Ijesm
Consulting, help, relaxation
INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & MANAGEMENT

A REVIEW ON VARIETY OF INTRUSION DETECTION SYSTEM AND THEIR FUNCTIOAL APPROACHES

Dheerendra Kumar Patel [1] , Raj Kumar Paul [2]
M.Tech Student, Department of Computer Science & Engineering, Vedica Institute of Technology, Bhopal (M.P.)-India[1]
Assistant Professor & HOD, Vedica Institute of Technology, Bhopal (M.P.), RKDF University, Bhopal (M.P.)[2]
er.dheerendrapatel@gmail.com

Abstract— It is being found that the increase of variety of network types network protection becomes a great challenge. This leads the necessity increase for data and increasingly exchanging information. Intrusion Detection Systems (IDS) are there to try to abolish unauthorized use of it in way of identifying abuse and misuse of computer systems. In response to the growth in the use and development of IDSs, it would most important aspect. In this article, we identify a number of general technical optimization of IDS. This item Provides die details of the methodology, including strategies for intrusion. This article contains also general information about IDS intrusions and our work to motivate. This article deals with mainly various methods of optimization and classification. Here different approaches are mentioned associated with Intrusion Detection Systems.

Keywords: Classifiers, Decryption, Encryption Intrusion Detection System, Optimization techniques, Mobile Agent etc.

INTRODUCTION

Computer security is an approach of preventing and detecting unauthorized use of the device. Preventive measures help us to prevent unauthorized users from accessing a portion of the computer system (also known as "intruders"). Recognition helps us to determine if someone is trying to enter our system if it was successful, and what can be done [1]. Computers are used for anything from banks and investing to shopping and communicating with others via e-mail or programs [2]. Probably they do not want to read strangers email computer attack with or intrusion Other systems, sending fake e-mail messages or computers, or checking personal data stored on your computer (such as annual accounts). Intruders (also known as attackers, biscuits) do not take our identity [3]. They often want to take control of your computer so they can use it to start attacks on other computer systems.

Intrusion detection systems (IDSs) are usually deployed along with other preventive security mechanisms, such as access control and authentication, as a second line of defense that protects information systems. There are several reasons that make intrusion detection a necessary part of the entire defense system. First, many traditional systems and applications were developed without security in mind. In other cases, systems and applications were developed to work in a different environment and may become vulnerable when deployed Intrusion detection complements these protective mechanisms to improve the system security. Moreover, even if the preventive security mechanisms can protect information systems successfully, it is still desirable to know what intrusions have happened or are happening, so that we can understand the security threats and risks and thus be better prepared for future attacks.

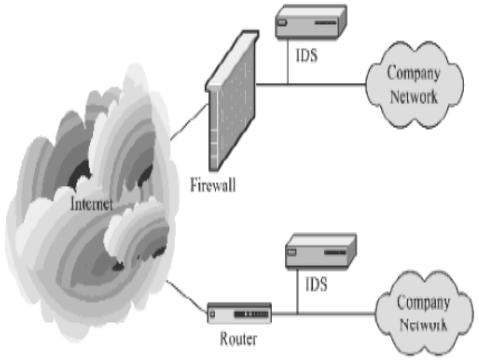

Fig 1:- IDS

The attack can be launched in term of fast attack or slow attack. Fast attack can be defined as an attack that uses a large amount of packet or connection within a few second [4]. Meanwhile, slow attack can be defined as an attack that takes a few minutes or a few hours to complete [6] . Both of the attack gives a great impact to the network environment due to the security breach decade. As in Fig:-1, Currently IDS is used as one of the defensive tools in strengthens the network security especially in detecting the first two phases of an attack either in form slow or fast attack An intrusion detection

system can be divided into two approaches which are behavior based (anomaly) and knowledge based (misuse) [8], [9]. The behavior based approach is also known as anomaly based system while knowledge based approach is known as misuse based system [10], [11].The misuse or signature based IDS is a system which contains a number of attack description or signature that are matched against a stream of audit data looking for evidence of modeled attack [12]. The audit data can be gathered from network traffic or an application log. This method can be used to detect previous known attack and the profile of the attacker has to be manually revised when new attack types are discovered. Hence, unknown attacks in network intrusion pattern and characteristic might not be capture using this technique [13].Meanwhile, the anomaly based system identifies the intrusion by identifying traffic or application which is presumed to be normal activity on the network or host . The anomaly based system builds a model of the normal behavior of the system and then looks for anomalous activity such as activities that do not confirm to the established model. Anything that does not correspond to the system profile is flagged as intrusive. False alarms generated by both systems are major concern and it is identified as a key issues and the cause of delay to further implementation of reactive intrusion detection system [16].

INTRUSION DETECTION SYSTEM DESCRIPTION

An intrusion detection system is a software program which helps to identify the malicious program which enter our system or in network. It helps to secure our system by responding to the malicious program. It is divided into two types. They are host based intrusion detection system and network based intrusion detection system. The active system will respond to the malicious program. But the passive system will detect only whether any malicious packets entered the system or not [12].

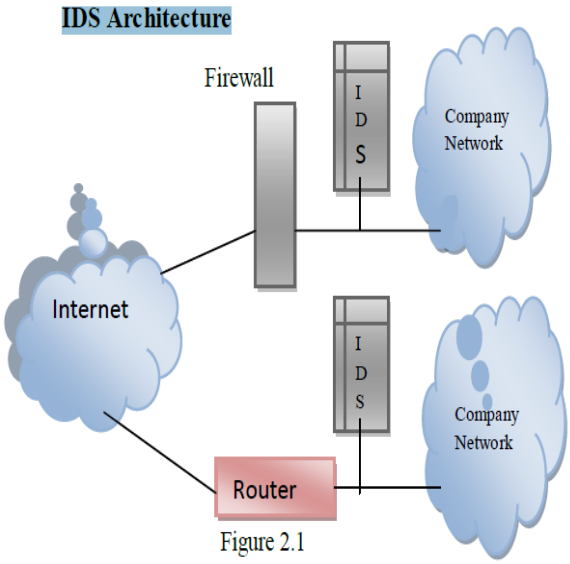

Figure 2.1

Intrusion detection system came into picture around 1980 with the publication of John Anderson's Computer Security Threat Monitoring and Surveillance, which was one of the earliest papers in the field. "An Intrusion Detection Model", published in 1987, provided a methodological framework that inspired many researchers and laid the groundwork for commercial products [17].

Intrusion Detection System (IDS) are the popular and useful tools for enhancing the security of the system and because of their value; they have now become a very important part of modern network security technology. Intrusion detection (ID) is a type of security management system for various computers as well as networks. An Intrusion Detection System collects all the information from the Host or the networks which include both anomaly and misuse intrusions. Intrusion detection functions include:

- ✓ Monitoring and analysing both user and system activities,
- ✓ Analysing system configurations and vulnerabilities,
- ✓ Assessing system and file integrity.

IDS CATEGORIES

There exist multiple categories of intrusion detection systems according to their functionality and behavior. In general IDS can be categorized in two ways: one is Host based Intrusion Detection System (HIDS) and another one is Network Intrusion Detection System (NIDS).there are some another ways to differentiate IDSs. Some of them are mentioned here:

Network Intrusion Detection Systems (NIDS): It usually consists of a network appliance (or sensor) with a Network Interface Card (NIC) operating in promiscuous mode and a separate management interface. It is strengthened with lower cost, real time packet detection along with operating system independence.

Host Intrusion Detection Systems (HIDS): A HIDS and software applications (agents) installed on workstations which are to be monitored. The agents monitor the operating system and write data to log files and/or trigger alarms. A HIDS can only monitor the individual workstations on which the agents are installed and it cannot monitor the entire network [14-15].it strengthened with log based analysis of attacks and also easy to implement.

Active Intrusion Detection Systems: An active Intrusion Detection Systems is configured to automatically block suspected attacks without any intervention required by an operator. Intrusion Detection and Prevention System has the advantage of providing real-time corrective action in response to an attack. It is also termed as Intrusion Detection and Prevention System (IDPS).

Active Intrusion Detection Systems: It is configured to only monitor and analyze network traffic activity and alert an operator to potential vulnerabilities and attack.

Anomaly Based IDS: It is signature based IDS, functions with learnt baseline behavior

Signature Based IDS: A knowledge-based (Signature-based) Intrusion Detection Systems (IDS) references a database of previous attack signatures and known system vulnerabilities. The meaning of word signature, when we talk about Intrusion Detection Systems (IDS) is recorded evidence of an intrusion or attack.

MOBILE AGENT BASED IDS:

While mobile agents [5-11] do not directly improve the techniques for detection, they can reshape the way the techniques are applied, thereby improving efficiency and effectiveness

IDS PARALANCES

There is need of awareness of different terminologies corresponding to IDS and its better performances. Some of them are enlisted below:

- ***True Positive*:** A true positive means that the IDS device recognized and responded to an attack [15].
- ***True Negative:*** This means that non-offending or benign traffic did not trigger an alarm [15].
- ***False Negative*:** A false negative occurs when attack traffic does not trigger an alert on the IDS device. This is often viewed as the worst type of false alarm—for obvious reasons [15].
- ***True Alarms*:** The two types of true alarms in IDS terminology are true positive and true negative. Both are desirable [19].
- ***False Alarms*:** False alarms are IDS events that are not supposed to be occurring in implementation. The two types of false alarms are false positives and false negatives. Both are undesirable [15].
- ***False Positive:*** A false positive means that an alert has been triggered, but it was for traffic that does not constitute an actual attack. This type of traffic is often called benign traffic [15].
- ***Vulnerability:*** Vulnerability is a weakness that compromises the security or functionality of a particular system in your network

RELATED WORK

In Intrusion detection system, a lot of research work is going on these days to improve the performance of system and the networks. The research work that has been done in the field of Mobile Agent based Intrusion Detection Systems (MA-IDSs) focusing upon its architecture, technique, strength and weakness is discussed in this paper. Intrusion is an act which is undesirable and can lead to losses in many forms of different magnitudes. Intrusion detection (ID) is a very important tool which not only detects the intrusion of unauthorized and suspicious activities that can compromise the security pillars (Authentication, availability, Confidentiality and Integrity) of data or information. In [5] IDS with the integration of Mobile Agents is presented which looks after the anomalies and responds by taking suitable measures with the help of agents.

Mobile agent approach: Mobile agent Monitoring the neighboring nodes and collect the information from neighboring home agent to determine the co relation among the observed anomalous pattern before it send the data. This approach provides security to current node, neighboring node and global network.

Peer to Peer Intrusion Detection System: In peer to peer IDS, suspicious activities are checked by sending the detection request to other hosts of the system. It is used to avoid single point failure. The six types of agents discussed in this model are-Monitor Agent, Analysis Agent, Executive Agent and Manager Agent are static agents whereas Retrieval Agent and Result Agent are dynamic agents.

Intrusion Detection based on SNORT: The snort and sniffer is open application software both are used to detect the malicious activity on distributed intrusion detection system. This includes overcoming latency, reducing network load and adapting dynamic environments [28].

Multilevel Anomalies Detection approach: In existing architecture, implementation of "Plug-in" used in anomalies detection system (ADS), so ADS need signatures' database and in computer system for movable

nature ADS suffers a big outgoing flow. This centralized ADS architecture correlates in single level after taking incoming events.

Central coordinator approach: The architecture for IDS on mobile agent detects the complex attack to the networks. It imposes the light load on entire network and thus detects the suspicious activity.

Issues: Present-day IDSs are less than perfect. Developers continue to address shortcomings through the improvement and refinement of existing techniques, but some shortcomings are inherent in the way IDSs are constructed. The most common shortcomings include the following items:

Lack of efficiencies: This requirement is difficult to meet when faced with a very large number of events as is typical in today's networks.

Burdensome Maintenance: The configuration and maintenance of intrusion detection systems often requires special knowledge and substantial effort.

Flexibility: Intrusion detection systems have typically been written for a specific environment and have proved difficult to use in other environments that may have similar policies and concerns. There is a consolidated information in Table 1 given below which contains different agent based IDS approaches and their strengths

Table 1: Agent Based IDS Review

ARCHITECTURE	APPROACH	TECHNIQUE	STRENGTH
Adhoc based	Destination Sequence Distance Vector Routing(DSDV)	Authentication mechanism(RSA 1024, AES 128) Clustering of mobile agent	Low routing, less overhead
Adhoc based	Anomaly detection using MA	Bayesian classification	High rate of anomaly, Reduced false alarm
Distributed based	Anomaly detection	Event correlation engine, Agent synergy	Reduced false alarm rate, ID is greater than SNORT
Hybrid and Distributed based	Distributed multilevel(synchronous and distributed correlation) approach	SynFlooding	Least result of false positive rate, false negative rate, semantic detection
Distributed	Immune based	Dynamic clonal selection algorithm and collaborative signal mechanism	Reduced false positive rate, Increased detection rate
Distributed	SNORT based	Message exchange between server and SNORT	SNORT performance is good
Distributed	Peer to peer IDS	Retrieval agent generation, retrieval agent dispatch	Efficient migration strategies, MADIDF is better than MASHD
Distributed	Central coordination peer to peer IDS	Agent based	Less load on entire network, detection more complex, distributed attack

ARIOUS OPTIMIZATION TECHNIQUES

IDS use several techniques, which involve the IDS stopping the attack itself, changing the security environment (e.g., reconfiguring a firewall), or changing the attack's content.

The types of IDS technologies are differentiated primarily by the types of events that they monitor and the ways in which they are deployed.

A. Network Behavior Analysis (NBA), which examines, network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service (DDoS) attacks, certain forms of malware, and policy violations (e.g., a client system providing network services to other systems). Behavior-based analysis learns the normal behavior of traffic and systems and then continually examines them for potentially harmful anomalies and for behavior that frequently accompanies incidents. This approach recognizes attacks based on what they do, rather than whether their code matches strings used in a specific past incident. —It stops traffic that is not malicious on its face but that will do malicious things said Allan Paller [18].

B. Wireless

This technique monitors wireless network traffic and analyzes it to identify suspicious activity involving the wireless networking protocols themselves [19].

C. Host-based

It can analyze activities on the host it monitors at a high level of detail, it can often determine which processes and/or users are involved in malicious activities. Though they may each focus on a single host, many host-based IDS systems use an agent-console model where agents run on (and monitor) individual hosts but report to a single centralized console (so that a single console can

configure, manage, and consolidate data from numerous hosts). Host-based IDSs can detect attacks undetectable to the network-based IDS and can gauge attack effects quite accurately [20].

Refer various Optimization techniques are listed below in Table 2:
Table 2: Optimization techniques

S. No.	Techniques	Brief
1	Network Behavior	examines, network traffic to identify threats that generate unusual traffic flows
2	Wireless	technique monitors wireless network traffic and analyzes
3	Host-based	It use an agent-console model where agents run on (and monitor) individual hosts but report to a single centralized console (so that a single console can configure, manage, and consolidate data from numerous hosts).

VARIOUS CLASSIFICATION TECHNIQUES

The following criteria will be adopted in the classification of the IPS/IDS:

Reliability: The generated alerts must be justified and no intrusion to escape.

Reactivity: An IDS/IPS must be capable to detect and to prevent the new types of attacks as quickly as possible. Thus, it must constantly self-update. Capacities of automatic update are so indispensable.

Facility of implementation and adaptability: An IDS/IPS must be easy to function and especially to adapt to the context in which it must operate. It is useless to have an IDS/IPS giving out some alerts in less than 10 seconds if the resources necessary to a reaction are not available to act in the same constraints of time.

Performance: the setting up of an IDS/IPS must not affect the performance of the supervised systems. Besides, it is necessary to have the certainty that the IDS/IPS has the capacity to treat all the information in its disposition because in the reverse case it becomes trivial to conceal the attacks while increasing the quantity of information. These criteria must be taken into consideration while classifying an IDS/IPS, as well:

- ✓ The sources of the data to analyze, network, system or application
- ✓ The behaviour of the product after intrusion passive or active
- ✓ The frequency of use, periodic or continuous
- ✓ The operating system in which operate the tools, Linux, Windows, etc.
- ✓ The source of the tools, open or private [21].

Various Classifiers are listed below:

Table 3: Classifiers

S. No.	Techniques	Methods
1	Soft Computing Based	Neural Network
		Genetic Algorithm
		Fuzzy
2	Tree Based	J48
		ID3
		CART
3	Others	Binary, etc

PREVIOUS WORK

Intrusion Detection System (IDS) has been used as a vital instrument in defending the network from this malicious or abnormal activity. it is still desirable to know what intrusions have happened or are happening, so that we can understand the security threats and risks and thus be better prepared for future attacks With the ability to analyze network traffic and recognize incoming and ongoing network attack, majority of network administrator has turn to IDS to help them in detecting anomalies in network traffic In this paper, we focus on different types of attacks on IDS this paper gives a description of different attack on different protocol such as TCP ,UDP,ARP and ICMP [22]

Web servers are ubiquitous, remotely accessible, and often misconfigured. In addition, custom web-based applications may introduce vulnerabilities that are overlooked even by the most security-conscious server administrators. Consequently, web servers are a popular target for hackers. To mitigate the security exposure associated with web servers, intrusion detection systems are deployed to analyze and screen incoming requests. The goal is to perform early detection of malicious activity and possibly prevent more serious damage to the protected site. Even though intrusion detection is critical for the security of web servers, the intrusion detection systems available today only perform very simple analyses and are often vulnerable to simple evasion techniques. In addition, most systems do not provide sophisticated attack languages that allow a system administrator to specify custom, complex attack scenarios to be detected. This paper presents WebSTAT, an intrusion detection system that analyzes web requests

looking for evidence of malicious behavior. The system is novel in several ways. First of all, it provides a sophisticated language to describe multistep attacks in terms of states and transitions. In addition, the modular nature of the system supports the integrated analysis of network traffic sent to the server host, operating system-level audit data produced by the server host, and the access logs produced by the web server. By correlating different streams of events, it is possible to achieve more effective detection of web-based attacks. [23]

[25]In this paper capturing of network traffic, performance and reports analysis generated by snort and corresponding alert ratio of signatures for the particular attack are to be evaluated. This intrusion detection system is one of the security defense tools for computer networks. In recent years this research has lacked in direction and focus today SNORT stands out as the most widely deployed IDS, We survey the existing techniques, types and architectures of Intrusion Detection Systems in the literature. Performance analysis of real time Intrusion Detection and prevention system and traffic analysis by Snort from the network are to carried out.

[26] In this system we addressed the dual problem of Accuracy and Efficiency for building robust and efficient intrusion detection systems. This method is much suitable for detecting R2L and U2R attacks.

[27] Here a methodology of applying classification technique for IDS using data mining, in use genetic algorithm into network intrusion detection techniques. A brief overview of Intrusion Detection System (IDS), genetic algorithm, and related detection techniques are discussed.

[28] This article outlines and surveys about anomaly based intrusion detection system and that is around, as well as highlights the deficiencies. In this paper we have discuss the types of anomalies and anomalies and theoretical methods to detect them.

[29] Snort is mostly used signature based IDS because of it is Lightweight and open source software. Basic analysis and security engine (BASE) is also used to see the alerts generated by Snort. In this paper the signature-based Network intrusion detection using Snort and WinPcap implemented.

[30] To make our information or network protected, it is the key problem to detect the intruders while various authors designed the system for the detection of intrusion and also Proposed the method such as neural network, decision tree, hidden markov model.

IDS TOOLS

SNORT: Snort is network intrusion detection and prevention system capable of performing real-time traffic analysis and packet logging on IP networks. Initially called a “lightweight” intrusion detection technology, Snort has evolved into a mature, feature-rich IPS technology that has become the de facto standard in intrusion detection and prevention. With over 4 million downloads and nearly 400,000 registered users, it is the most widely deployed intrusion prevention technology in the world. Snort can perform protocol analysis and content searching/matching [18].

WEKA:

WEKA is a data mining system developed by the University of Waikato in New Zealand that implements data mining algorithms. WEKA is a state-of-the-art facility for developing machine learning (ML) techniques and their application to real-world data mining problems. It is a collection of machine learning algorithms for data mining tasks. The algorithms are applied directly to a dataset. WEKA implements algorithms for data preprocessing, classification, regression, clustering, association rules; it also includes a visualization tools. The new machine learning schemes can also be developed with this package. WEKA is open source software issued under the GNU General Public License

RISK ANALYSIS

Risks in packets: There are some possible risks are enlisted in the Table 4: Risk Table. These are responsible for adverse service behavior.

Table 4: Risk Review

Intrusion	Protocol	Description (Risks for Services)
SYN Flooding	TCP	Sending large numbers of TCP connection initiation requests to the target. The target system must consume resources to keep track of these partially open connections.
Teardrop	TCP fragments	Sends overlapping IP fragments.
Smurf	ICMP	ICMP ping requests to a directed broadcast address. The forged source address of the request is the target of the attack. The recipients of the directed broadcast ping request respond to the request and flood the target's network.
Open/Close	TCP/UDP	The open/close attack opens and closes connections at a high rate to any port serviced by an external service through intend. The number of connections allowed is hard coded inside intend.
ICMP Unreachable	ICMP	. This causes the TCP session to retry and as more “ICMP unreachable”

		messages are sent, a DoS condition occurs.
ICMP Redirect	ICMP	ICMP redirects can cause data overload to the system being targeted.
Land	TCP SYN	Source and destination IP addresses are the same causing the response to loop.
Ping of Death	ICMP	ICMP packets greater than 65536 bytes can shut down a system.

CONCLUSION

The main objective of this paper is to provide an overview of the necessity and utility of intrusion detection system. This paper gives complete study about types of IDS, life cycle, various domains, types of attacks. IDS are becoming essential for day today security in corporate world and for network users. IPS defines about the preventing measures for the security. In the lifecycle the phases developed and the stages are illustrated. Still, there are more challenges to overcome. The techniques of anomaly detection and misuse detection are specifically illustrated and more techniques can be used. Further Work will be done on comparative analysis of some popular data mining algorithms (classier) applied to IDS and enhancing a classification based IDS by various optimization techniques.

References

[1] Wang Yu, Cheng, Xiaohui and Wang Sheng ,"Anomaly Network Detection Model Based on Mobile Agent", IEEE,Third International Conference on Measuring Technology and Mechatronics Automation, 2011

[2] Jaydip Sen "An Agent-Based Intrusion Detection System for Local Area Networks" published in International Journal of Communication Networks and Information Security (IJCNIS) Vol. 2, No. 2, August 2010 PP 128-140

[3] Mr. Suryawanshi G.R, Prof. Vanjale S.B "Mobile Agent for Distributed Intrusion detection System in Distributed System" Publication in" International Journal of Artificial Intelligence and Computational Research (IJAICR.) ", Jan-June 2010 . ISSN-0975-3974. PP 1-8.

[4] Nicholas J. Puketza, Kui Zhang, Mandy Chung, Biswanath Mukherjee*, Ronald A. Olsson, "A Methodology for Testing Intrusion Detection Systems".

[5] Ionita, I.; Ionita, L. "An agent-based approach for building an intrusion detection system" Published in Networking in Education and Research, 2013 RoEduNet International Conference 12th Edition 26-28 Sept. 2013 Page(s):1 - 6 ISSN :2068-1038 Print ISBN: 978-1-4799-2599-5

[6] Faizal, M.A., Mohd Zaki M., Shahrin Sahib, Robiah, Y., Siti Rahayu, S., and Asrul Hadi, Y. "Time Based Intrusion Detection on Fast Attack for Network Intrusion Detection System", Second International Conference on Network Applications, Protocols and Services, IEEE, 2010.

[7] Jitendra S Rathore, Praneet Saurabh, Bhupendra Verma "AgentOuro: A Novelty Based Intrusion Detection and Prevention System" Computational Intelligence and Communication Networks (CICN), 2012 Fourth International Conference on 3-5 Nov. 2012 Page(s): 695 - 699

[8] Cuppen, F. & Miege, A. (2002). Alert Correlation in a Cooperative Intrusion Detection Framewok. In Proceeding of the 2002 IEEE Symposium on Security and Privacy. IEEE, 2002]

[9] Cabrera, J.B.D., Ravichandran, B & Mehra R.K. (2000). Statistical Traffic Modelling for Network Intrusion Detection. In Proceeding of the IEEE Conference.

[10] Yeophantong, T, Pakdeepinit, P., Moemeng, P & Daengdej, J. (2005).Network Traffic Classification Using Dynamic State Classifier. In Proceeding of IEEE Conference

[11] Farah J., Mantaceur Z. & Mohamed BA. (2007). A Framework for an Adaptive Intrusion Detection System using Bayesion Network. Proceeding of the Intelligence and Security Informatics, IEEE, 2007.

[12] Cabrera, J.B.D., Ravichandran, B & Mehra R.K. (2000). Statistical Traffic Modelling for Network Intrusion Detection. In Proceeding of the IEEE Conference.

[13] Sekar, R., Gupta, A., Frullo, J., Shanbhag, T., Tiwari, A., Yang, H. & Zhou, S. (2002). Spesification-based Anomaly Detection: A New Approach for Detecting Network Intrusions. In Proceeding of CCS ACM Conference.

[14]E. Lundin, E. Jonsson, Survey of research in the intrusion detection area, Technical report 02-04, Department of Computer Engineering, Chalmers University of Technology, Göteborg January 2002, http://www.ce.chalmers.se/staff/emilie/papers/Lundin_survey02.pdf.

[15] Stonesoft Corp. Stonesoft Corp "Intrusion Detection and Analysis for Active Response - Version 1.2" available

[16] Karl Levitt. (2002). Intrusion Detection: Current Capabilities and Future Direction. Proceeding of IEEE Conference of the 18th Annual Computer Security Application, IEEE, 2002.

[17] Anderson, J.P., 1980. Computer Security and Threat Monitoring Surveillance. Technical report at Co. Fort Washington Pennsylvania.

[18] David Geer, Behavior-Based Network Security Goes Mainstream, IEEE,14-17, march 2006

[19] Tiwari Nitin, S. R. Singh and P. G. Singh, Intrusion Detection and Prevention System (IDPS) Technology-Network Behavior Analysis System (NBAS), International Science Congress Association , 51-56, July (2012).
[20] Karen Scarfone, Peter Mell, Guide to Intrusion detection and prevention systems (IDPS), NIST, 1 to 127, 2007.
[21] B. Santos Kumar et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 4 (1) , 2013, 77 – 82, "Intrusion Detection System- Types and Prevention".
[22] Volume 2, Issue 8, August 2012, " An Overview on Intrusion Detection System and Types of Attacks It Can Detect Considering Different Protocols".
[23] Giovanni Vigna William Robertson Vishal Kher Richard A. Kemmerer, "A Stateful Intrusion Detection System for World-Wide Web Servers".
[24] C. Krügel, T. Toth, Applying Mobile Agent Technology to Intrusion Detection, ICSE Workshop on Software Engineering and Mobility, Toronto May 2001
[25] Mukesh Sharma,Akhil Kaushik, Amit Sangwan Performance Analysis of Real Time Intrusion Detection and Prevention System using Snort.,IJERT, July – 2012
[26] Vaishali T.Deshmukh, Shubhangi Vaikole, Layered Crf A Model To Build More Accurate Intrusion Detection System, IJERT, October – 2012
[27] Bhavana G.Rathwa,Prof.Purnima Singh Genetic Algorithm Methodology for Intrusion Detection System, IJERT,December- 2012
[28] Vasima Khan, Anomaly Based Intrusion Detection And Prevention System, IJERT, March – 2013
[29] Sagar N. Shah , Ms. Purnima Singh ,Signature-Based Network Intrusion Detection System Using SNORT And WINPCAP, IJERT, December- 2012
[30] Preeti Singh, Amrish Tiwari, A Review Intrusion Detection System using KDD'99 Dataset, IJERT, 2014