection system is considered as the backbone for securing system/network by intrusions. Intrusion detection system enables us to secure the system from the unauthorized users, who intend to misuse the system. Intrusion Detection system is defined as a solution of system security to identify the abnormal activities in a computer system or network. Different types of techniques, approaches have been deployed within the field of intrusion detection system (IDS). In this paper, a survey on intrusion detection system is carried out. The paper provides an introduction to the concepts of intrusion detection system, a brief survey about the literature, techniques and counter attack methodologies that are used within the intrusion detection system. This survey will provide helpful insight into the related literature of intrusion detection systems.

I. INTRODUCTION

The problems that exist within the computer security domain are addressed by the computer security. The viruses, worms, hackers, etc become the problems that network security must solve. Though many techniques have been implemented, The Intrusion Detection System has become a needful component in a well formed network security policy.

In 1987 Dorothy E. Denning projected intrusion detection as a method to counteract the computer and networking attacks and misuses [1]. Intrusion detection is used by the method called IDS. In general, most of these saleable implementations are relative ineffective and inadequate, which gives augment for research on more vibrant intrusion detection systems.

Generally an intruder is defined as a system, program or individual who wants to break and most probably turn into successful results in breaking the information system or execute an program that is not legally permitted .Generally intrusion are referred as any set of events that attempt to compromise the integrity, confidentiality, or availability of a computer resource [2]. The act of detecting actions that try to negotiate the integrity, confidentiality, or availability of a computer resource, and this approach is referred as intrusion detection [2]. An intrusion detection system is a device or software application that views the network and/or system actions for the actions/intrusions or strategies that corrupts the system and makes the report of these illegal actions [3].

Intrusion Detection Systems (IDS) are mainly focused on identifying apparent incidents, monitoring information about them, attempts to stop them, and reporting them to security administrators in real-time environment, and those that use audit data with some delay (non-real-time). The second approach would holdup the instance of detection in a certain amount of time. Additionally, associations concern IDSs for other reasons, such as classifying troubles with security policies, documenting accessible attacks, and preventing those from violating security policies. IDSs have become a vital addition to the security infrastructure of almost every organization. Today there are many commercial intrusion detection systems existing. A usual Intrusion Detection System is demonstrated in Figure 1.

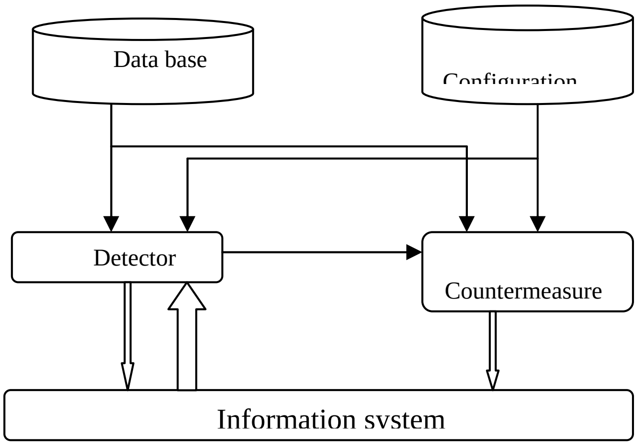

Figure 1.Simple Intrusion Detection System [37].

The arrow lines symbolize the amount of information flowing from one component to another

II. Literature Survey

Various renowned researchers are working to improve the related topic. The work of few researchers is discussed in this section.Communication technologies and trends have changed very much over last two decades. These days, every group is maintaining an online profile thus allocating the important as well as non-important resources over the globe [4].The concept of intrusion detection system starts in 1980 with the James Anderson (1980), which discusses the concept of monitoring the data over the local network by using some predefined profiles. With this the concept of intrusion and audit data came into lime light [5]. This beautiful concept made lot of improvement in auditing subsystems, and logically laid the base for formulation and development of intrusion detection systems [6]. The concept describes the basic design for audit trails, which was very much useful in understanding the performance of users. This concept makes an impressive impact on the world of security systems.

Dr. Dorothy Denning in 1985 introduces a prototype that would analyze audit trails from government systems and track user activity. Author named this system as Intrusion Detection Expert System (IDES) and it was the foundational research into IDS technology.

Researcher [7] in 1988 introduces a combined anomaly detection/misuse detection IDS that models individual users as well as groups of users. It assigns primary profile to fresh users, and updates the profiles once a pattern of definite activities is acknowledged. Haystack used a different statistical anomaly detection algorithm.

Lane and Brodley (1998) propose the applied Instance Based Learning (IBL) to learn the techniques of data (e.g., users) from sequential order of data. IBL came with the idea that is represented with a set of instances called instance dictionary that illustrated the concept of Ids. Classification of the new instance is done according to its relation that stores instances. IBL requires a concept of “distance” linking the instances so that the comparison of various instances can be considered and used to classify the instances.

Author [8] in 1990 used the concept of a time-based inductive machine (TIM) to judge the user’s pattern. Author recognizes ordinary sequential patterns in a string of events. The sequential patterns characterize extremely rhythmic activities and are projected to grant predication. The ordinary patterns, which are represented in the form of rules, are generated and personalized from the input data by means of a logical inference called inductive generalization. When the approach is applied to intrusion detection, the rules explain the performance patterns of both user and group of users on the basis of past audit history.

Alessandri, D, 2001 explained the concept of activity scope and blend of classification introduction that made available a flexible and practical tool to articulate the idea of intrusion detection system. This taxonomy has been considered to give details about the functional aspects i.e., the capabilities of intrusion detection system such that one is able to assess intrusion detection system in a next step to identify attacks, generate false positives etc.

Author [9] in 1996 describes the overview of intrusion detection concepts and taxonomy was given. It introduces and discusses several commercial and public-domain IDS's available. This paper also describes recent developments in conventional intrusion detection: Distributed, modular system which includes both anomaly and misuse detection. A peek at the new breed of pro-active, preventative tools so-called Delphic tools identifies the threats and risks in the very early attack stages.

Jeyanthi Hall, 2007 demonstrated an anomaly-based intrusion detection method, which unites with Radio Frequency Fingerprinting (RFF) and Hotelling's T 2, for the performance of statistical process control, for detecting this attack. RFF is a procedure used to exclusively recognize a transceiver based on the transceiver print (set of features) of the signal it raises. The method connects a transceiver profile of a wireless device with its comparable MAC address, even though the MAC address can silently be spoofed, the transceiver prints as a unrecognized machine that did not resemble with the profile of the legal machine. Moreover, the high achievable rate of a wireless IDS can be enhanced by analyzing several prearranged transceiver prints, former to representation of a decision.

Various Genetic Algorithms (GAs) and Genetic Programming (GP) have been used for recognizing intrusions in various situations. Several use Genetic Algorithms to achieve taxonomy regulations [10]. Genetic algorithms choose obligatory skills and chooses mainly admirable and slightest bound of various main functions in which unique Artificial Intelligence methods were used to design acquisition rules [11].

The use of GAs for intrusion detection came into the consideration in 1995, when the authors [12] implemented several agent technology and GP to identify network anomalies [13]. For agents the use of GP used to resolve anomalous network behaviors and every agent can observe one constraint of the network audit data. The expected method has the advantage, that various small autonomous agents are used but it has difficulty in communicating between the agents and also if the agents are not appropriately initialized the training process can be time consuming.

Author [14, 15] described a method using GA to detect anomalous network intrusion. The approach includes both quantitative and categorical features of network data for deriving classification policy. However, the enclosure of quantitative feature can enhance detection rate but no investigational results are available.

III. Networking Attacks

This section is a summary of the four major categories of networking attacks. Every attack on a network can contentedly be placed into one of these groupings [36].

Denial of Service (DoS): A Denial of service attack is a type of attack in which the hacker makes an attempt to make a machine or network resource unavailable to its dedicated users. DOS attacks normally mark sites of service hosted on high profile web services such as banks, credit cards, payment gateways and even root name servers. It involves saturating the target machine with external communication requests, so that it cannot respond or respond so slowly. Mail bomb, Apache,Smurf, Neptune, UDP storm, Ping of death etc. are all Denial of service attack attacks.

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 s/he does not have right to use in order to rendering the machines vulnerabilities and utilize privileges which a local user would have on the computer e.g. sendmail dictionary, xlock, phf, guest, xnsnoop, etc.

User to Root Attacks (U2R): These attacks are exploitations in which the hacker starts off on the system with a normal user account and attempts to misuse vulnerabilities in the system in order to achieve super user privileges e.g. xterm, perl. Probing: Probing is an attack in which the hacker scans a machine or a networking device in order to find out weaknesses or vulnerabilities that may later on be exploited so as to compromise the system. This technique is normally used in data mining e.g. mscan, saint, portsweep, nmap etc.

IV. Components of Intrusion Detection System

Based on the types of network attacks available the network has to secure from these types of attacks. Different approaches are available to defend the network/system, Intrusion detection system is the one approach that is used for securing the system, and is considered as the first defense line in protecting the system/network, IDS is designed for monitoring and securing the system against the intrusions. An intrusion detection system in general is categorized on the three operable components [17]. The operable components are shown in figure.2

Data source is divided into the four different types which are generally called as: Host-based monitors, Network-based monitors, Application-based monitors and Target-based monitors.

The second module of an intrusion detection system is recognized as the analysis engine. This module collects the information from the data source and monitors the data for the possibility of attacks or other method of violations. The approaches used by the analysis engine can use one or both of the following analysis method [18]:

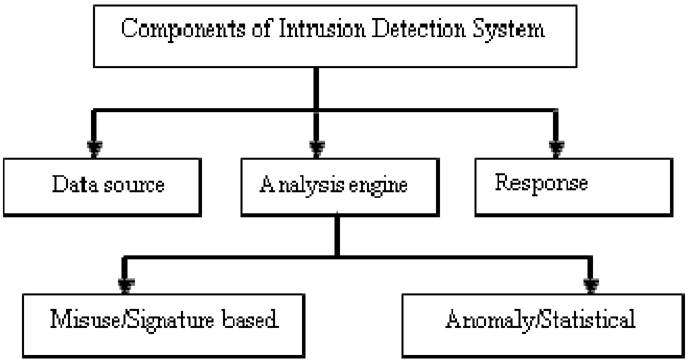

Figure 2: Components of intrusion detection system

Misuse/Signature-based detection: These systems are most extensively used and they detect intruders with known patterns. The patterns and signatures used to identify attacks that consist of various fields of a network packet, like destination address, source address, and source and destination ports. These systems show a negative aspect in the sense that only the attacks that already exist in the attack database can be detected, so this model needs continuous updating, but they have a virtue of having very low false positive rate [4].

Misuse detection is wholly valuable in revealing known attacks, it is useless when faced with unidentified or new forms of attacks for which the signatures passes all probable variations of the attack is difficult. Any mistake in the definition of these signatures will enhance the false alarm rate and reduce the efficiency of the detection method.

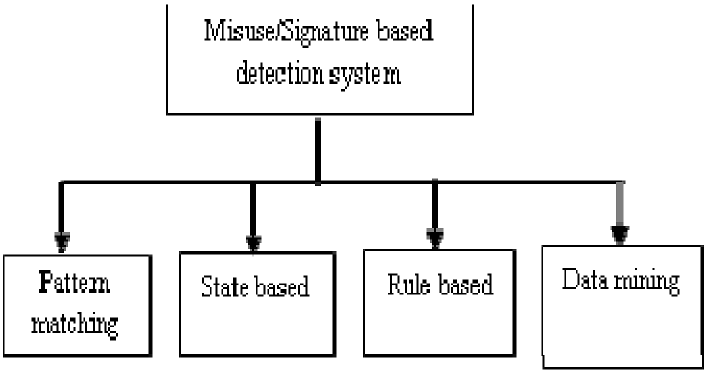

Figure 3: Misuse based detection system

Four classes of techniques are commonly used to implement misuse detection, namely pattern matching, rule-based techniques, state-based techniques, and data mining. The techniques used are shown in figure 3.

Pattern matching based intrusion detection approaches are commonly used in the network based intrusion detection systems in which attack patterns are modeled, matched and identified based on the packet head, packet content or both. Attack patterns could also be established in host-based intrusion detection systems through concatenating the words representing the system calls in a system audit trail. With the continual emerging of new types and varied forms of attacks the number of signatures is constantly growing, thus making the pattern matching more expensive in terms of the computational cost

Rule-based expert system is one of the earliest techniques used for misuse detection. Expert systems encode intrusive scenarios as a set of rules, which are matched against audit or network traffic data. Any deviation in the rule matching process is reported as an intrusion. Examples of rule-based systems include MIDAS (Multics Intrusion Detection and Alerting System)[19], IDES (Intrusion Detection Expert System)[20], and NIDES (Next-generation Intrusion Detection Expert System)[21,22]

State-based techniques detect known intrusions by using expressions of the system state and state transitions. State models simplify the specification of patterns for known attacks and can be used to describe attack scenarios easier than rule-based languages such as P-BEST. In state-based techniques, activities contributing to intrusion scenarios are defined as transitions between system states, and thus intrusion scenarios are defined in the form of state transition diagrams.

Anomaly/Statistical detection: Anomaly detection systems recognize deviations from normal behavior and alert to potential unknown or novel attacks without having any prior knowledge of them. The anomaly detection determines whether deviation from the established normal usage patterns can be flagged as intrusions [23]. They exhibit higher rate of false alarms, but they have the capability of detecting unknown attacks and carry out their task of looking for deviations much faster [4].

Different from misuse detection, anomaly detection is dedicated to establishing normal activity profiles for the system. It is based on the assumption that all intrusive activities are necessarily anomalous. Anomaly detection studies start by forming an opinion on what the normal attributes for the observed objects are, and then decide what kinds of activities should be flagged as intrusions and how to make such particular decisions. Anomaly based approaches are shown in figure 4.

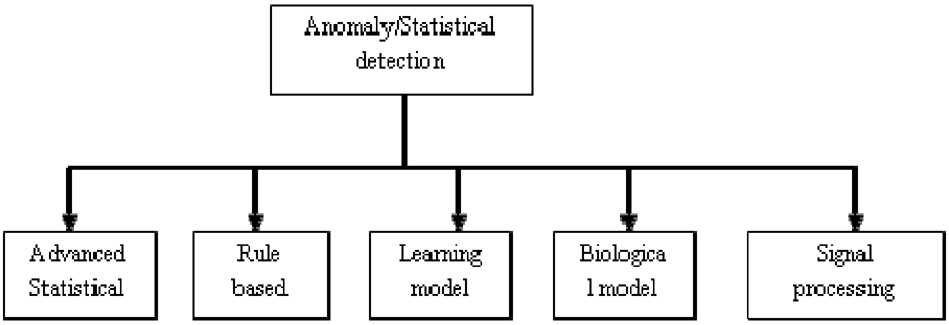

Figure 4: Anomaly based detection system

Many anomaly detection techniques have been proposed in the literature. These range from advanced statistical models to artificial intelligence and biological models based on human immune systems. Although it is difficult to classify these techniques we can divide them into four categories based on previous surveys on anomaly detection systems [24, 25, 26, and 27]. These include advanced statistical models, rule-based models, learning models, biological models, and signal processing techniques based models.

The third module of an intrusion detection system is the response manager. In simple form, the response manager resolves the inaccuracies (feasible intrusion attacks) only when they are found on the system, in the form of a response by informing someone or something [28].

© 2015, IJARCSMS All Rights Reserved

1.1 Classification of Intrusion detection System

Intrusion detection system is divided into two parts. They are

- **Host based Ids:** Host Ids get audit data from host audit trails and detects attack against a single host.[16]
- **Network based Ids:** Use network traffic as the audit data source, relieving the burden on the hosts that usually provide normal computing services and Detect attacks from network. [16]

1.2 Working of Intrusion Detection System

Intrusion Detection system is a software application that monitors system and network activities & reports the suspected intrusions as defined by the enable IDS policies. Some IDS reports the intrusion and some attempt to stop an intrusion attempt .An IDS works by examining and collecting information for unknown occurrences.

An IDS works by examining following events: observing activity, viruses, vulnerabilities, file settings, services, packet sniffing, PC check. The following show how IDS works;

- When the service stack detects forbid intrusion, it sends a message “an event” to IDS task.
- The IDS task’s purpose is to counterpart each event in the (one at a time) line with normal form in port table. It also keeps a way and record of intrusive events.
- If any event exceeds a definite threshold according to IDS policies it generates a signal.
- If an event is signaled, the intrusion monitor authentication is formed in audit journal.
- The GUI of the Ids displays the intrusion events from the intrusion checking audit records.
- The system for message notification on IDS properties page, IDS notification sends an e-mail to particular email address.

V. Existing Systems And Their Problems

Snort: A liberated and unwrap source network intrusion detection and prevention system was created by Martin Roesch in 1998 and presently designed by Sourcefire, in 2009, Snort entered InfoWorld's Open Source Hall of Fame as one of the “greatest open source software of all time” [31][32].Thousands of worms are detected during the content exploration, procedure research, and different pre-processors with the use of Snort, vulnerability exploit attempts, port scans, and other concerned activities [29][30].

OSSEC: An open source host-based intrusion detection system uses the method of log research, root kit detection, time-based alerting, integrity checking, and active response [29] [30]. In addition to its IDS functionality, it is generally used as a SEM/SIM resolution because of its influential log analysis engine, ISPs, data centers and universities use the OSSEC HIDS to observe and estimate their firewalls, web servers, IDSs, and authentication logs.

OSSIM: The objective of Open Source Security Information Management, OSSIM is to offer an extensive collection of tools which, when executed together, giving network/security administrators with a thorough view over each and every part of networks, physical access devices, host, and servers [30]. OSSIM incorporates numerous other tools, including Nagios and OSSEC HIDS.

Suricata: This type of intrusion detection system is based on open source was designed and implemented by the Open Information Security Foundation (OISF) [33].

Bro: An open-source, Unix-based network intrusion detection system [34]. Bro detects intrusions by first parsing network traffic to remove its application-level semantics and then executing event-oriented analyzers that weigh against the activity with patterns deemed difficulties.

Fragroute/Fragrouter: A network intrusion detection evasion toolkit [29]. Fragrouter helps an attacker launch IP-based attacks while avoiding detection. It is part of the NIDS bench suite of tools by Dug Song.

BASE: The Basic Analysis and Security Engine, BASE is a PHP-based analysis engine to examine and process a database of protection events generated by different IDSs, network monitoring tools and firewalls [29].

Sguil: Sguil is built by network security analysts for network security analysts [29][30]. Its core module is an intuitive GUI that provides real-time actions from Snort/barnyard. It also includes other mechanism which facilitate the practice of network security monitoring and event driven analysis of IDS alerts

VI. Problems with Existing Systems

Most available intrusion detection systems suffer from at least two of the following problems [35]: *First*, The fidelity problem. Information used by the intrusion detection system is obtained from packets or from audit trails on a network. Data has to pass through a longer path from its source to the IDS and in the process data can potentially be broken or customized by an attacker. In addition, the intrusion detection system has to realize the manners of the system where from the data is collected, which can effect in misinterpretations or missed events.

Second, The resource usage problem, The intrusion detection system continuously uses additional resources in the system it observe even when there are no intrusions available, because the mechanism of the intrusion detection system have to be running all the time[35,39].

Third is, the reliability problem, the mechanism of the intrusion detection system implement as separate programs, they are focus to tampering. An intruder can potentially end or alter the programs running on a system, leaving the intrusion detection system useless or unreliable [35].

VII. Conclusion

An intrusion detection system is a component of the defensive operations that complements the defenses such as firewalls. The intrusion detection system mainly detects attack signs and then alerts the system for such intrusions. According to the detection method, intrusion detection systems are usually categorized as misuse detection and anomaly detection systems. The operation point of view, they are be classified in network based or host based IDS. In current intrusion detection systems information is composed from both network and host resources. In terms of presentation, an intrusion detection system becomes more correct as it detects more attacks and raises less false positive alarms.

References

1. DE Denning, “An intrusion-detection model”, IEEE Transactions on software Engineering (1987), pp. 222–23
2. Sebring, E. Shellhouse, M. Hanna, and R. Whitehurst, “Expert systems in intrusion Detection”: A case study, Proceedings of the 11th National Computer Security Conference,1988, pp. 74–81.
3. T. Lunt, R. Jagannathan, R. Lee, S. Listgarten, D. Eclwards, P. Neumann, H. Javitz, and A. Valdes, IDES: “The Enhanced Prototype. A Real-Time Intrusion Detection System”, Tech. report, Technical Report SRI Project 4 185-010, SRI- CSL-88, 1988.
4. Zorana Bankovic, “Improving network security using genetic algorithm approach, ETSI Telecomunicacion”, computers and electrical engineering, year 2007, pp.no 1-14
5. Anderson, J. P. “Computer Security Threat Monitoring and Surveillance”, Technical report, published on February 26 1980.
6. Beigh, Bilal Maqbool, and M. A. Peer. "Intrusion Detection and Prevention System: Classification and Quick." (2011).
7. Haystack. “An intrusion Detection System” published in Aerospace computer security applications conference, 1988., fourth IEEE, pp.37-44
8. “Adaptive real time anomaly detection using inductively generated sequential patterns”, published in Research in security and privacy ,1990. Proceedings., 1990 IEEE Computer Society Symposium. Pp. 278-284

9. Aurobindo Sundaram. An “introduction to intrusion detection systems” published in Magazine- special issues on computer security volume 2 issue 4, March 1996, pp 3-7

10. M. M. Pillai, J. H. P. Eloff, H. S. Venter, “An Approach to Implement a Network Intrusion Detection System using Genetic Algorithms”, Proceedings of SAICSIT, pp:221- 228, 2004.

11. M. Middlemiss, G. Dick, “Feature selection of intrusion detection data using a hybrid genetic algorithm/KNN approach”, Design and application of hybrid intelligent systems, IOS Press Amsterdam, pp.519-527, 2003.

12. M. Crosbie, E. Spafford, “Applying Genetic Programming to Intrusion Detection”, Proceedings of the AAAI Fall Symposium, 1995.

13. R. H. Gong, M. Zulkernine, P. Abolmaesumi, “A Software Implementation of a Genetic Algorithm Based Approach to Network Intrusion Detection”, 2005.

14. W. Li, “Using Genetic Algorithm for Network Intrusion Detection”. “A Genetic Algorithm Approach to Network Intrusion Detection”. SANS Institute, USA, 2004.

15. W. Lu, I. Traore, “Detecting New Forms of Network Intrusion Using Genetic Programming” Computational Intelligence, vol. 20, pp. 3, Blackwell Publishing Malden, pp. 475-494, 2004.

16. Anjali karar and Manju khari. “Intrusion detection and fighting with intrusions : a survey vsrd” International Journal of Computer Science & Information Technology, Vol. 3 No. 6 June 2013. Pp no 236

17. R. G. Bace, “Intrusion Detection”, Macmillan Technical Publishing. 2000.

18. 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), Vol.4, No.2, March 2012 p.no 111

19. T. Lunt, R. Jagannathan, R. Lee, S. Listgarten, D. Eclwards, P. Neumann, H. Javitz, and A. Valdes, IDES: “The Enhanced Prototype. A Real-Time Intrusion Detection System”, Tech.report, Technical Report SRI Project 4 185-010, SRI- CSL-88, 1988.

20. D. Anderson, T. Frivold, and A. Valdes, “Next-generation intrusion detection expert System (NIDES): A summary”, SRI International, Computer Science Laboratory, 1995.

21. D. Anderson, T.F. Lunt, H. Javitz, A. Tamaru, and A. Valdes, “Detecting unusual Program behavior using the statistical component of the Next-generation Intrusion Detection Expert System (NIDES)”, SRI International, Computer Science Laboratory, 1995.

22. U. Lindqvist and P.A.Porras, “Detecting computer and network misuse through the Production based expert system toolset (P-BEST”), Proceedings of the IEEE Symposium on Security and Privacy, 1999, pp. 146–161.

23. “Intrusion Detection System Techniques: A Review”, International Journal of Advanced Research in Computer Science & Software Engineering, Volume 3, Issue 4, April 2013.

24. S. Axelsson, “Intrusion detection systems: A survey and taxonomy”, Tech. Report 99-15, Chalmers University of Technology, Department of Computer Engineering, 2000.

25. J. Lee, S. Moskovics, and L. Silacci, “A Survey of Intrusion Detection Analysis Methods,” 1999.

27. A. Jones and R. Sielken, “Computer system intrusion detection: A survey”, Tech report, Department of Computer Science, University of Virginia, Thornton Hall Charlottesville, VA, September 2000.

28. J. McHugh, “Intrusion and intrusion detection”, International Journal of Information Security 1(2001), no. 1, 14–35

29. 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), Vol.4, No.2, March 2012 pp.no 111

30. Sectools.Org: 2006 Results; http:// sectools.org/tools2006.html

31. SecTools.Org: Top 125 Network Security Tools; http://sectools .org/tag/ids/

32. Snort (software); http:// en.wikipedia .org /wiki/Snort_%28software%29

33. InfoWorld, The greatest open source software of all time, 2009; http://www.infoworld.com /d/opensource/greatest-open-source-software-all-time-776?source=fssr

34. Suricata (software); http:// en.wikipedia .org/wiki/Suricata_(software)

35. The Bro Network Security Monitor; http://bro-ids.org

36. R. Graham, “FAQ: Network Intrusion Detection Systems”. March 21, 2000.

37. S.E. Smaha, Haystack: “An intrusion detection system”, Aerospace Computer Security Applications Conference, 1988. Fourth, 1988, pp. 37–44

38. Mostaque Md. Morshedur Hassan “Current studies on intrusion detection system genetic algorithm and fuzzy logic” International Journal of Distributed and Parallel Systems (IJDPS) Vol.4, No.2, pp,36 March 2011

39. Atul Garg et. al “Mobility Management-Framework, Issues and challemges”, international journal of Applications or innovations in engineering and management, volume 3,issue 3,March 2014

40. Juneja D., Chawla R. and Singh A., “An Agent-Based Framework to counter attack DDoS Attacks”. International Journal of Wireless Networks and Communications, Vol. 1, No. 2, pp. 193 – 200, 2009.