American Journal of Information Systems, 2016, Vol. 4, No. 3, 69-88
Available online at http://pubs.sciepub.com/ajis/4/3/2
©Science and Education Publishing
DOI:10.12691/ajis-4-3-2

A Survey on Secure Network: Intrusion Detection & Prevention Approaches

Manu Bijone[*]

M.Tech-Computer Science and Engineering, Lakshmi Narain College of Technology-Indore (RGPV, Bhopal), MP, India
*Corresponding author: mbijone@gmail.com

Abstract With the growth of the Internet and its potential, more and more people are getting connected to the Internet every day to take advantage of the e-Commerce. On one side, the Internet brings in tremendous potential to business in terms of reaching the end users. At the same time it also brings in lot of security risk to the business over the network. With the growth of cyber-attacks, information safety has become an important issue all over the world. Intrusion detection systems (IDSs) are an essential element for network security infrastructure and play a very important role in detecting large number of attacks. This survey paper introduces a detailed analysis of the network security problems and also represents a review of the current research. The main aim of the paper is to finds out the problem associated with network security for that various existing approaches related to intrusion detection and preventions are discussed. This survey focuses on presenting the different issues that must be addressed to build fully functional and practically usable intrusion detection systems (IDSs). It points out the state of the art in each area and suggests important open research issues.

Keywords: *network security, intrusion detection system, cyber attacks, intrusion prevention system, data security, artificial neural networks, computer network, soft computing, swarm intelligence, fuzzy system*

Cite This Article: Manu Bijone, “A Survey on Secure Network: Intrusion Detection & Prevention Approaches.” *American Journal of Information Systems*, vol. 4, no. 3 (2016): 69-88. doi: 10.12691/ajis-4-3-2.

1. Introduction

The intrusion detection field has grown considerably in the last few years, and a large number of intrusion detection systems have been developed to address different needs. Many historical events have shown that intrusion prevention techniques alone, such as encryption and authentication, which are usually a first line of defense, are not sufficient. As the system become more complex, there are also more weaknesses, which lead to more security problems. Intrusion detection can be used as a second wall of defense to protect the network from such problems. If the intrusion is detected, a response can be initiated to prevent or minimize damage to the system. After the perimeter controls, firewall, and authentication and access controls block certain actions, some users are admitted to use a computing system. Most of these controls are preventive: they block known bad things from happening. Intrusion detection systems (IDS) complement these preventive controls as the next line of defense.

The definition of an intrusion detection system does not include preventing the intrusion from occurring, only detecting it and reporting it to an operator. There are some intrusion detection systems (IDPS) that try to react when they detect an unauthorized action occurring. This reaction usually includes trying to contain or stop the damage, for example, by terminating a network connection. When an IDS detects an intrusion, it logs the event, store relevant data/traffic, notify an administrator, and in some cases it will try to intervene. Besides the obvious advantages of an IDS, the stored data and the logs provide valuable forensic information and may be used as evidence in a legal case against the attacker. Most intrusion detection systems try to perform their task in real time, but there are also intrusion detection systems that do not operate in real time, either because of the nature of the analysis they perform, or because they are geared for forensic analysis.

An IDS is much like an alarm system, some being more advanced and intelligent than others. When building an IDS one needs to consider many issues, such as data collection, data pre-processing, intrusion recognition, reporting, and response. Among them, intrusion recognition is at the heart. Audit data are examined and compared with detection models, which describe the patterns of intrusive or benign behavior, so that both successful and unsuccessful intrusion attempts can be identified. Many intrusion detection systems have been proposed in traditional wired networks, where all traffic must go through switches, routers, or gateways. Hence, IDS can be added to and implemented in these devices easily [22,23]. On the other hand, MANETs do not have such devices. Moreover, the medium is wide open, so both legitimate and malicious users can access it. Furthermore, there is no clear separation between normal and unusual activities in a mobile environment. Since nodes can move arbitrarily, false routing information could be from a compromised node or a node that has outdated information. Thus, the current IDS techniques on wired networks cannot be applied directly to MANETs.

Cloud security is an evolving sub-domain of computer security, network security, and, more broadly, information security. There is a number of security issues/concerns associated with cloud computing but these issues fall into two broad categories: security issues faced by cloud providers (organizations providing software-, platform-, or infrastructure-as-a-service via the cloud) and security issues faced by their customers (companies or organizations who host applications or store data on the cloud) [2,63,64]. In a public cloud enabling a shared multi-tenant environment, as the number of users increase, security risks get more intensified and diverse. It is necessary to identify the attack surfaces which are prone to security attacks and mechanisms ensuring successful client-side and server-side protection [2,63,64]. Private clouds are considered safer in comparison to public clouds; still they have multiple issues which if unattended may lead to major security loopholes.

The performance of intrusion detection is enhanced according to optimal feature subset election, which is gathered from GA and PCA [46]. However, the primary problem is their performance, which can be improved by raising the recognition rates and diminishing false positives. The authors of this paper, for experimentation used KDD cup dataset. This method indicates that the suggested method improved SVM performance in recognition intrusion that becomes batter than current approaches which is capable to increase the detection rates and reduce the number of features. Using and testing other optimization techniques such as (Particle swarm optimize) PSO and (gravity search algorithm) GSA because these optimizations techniques have higher speed in convergence. To improve performances of IDS systems with real network traffic, a large-scale realistic Intrusion Detection data-base is also necessary.

The main aim of the paper is to finds out the problem associated with network security. Paper extracts the issues and focuses on data security and privacy during communication on the network. In the paper, research contributions in each field of network security are systematically summarized and compared, allowing us to clearly define existing research challenges, and to highlight promising new research directions.

The paper is organized as follows. Various types of network attack are given in Section 2. Concepts of IDS are presented in Section 3. Section 4 to 8 deals classification of IDS system. Section 9 gives the idea about IPS systems. Different approaches that are used for IDS and IPS are discussed in Section 10. Conclusion and future work are summarized in Section 11.

2. Network Attacks: Detected by a NIDS

Network attacks can be classified into following three categories as shown in Figure 1:

2.1. Denial of Service (DoS) Attacks

A Denial of Service attack attempts to slow down or completely shut down a target so as to disrupt the service and deny the legitimate and authorized users can access [1,19]. Such attacks are very common in the Internet where a collection of hosts are often used to bombard web servers with dummy requests. Such attacks can cause significant economic damage to ecommerce businesses by denying the customers an access to the business. There are a number of different kinds of DoS attacks, some of which are mentioned below.

Flooding DoS Attacks: In a flooding attack [1,63,64], an attacker simply sends more requests to a target that it can handle. Such attacks can either exhaust the processing capability of the target or exhaust the network bandwidth of the target, either way leading to a denial of service to other users. DoS attacks are extremely difficult to combat, as these do not exploit any vulnerability in the system, and even an otherwise secure system can be targeted.

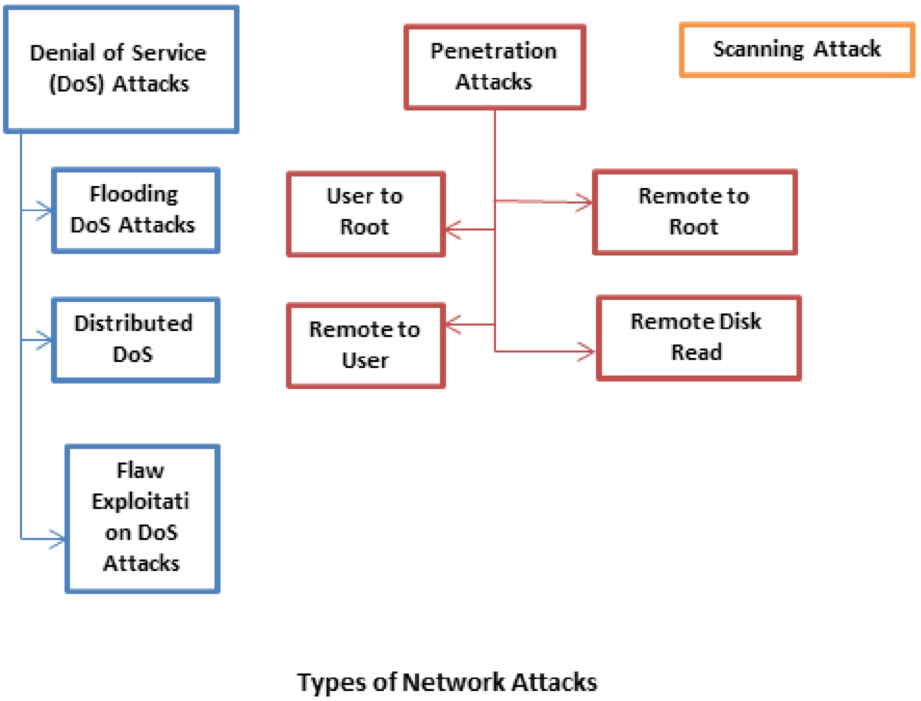

Figure 1. Categories of Network Attacks

Distributed Denial of Service attack (DDoS): A more dangerous version of DoS attack is called Distributed Denial of Service attack (DDoS), which uses a large pool of hosts to target a given victim host [63]. A hacker (called botmaster) can initiate a DDoS attack by exploiting vulnerability in some computer system, thereby taking control of it and making this the DDoS master. Afterwards the intruder uses this master to communicate with the other systems (called bots) that can be compromised. Once a significant number of hosts are compromised, with a single command, the intruder can instruct them to launch a variety of flood attacks against a specified target [20].

Flaw Exploitation DoS Attacks: In such attacks, an attacker exploits a flaw in the server software to either slow it down or exhaust it of certain resources. Ping of death attack is one such well known attack. A ping of death (POD) [63] is a type of attack on a computer that involves sending a malformed or otherwise malicious ping to a computer. A ping is normally 64 bytes in size (or 84 bytes when IP header is considered); many computer systems cannot handle a ping larger than the maximum IP packet size, which is 65,535 bytes. Sending a ping of this size can crash the target computer. Some limitations of the protocol implementation also lead to vulnerability which can be exploited to implement DoS attacks such as DNS amplification attack, which uses ICMP echo messages to bombard a target. For these attacks, a signature can be devised easily, such as to determine a ping of death attack a NIDS needs to check the ping flag and packet size.

2.2. Penetration Attacks

In penetration attack, an attacker gains an unauthorized control of a system, and can modify/alter system state, read files, etc. Generally such attacks exploit certain flaws in the software, which enables the attacker to install viruses, and malware in the system. A penetration test can help determine whether a system is vulnerable to attack, if the defenses were sufficient, and which defenses (if any) the test defeated. A penetration test target may be a *white box* - which provides background and system information) or *black box* - which provides only basic or no information except the company name). The most common types of penetration attacks are:

User to Root: A User to Root (U2R) is an attack that aims to gain super user access to the system. Attacker gain super user access by exploiting vulnerability in operating system or application software. The attacker starts out with access to a normal user account on the system (perhaps gained by sniffing password, a dictionary attack or social engineering) and is able to exploit some vulnerability to gain root access to the system. Improving the detection rate of user to root (U2R) attack classes is an open research problem. Most common attack in this class of attack is buffer overflow attack. Other attacks include Loadmodule, Perl, Ps, Xterm etc.

An extensive set of machine learning and pattern classification techniques trained and tested on KDD dataset failed in detecting most of the *user-to-root* attacks [91]. Paper [91] provides an approach for mitigating negative aspects of the mentioned dataset, which led to low detection rates. Genetic algorithm is employed to implement rules for detecting various types of attacks. Rules are formed of the features of the dataset identified as the most important ones for each attack type. In this way [91] introduce high level of generality and thus achieve high detection rates, but also gain high reduction of the system training time. Thenceforth [91] re-check the decision of the *user-to- root* rules with the rules that detect other types of attacks. In this way [91] decrease the *false-positive rate*. The model was verified on KDD 99, demonstrating higher detection rates than those reported by the state- of-the-art while maintaining low *false-positive rate*.

Remote to User: A Remote to User (R2U) is an attack in which the attacker tries to gain unauthorized access from a remote machine into super user account of the target system. In this type of attack, attacker sends packets to a machine over a network and then exploits some vulnerability to gain local access as a user of that machine. Examples of remote to user attack are Dictionary, Ftp_write, Guest, Imap, Phf etc.

Remote Disk Read: A remote attack is a malicious action that targets one or a network of computers. The remote attack does not affect the computer the attacker is using. Instead, the attacker will find vulnerable points in a computer or network's security software to access the machine or system. In R2DR, an attacker on the network gains access to the inaccessible files stored locally on the host that why it is also called R2L attack.

In order to determine Remote to Local (R2L) attack, an intrusion detection technique based on artificial neural network is presented in [90]. This technique uses sampled dataset from Kddcup99 that is standard for benchmarking of attack detection tools. The back-propagation algorithm is used for training the feed-forward neural network. The developed system is applied to R2L attacks. Moreover, experiment indicates this technique has comparatively low *false positive rate* and *false negative rate*, consequently it effectively resolves the deficiency of existing intrusion detection approaches.

Remote to Root: In R2R, a user across the network gains the complete control of the system.

2.3. Scanning Attack

In such attacks, an attacker sends various kinds of packets to probe a system or network for vulnerability that can be exploited. When probe packets are sent the target system responds; the responses are analyzed to determine the characteristics of the target system and if there are vulnerabilities. Thus scanning attack essentially identifies a potential victim. Network scanners, port scanners, vulnerability scanners, etc. are used which yields following information:

- The network topology.
- The type of firewall used by the system.
- The identification of hosts that are responding.
- The software, operating systems and server applications that are currently running.

Once the victim is identified, the attacker can penetrate them in a specific way. Scanning is typically considered a legal activity and there are a number of examples and applications that employ scanning. The most well-known scanning applications are Web search engines. On the other hand independent individual ay scan a network or the entire Internet looking for certain information, such as a music or video file. Some well-known malicious scanning include Vertical and Horizontal port scanning, ICMP (ping) scanning, very slow scan, scanning from multiple ports and scanning of multiple IP addresses and ports. NIDS signatures can be devised to identify such malicious scanning activity from a legitimate scanning activity with fairly high degree of accuracy [21].

The first step in securing a networked system is to detect the attack. Even if the system cannot prevent the intruder from getting into the system, noticing the intrusion will provide the security officer with valuable information. The Intrusion Detection (ID) can be considered to be the first line of defense for any security system.

3. IDS: Intrusion Detection System

An intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations. Any detected activity or violation is typically reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system combines outputs from multiple sources, and uses alarm filtering techniques to distinguish malicious activity from false alarms [9]. A good definition is given by Rouse [14] in that a SIEM gives the ability to see trends and patterns of security data from a single point of view even though the security data can originate from diverse heterogeneous sources such as the network, end-user devices, servers, firewalls, antivirus systems, and intrusion prevention systems (IPS). SIEM systems are architecturally different than typical IDS solutions, and are the result of computer security vendors in the commercial sector seeking to profit by solving problems that enterprises were experiencing. IDS is considered to be a passive-monitoring system, since the main function of an IDS product is to warn you of suspicious activity taking place − not prevent them. IDSs perform a variety of functions:

- monitoring users and system activity
- identifying abnormal activity through statistical analysis
- recognizing known attack patterns in system activity
- correcting system configuration errors
- installing and operating traps to record information about intruders
- auditing system configuration for vulnerabilities and misconfigurations
- managing audit trails and highlighting user violation of policy or normal activity
- assessing the integrity of critical system and data files

An IDS specifically looks for suspicious activity and events that might be the result of a virus, worm or hacker. This is done by looking for known intrusion signatures or attack signatures that characterize different worms or viruses and by tracking general variances which differ from regular system activity. The IDS is able to provide notification of only known attacks. Some IDS have the ability to respond to detected intrusions. Systems with response capabilities are typically referred to as an intrusion prevention system. Overview of an IDS is shown is Figure 2.

There are many factors to evaluate the IDS such as speed, cost, resource usage, effectiveness, etc. [15]. However, recently false alarms rate and accuracy of detection are happen to be the most important issues and challenges in designing effective IDSs [16]. The effectiveness of IDS is evaluated by its prediction ability to give a correct classification of events to be attack or normal behavior [17]. Wu and Ye [18] compared the accuracy, detection rate, false alarm rate for four attack types: Probe, Dos, U2R, R2L. They provide accuracy comparison of these four kinds of attacks by C4.5 and SVM algorithms. They show that C4.5 acts better than SVM in accuracy of Probe, DoS and U2R attacks detection; but in false alarm rate, SVM is better. They suggest combining the two methods, so that overall accuracy can be increased greatly.

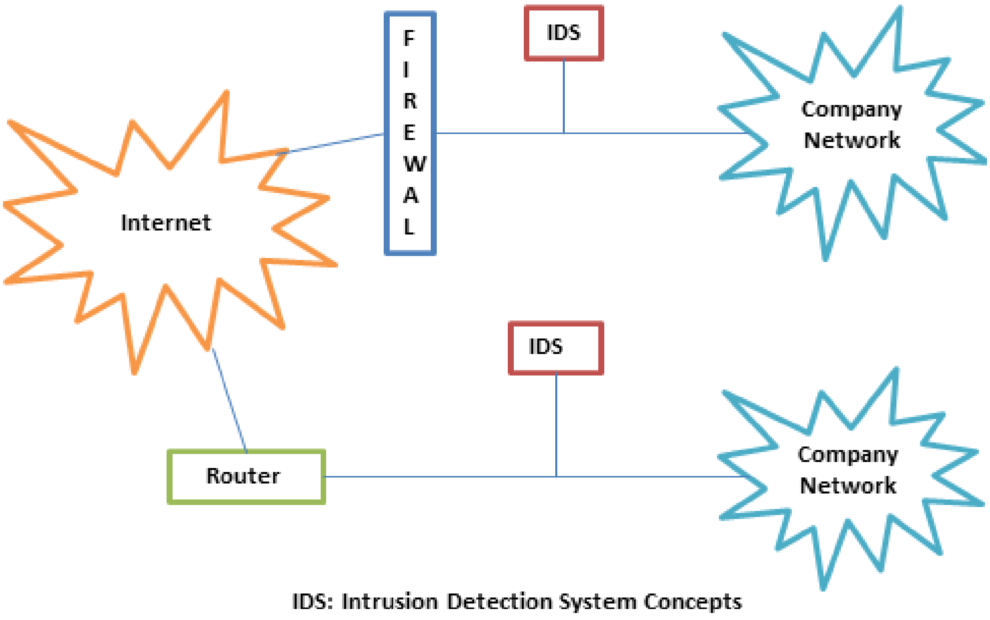

Figure 2. Concepts of IDS

Paper [62] reports a brute force attack event (Brute force attacks with disciplined IPs, DBF) by analyzing log with site-federated viewpoint analysis. The analyses can lead us to the structure of DBF and the existence of attackers behind the DBF. This paper also present TOPASE, which detect victim hosts of DBF. Combining TOPASE and shutting down based on the regularity of DBF can mitigate the DBFs to those victims.

There are many tools available for intrusion detection. Suricata [36] is a free and open source, mature, fast and robust network threat detection engine. It is capable of real time intrusion detection (IDS), inline intrusion prevention (IPS), network security monitoring (NSM) and offline pcap processing. Suricata inspects the network traffic using a powerful and extensive rules and signature language, and has powerful *Lua scripting* support for detection of complex threats.

Figure 3 shows the classification of IDS based on used Methodology. Section 4 to 8 deals classification of IDS system.

3.1. IDS and Firewall

IDS and Firewall appear same but having different concept. While they both relate to network security, an IDS differs from a firewall in that a firewall looks out for intrusions in order to stop them from happening. A firewall forms a barrier through which the traffic going in each direction must pass. A firewall security policy dictates which traffic is authorized to pass in each direction [3]. Also it imposes restrictions on incoming and outgoing Network packets to and from private networks. The firewall limits the access between networks in order to prevent intrusion and does not signal an attack from inside the network. An IDS is not a replacement for either a firewall or a good antivirus program. An IDS evaluates a suspected intrusion once it has taken place and signals an alarm. An IDS also watches for attacks that originate from within a system. The network-based intrusion protection system can also detect malicious packets that are designed to be overlooked by a firewall's simplistic filtering rules.

3.2. IDS and Big Data

Intrusion Detection frequently involves analysis of Big Data, which is defined as research problems where mainstream computing technologies cannot handle the quantity of data. Even a single security event source such as network traffic data can cause Big Data challenges. Analyzing security data across heterogeneous sources can be difficult for Intrusion Detection where homogeneous sources already face Big Data challenges. Integrating across more security sensors would increase Big Data issues in terms of: *Volume* in having to store more information collectively, *Velocity* in that more information would be flowing collectively at a higher rate in and out of the monitoring system, and especially *Variety* in terms of many different types of information coming from very different sources and also collectively yielding higher dimensionality.

When Big Data is present in heterogeneous forms, it can be considered Big Heterogeneous Data regardless of whether that data is input(s) or output(s) of the system. For example, this can arise due to the additive properties of Big Data. If one input is deemed Big Data and is added to another input which is not Big Data, the result will still be Big Data. Intrusion Detection systems need to consider more diverse heterogeneous sources to provide better situational awareness within cyberspace.

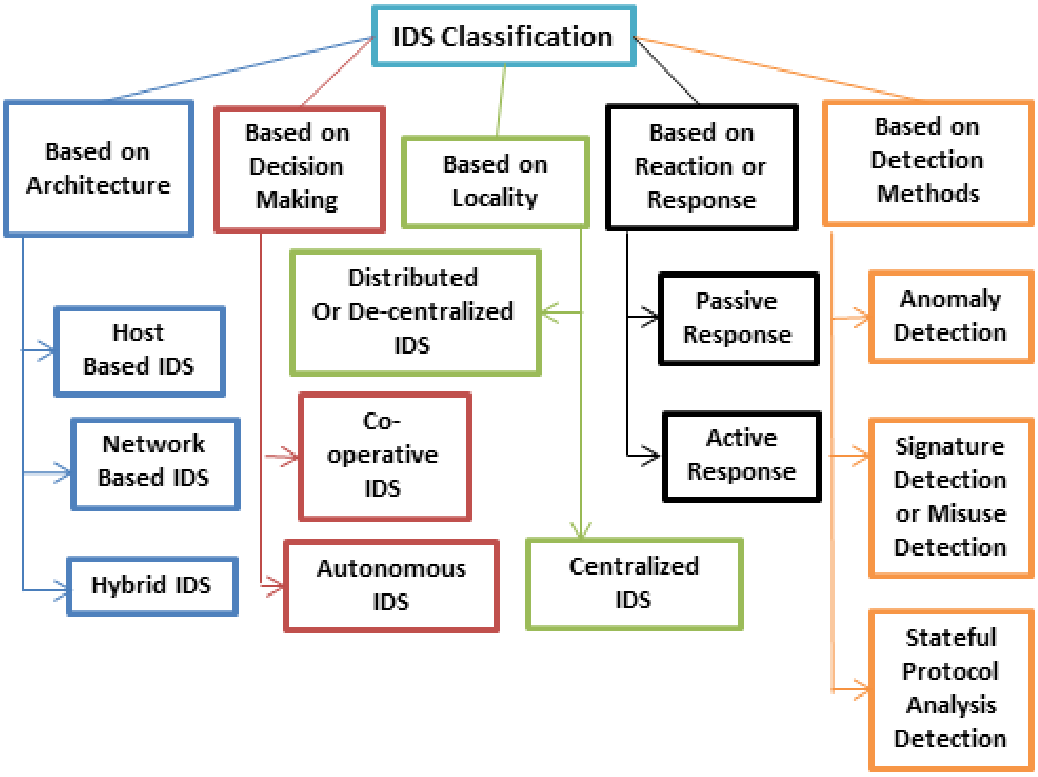

Figure 3. Classification of IDS based on used Methodology

Jeong et al. [10] give an overview of issues encountered with Intrusion Detection and Big Data and how various Hadoop technologies can address these challenges, specifically focusing on anomaly-based (misuse) IDSs. They describe various techniques and issues found with Intrusion Detection, as well as what some of the main issues are in applying Hadoop technologies for Intrusion Detection. Their study provides a good introduction for readers not already familiar with Hadoop technologies and how they can be applied to Big Data challenges found with Intrusion Detection.

Cheon and Choe [11] propose a distributed IDS architecture based on Snort and Hadoop technologies. They performed an experiment to see if additional Hadoop-based nodes for analysis could increase processing efficiency. Their methodology was to use replay files rather than real-time data, and then to evaluate the efficiency in terms of total processing time of the replay files while varying the number of Hadoop-based analysis nodes from zero to eight. A total of nine computers were used in the experiment with one acting as the “master node”. They discovered that the performance efficiency increased (it took less time to process the dataset) as they increased the number of Hadoop-based nodes. However, processing efficiency actually decreased with only one Hadoop-based analysis node. Lee and Lee [12] conducted an experiment with Hadoop technologies (e.g., HDFS, MapReduce, and Hive) to measure and analyze Internet traffic for a DDOS Detector. Hadoop and its related technologies show good feasibility as an Intrusion Detection tool as they were able to achieve up to 14 Gbps for a DDOS detector.

Bass [13] made a major contribution to Intrusion Detection research by suggesting data fusion as a technique to aggregate Intrusion Detection data from many different heterogeneous sources such as: numerous distributed packet sniffers, system log files, SNMP traps and queries, user profile databases, system messages, and operator commands.

3.3. False Positive and Negatives

The term *false positive* itself refers to security systems incorrectly seeing legitimate requests as spam or security breaches. Basically, the IDS will detect something it is not supposed to. Alternatively, IDS is prone to *false negatives* where the system fails to detect something it should. Both of these problematic problems are associated with IDS, but are issues vendors spend a lot of time working on, and as a result, it is not believed that IDS detects a high percentage of *false positive* or *false negatives*. Still, it is a topic worth consideration when looking at different IDS solutions.

False negatives are any alert that should have happened but didn't. False negative create two problems. First, there are missed attacks that will not be mitigated. Second, and probably more important, false negatives give a false sense of security. There are a number of reasons for *false negatives* including:

- Many attackers will frequently change their attack just enough to evade current signatures. Many attack toolkits include the ability to obfuscate the attack on the fly.
- In a signature based system there will be a period where new attacks are not recognized.
- Overloaded IDS will drop packets potentially causing false negatives.
- In an environment relying on anomaly detection or a host based intrusion detection system (HIDS) relying on file changes, the assumption must be that at the time of training the network or system was not compromised. If this is not true there will be false negatives for any already exploited conditions.

The major problem that *false positives* create is that they can easily drown out legitimate IDS alerts. A single rule causing false positives can easily create thousands of alerts in a short period of time. Simply stated, a *false positive* is any normal or expected behavior that is identified as anomalous or malicious. This can fall into several categories.

- Some legitimate applications do not strictly follow RFCs. Signatures written to the RFC may trigger when such applications run.
- A signature can be written too broadly and thus include both legitimate and illegitimate traffic.
- Anomalous behavior in one area of an organization may be acceptable while highly suspect in another. As an example NBT traffic is normal in a Windows LAN environment but not generally expected on the Internet.
- An application not seen in the training stage of an anomaly detection system will likely trigger an alert when the application attempts to run.

According to the real nature of a given event and the prediction from IDS, four possible outcomes are shown in Table 1, which is known as the confusion matrix [17,18]. True negatives as well as true positives correspond to a correct operation of the IDS; True negatives (TN) are events which are actually normal and are successfully labeled as normal, true positives (TP) are events which are actually attacks and are successfully labeled as attacks. Respectively, false positives (FP) refer to normal events being classified as attacks; false negatives (FN) are attack events incorrectly classified as normal events. Confusion matrix shows numerical parameters that apply following measures to evaluate the IDS performance.

$$\text{False Positive Rate } (\text{FPR}) = \text{FP}/(\text{FP}+\text{TN})$$

$$\text{False Negative Rate } (\text{FNR}) = \text{FN}/(\text{FN}+\text{TP})$$

$$\text{True Positive Rate } (\text{TPR}) = \text{TP}/(\text{TP}+\text{FN})$$

$$\text{True Negative Rate } (\text{TNR}) = \text{TN}/(\text{TN}+\text{FP})$$

$$\text{Accuracy} = (\text{TP}+\text{TN})/(\text{TP}+\text{TN}+\text{FN}+\text{FP})$$

$$\text{Precision } = \text{TP}/(\text{TP}+\text{FP}).$$

False positive rate (FPR) also known as *false alarm rate* (FAR), refers to the proportion that normal data is falsely detected as attack behavior. A high FPR will seriously cause the low performance of the IDS and a high FNR will leave the system vulnerable to intrusions. TNR also known as detection rate or sensitivity refers to proportion of detected attacks among all attack events. Accuracy refers to the proportion of events classified as an accurate type in total events [18]. So, to have effective

IDS both FP and FN rates should be minimized, together with maximizing accuracy and TP and TN rates.

In [45], K. Atefi et al. proposed an improved anomaly detection according to GA and SVM that raised or enhanced the accuracy to recognize intrusion while focus on the hybrid model by combining (GA and SVM) rather primary algorithms (SVM). When a researcher uses hybrid model this method achieve an acceptable percentage of alarm as far as: True Negative, False Negative, True positive and False positive. But, there are many suspicious behaviors in network intrusion detection, and unfortunately firewall techniques cannot guarantee against intrusion, due to the fact that the defense is extremely vital. Although, various studies already have been carried out in this area, there are few of them that use the potential benefit to combine SVM via GA. For evaluation by this algorithm author used KDDCUP'99 data set. At last, the results illustrated the hybrid model toward primary algorithm have high accuracy to recognize intrusion, additionally, have an acceptable percentage of alarms as far as (TN, FN, TP and FP).

3.4. Dataset in Context of IDS

This section summary the popular benchmark datasets measures in intrusion detection domain. Since computational intelligence approaches build detection models from data, the quality of training datasets directly affects the quality of trained models. For the research works we survey here, data is normally collected from three sources: data packages from networks, command sequences from user input, or system low-level information, such as system call sequences, log files, system error logs, and CPU/memory usage. We list some commonly used benchmarks in Table 2. All of these datasets have been used in either misuse detection or anomaly detection.

SUN has provided a new kernel auditing tool called the Basic Security Module (BSM). This tool can be activated to upgrade the security level of a Solaris 8 system to C2 (added auditing capability and access control). It can create an extremely detailed audit trail for all processes on the system. The level of auditing produced is at the level required by systems attempting to achieve the DoD This tool provides kernel auditing and device allocation features. The disadvantage of using the BSM tool is that, in general, system performance can be reduced by about 10 percent.

The KDD99 dataset was derived from the DARPA98 network traffic data in 1999 by a Bro program which assembled individual TCP packets into TCP connections. It was the benchmark dataset used in the International Knowledge Discovery and Data Mining Tools Competition, and also the most popular dataset ever used in the intrusion detection field. To reduce deficiencies of KDD99 dataset for machine learning algorithms, Tavallaee et al. [76] introduced NSL-KDD dataset. NSL-KDD has been generated by removing redundant and duplicate instances, also by decreasing size of dataset. Since it is a re-sampled version of KDD99, IDS deficiencies remain in NSL-KDD.

DARPA 2000 has been widely used by researchers in the field. The type of NIDSs used to replay the dataset is signature–based RealSecure Version 6.0 (Internet Security System, 2000). This data are downloaded from Ning (2002). It contains four separated files which represent two types of simulated scenarios (Scenario One and Scenario Two) of Distributed Denial of Services (DDoS) network attack on two different networks. Haines (2000) mentioned that attacks in Scenario Two were stealthier than Scenario One. They contain thousands of event logs or network packets that have been reported from the Demilitarized Zone (DMZ) and Inside Networks.

The UNB ISCX IDS 2012 dataset consists of labeled network traces, including full packet payloads in pcap format, which along with the relevant profiles are publicly available for researchers. The underlying notion is based on the concept of profiles which contain detailed descriptions of intrusions and abstract distribution models for applications, protocols, or lower level network entities. Real traces are analyzed to create profiles for agents that generate real traffic for HTTP, SMTP, SSH, IMAP, POP3, and FTP.

ADFA IDS Datasets cover both Linux and Windows; they are designed for evaluation by system call based HIDS. ADFA-LD dataset provides a contemporary Linux dataset for evaluation by traditional HIDS while ADFA-WD dataset provides a contemporary Windows dataset for evaluation by HIDS.

Table 1. Confusion Matrix: Actual Class & Predict Class [17,18]

	Normal	**Attack**
Normal	True Negative (TN)	False Positive (FP)
Attack	False Negative (FN)	True Positive (TP)

Table 2. Frequently used Datasets in IDS

Data Source	Dataset
User Behavior	UNIX User Dataset (UNIXDS)
System Call Sequences	DARPA 1998 BSM Files (BSM98)
	DARPA 1999 BSM Files (BSM99)
	University of New Mexico Dataset (UNM)
	ADFA IDS Datasets (2013-14)
Network Traffic	DARPA 1998 TCPDump Files (DARPA98)
	DARPA 1999 TCPDump Files (DARPA99)
	DARPA 2000 TCPDump Files (DARPA 2000)
	KDD99 Dataset (KDD99)
	10% KDD99 Dataset (KDD99-10)
	Internet Exploration Shootout Dataset (IES)
	University of New Brunswick, Information Security Centre of Excellence (ISCX) (UNB ISCX IDS 2012)

3.5. IDS Feature and It's Goal

Ideally, IDS should be fast, simple, and accurate, while at the same time being complete. It should detect all attacks with little performance penalty. An IDS could use some—or all—of the following design approaches:

- filter on packet headers
- filter on packet content
- maintain connection state
- use complex, multi-packet signatures
- use minimal number of signatures with maximum effect
- filter in real time, online
- hide its presence
- use optimal sliding time window size to match signatures

4. IDS Classification: Based on Architecture

Based on architecture, IDS can be classified as: Host IDS, Network IDS and Hybrid IDS. A system that monitors important operating system files is an example of a HIDS, while a system that analyzes incoming network traffic is an example of a NIDS.

4.1. Host Based IDS

A host-based IDS (HIDS) is usually a software application installed on a system and monitors activity only on that local system. It communicates directly with the operating system and has no knowledge of low-level network traffic. Most host-based IDSs rely on information from audit and system log files to detect intrusions [82]. They can also monitor system files and system resources, and incoming application data. Because a host-based IDS can produce a lot of data, hence an extra administrative load, they are often placed only on critical servers. To further reduce the load, the IDSs can report to a central console.

OSSEC [29,30] is a free, open-source host-based intrusion detection system (HIDS). It performs log analysis, integrity checking, Windows registry monitoring, rootkit detection, time-based alerting, and active response. It provides intrusion detection for most operating systems, including Linux, OpenBSD, FreeBSD, OS X, Solaris and Windows. OSSEC has a centralized, cross-platform architecture allowing multiple systems to be easily monitored and managed. Open Source Tripwire [31] is also a HIDS tool. Rather than attempting to detect intrusions at the network interface level (as in NIDS), Open Source Tripwire detects changes to file system objects. SMARTWatch [33] is also a Host based intrusion detection system which is a pre-emptive hacker Defence tool. It actively monitors a Windows computer system. With SMART Watch, changes to watched resources are detected and reported instantly. While other change detection techniques are based on polling, or must be integrated into the system's scheduler, SMART Watch's self-contained, silent operation actually wakes up when a change in the file system is detected. These operating system level changes tell SMART Watch when to verify if a resource is still intact. If a resource has changed or been deleted, SMART Watch can respond within milliseconds. In the case of a file modification or deletion, SMART Watch can actually restore the content of that file immediately! SMART Watch is not just a change detection tool.

Paper [7] presents a host-based combinatorial method based on k-Means clustering and ID3 decision tree learning algorithms for unsupervised classification of anomalous and normal activities in computer network.

4.2. Network Based IDS

A network intrusion detection system (NIDS) monitors the packets that traverse a given network link. A network-based IDS can be a dedicated hardware appliance, or an application running on a computer, attached to the network. Such a system operates by placing the network interface into promiscuous mode, affording it the advantage of being able to monitor an entire network while not divulging its existence to potential attackers. Because the packets that a NIDS is monitoring are not actually addressed to the host the NIDS resides on, the system is also impervious to an entire class of attacks such as the "*ping-of-death*" attack that can disable a host without ever triggering a HIDS. A NIDS is obviously of little value in detecting attacks that are launched on a host through an interface other than the network.

A network-based ID can monitor traffic only in its local network segment, unless it employs sensors. In switched and routed networks, a sensor is required in each segment (collision domain) in which network traffic is to be monitored. When a sensor detects a possible intrusion, it will report it to a central management console, which will take care of the appropriate passive or active response. Communication between the remote sensor and the management console should be secure to avoid interception or alteration by the intruder. One major shortcoming of NIDS [82] is that they are oblivious to local root attacks. The authorized user of the system that attempts to gain additional privileges will not be deleted if attack is performed locally. The authorized user of the system may be able to set up an encrypted channel when accessing the machine remotely [82].

The network card of a network-based IDS runs in promiscuous mode, which means it picks up all traffic from the media even if the destination address is not the IDS. It basically works like a sniffer.

On a heterogeneous network, a NIDS generally does not possess intimate knowledge of all of the hosts on the network and is incapable of determining how a host may interpret packets with ambiguous characteristics. Without explicit knowledge of a host system's protocol implementation, a NIDS is impotent in determining how a sequence of packets will affect that host if different implementations interpret the same sequence of packets in different ways [5].

Protocol ambiguities can also present a problem to a NIDS in the form of *crud*. Crud appears in a network stream from a variety of sources including erroneous network implementations, faulty network links, and network pathologies that have no connection to intrusion attempts [6]. If a NIDS performs insufficient analysis on a stream containing crud, it can generate *false positives* by incorrectly identifying this crud as being intrusive. While a NIDS therefore is in a very convenient position whereby it has complete access to all packets traversing a network link, its perspicacity is challenged due to ambiguities in network data and its limited perspective of host system implementations and network topology. NIDS should be capable of standing against large amount number of network traffic to remain effective. As network traffic increases exponentially NIDS must grab all the traffic and analyze in a timely manner.

BRO [34], is an open source Unix based network monitoring framework. It is used as NIDS as well as for collecting network measurements, conducting forensic investigations, traffic baselining and more.

In [39], M. Sailaja et al. proposed an architecture called IHDAIDS for the NIDS. Beside the real time potential application of IHDAIDS, it is intelligent, hybrid and adaptive. In addition, it produced a low rate false alarm and required a lower rate of human intervention. However, encryption software and firewalls, which are used for intrusion detection, do not provide complete security of the networks. Aggregation of these techniques with IDS can provide improved security. The proposed architecture has applied and tested on the KDDCUP'99 dataset. This architecture has used the combination of host based and network based IDS to provide a high level accuracy.

G. Zhao et al. in [40], represents a new network intrusion detection method using SVM. In addition the attributes are optimized using k-fold cross validation. Yet, the anomaly based and signatures base both rates as False Negative and False Positive are high. They have used their collected dataset. Comparisons on some proposed machine learning method, the result of online data experimental indicate that this technique can be used to decrease the rate of False-Negatives in the IDS.

4.3. Hybrid Based IDS

The current trend in intrusion detection is to combine both types host-based and network-based IDS to design hybrid systems. Hybrid intrusion detection system has flexibility and it increases the security level. It combines IDS sensor locations and reports attacks are aimed at particular segments or entire network.

The paper [44] focused on incremental SVM training algorithms to aimed network intrusion detection, and suggested an improved algorithm. It applied on hybrid with modifying kernel function U-RBF, to deal with network intrusion detection. However, given the fluctuation problem that usually happens in traditional incremental SVM's pursue learning process. Authors used benchmark KDD Cup 1999 as the dataset for experiments. Contrasted with different algorithms by experiments, the test of results shows, that the oscillation problem is more comforted by improving the incremental SVM algorithm in the training process, acquire satisfactory performance, nevertheless, its reliability is high. This work is not suitable based on the detection rate on foreseeing attacks, specifically for attacks of U2R and R2L [44].

Ref. [48] proposed combinatorial approach for unsupervised classification of anomalous and normal activities in computer network. The proposed approach combines the two well-known machine learning methods: the k-Means clustering and the ID3 decision tree learning approaches. The k-Means method was first applied to partition the training instances into k disjoint clusters. The ID3 decision tree built on each cluster learns the subgroups within the cluster and partitions the decision space into finer classification regions; thereby improving the overall classification performance.

Prelude [35] is a Hybrid IDS which comes with a large set of sensors, each of them monitoring different kind of events. Prelude permits alert collection to WAN scale, whether its scope covers a city, a country, a continent or the world. Prelude-SIEM compound is a hybrid of two different heterogeneous detectors types:

- A LML enabling the treatment of any type of log file as syslogs or stream
- Native compatibility with leading NIDS sensors and open-source HIDS available on the market (eg. Snort, Suricata, Samhain, etc.) and other types of probes

5. IDS Classification: Based on Decision Making

Based on decision making, IDS can be classified as: Co-operative IDS and Autonomous IDS.

5.1. Co-operative IDS

Co-Operative Intrusion Detection Systems are frequently used in Mobile Ad-Hoc Network (MANET). The existent protocol, application and services assume that MANET is a cooperative and friendly network environment and do not accommodate securityIn a cooperative IDS, if a node detects an anomaly, or the existent evidences be inconclusive, a cooperative mechanism triggers to produce a global intrusion detection action along with neighboring nodes. Even if a node be sure about the crime of another node, decision making also should be cooperative because the node which take the decision, can be malicious, itself.

Mobile Ad hoc Networks (MANETs) are wireless networks that lack infrastructure [84]. Security requirements in MANET have to be much efficient due to specific characteristics of ad hoc network. In paper [84], an idea is proposed to build an IDS based on a co-operative scheme to detect intrusions in a mobile ad hoc network using basic game theory concepts. To identify the intrusion proposed methodologies deal with two layers - the *application layer* with underlying grid architecture and the *network layer*. Authors also simulate a couple of intrusions in each of the two layers and look to resolve them using the coalition formation of the mobile nodes. These nodes obey the shapely value phenomena of the game theory concept and form coalitions to report intrusions in the network.

Paper [87] proposed a network-based intrusion detection system called AIMS (Active Intrusion Monitor System) that employs emerging active network technologies. Proposed methodology provides a flexible co-operative detection framework and an effective platform for intrusion detection.

5.2. Autonomous IDS

An autonomous agent (henceforth agent) can be defined as a software agent that performs a certain security monitoring function at a host. Because agents are independently-running entities, they can be added, removed and reconfigured without altering other components and without having to restart the intrusion detection system. Agents can be tested on their own before introducing them into a more complex environment.In this method, network nodes take decisions, and autonomously they gather evidences and criteria of anomaly and intrusion activities from the network and then make decision on node level. Other network nodes do not have cooperated in this decision making process. The main weaknesses of this approach are:

1) Security of network nodes is low, attackers can compromise them soon and easily. Hence, this leads to loss of the network control.
2) Enforcing excessive processing overhead on some network nodes; therefore, in attending to limited resources and being few key nodes, it leads to their lifetime reduction (energy waste and network node destruction).

Wireless body area networks (WBAN) are revolutionizing healthcare with their great potential to perform cost-effective, unobtrusive and constant real-time monitoring of health applications [83]. Since wearable, implantable medical and mobile devices in WBAN often control life critical data, it is important to ensure security in these networks. Severe resource constraints pose significant challenges in providing security to these systems. In [83] paper, an autonomous mobile agent based intrusion detection architecture is proposed to address security in wireless body area networks. They also provide a comparison of mobile agent based IDS proposed in other domains with WBAN systems and highlight the unique benefits of the proposed architecture.

The paper [85] presents a hierarchical and autonomous cloud based intrusion detection system, HA-CIDS. The framework continuously monitors and analyzes system events and computes the security and risk parameters. An autonomous controller receives security parameters computed by the framework and selects the most appropriate response to protect the cloud against detected attacks, as well as recover any corrupted data or affected services. Beside autonomous response to detected attacks, HA-CIDS has several autonomous capabilities to provide self-resilience and fault tolerance. Paper [86] presents a hierarchical, autonomous, and forecasting cloud based IDS (HAF-CIDS) that continuously monitors and analyzes system events and computes the risk level. The proposed system improves the detection accuracy through the integration with a forecasting engine that runs the Holt-Winters (HW) algorithm. HAF-CIDS uses HW forecast feature in detecting network aberrant behaviors. Furthermore, it can recover any corrupted data or affected services by interacting with an autonomous controller that selects the most appropriate response to detected attacks.

Vehicular ad hoc networks (VANETs) add new threats to self-driving vehicles that contribute to substantial challenges in autonomous systems [89]. These communication systems render self-driving vehicles vulnerable to many types of malicious attacks, such as *Sybil attacks, Denial of Service (DoS), black hole, grey hole* and *wormhole attacks*. Paper [89] proposed an intelligent security system designed to secure external communications for self-driving and semi self-driving cars. The proposed scheme is based on Proportional Overlapping Score (POS) to decrease the number of features found in the *Kyoto benchmark dataset*. The hybrid detection system relies on the Back Propagation neural networks (BP), to detect a common type of attack in VANETs: Denial-of-Service (DoS). The experimental results show that the proposed BP-IDS is capable of identifying malicious vehicles in self-driving and semi self-driving vehicles.

6. IDS Classification: Based on Locality

Based on locality and by the way intrusion detection systems components are distributed, IDS can be classified as: Distributed or De-centralized IDS, and Centralized IDS.

Table 3. Decentralized IDS vs. Centralized IDS

Parameters	Distributed/Decentralized IDS	Centralized IDS
Fault Tolerant	The state of the intrusion detection system is distributed, making it more difficult to store in a consistent and recoverable manner.	The state of the intrusion detection system is centrally stored, making it easier to recover it after a crash.
Scalability	A distributed intrusion detection system can scale to a larger number of hosts by adding components as needed. Scalability may be limited by the need to communicate between the components, and by the existence of central coordination components.	The size of the intrusion detection system is limited by its fixed number of components. As the number of monitored hosts grows, the analysis components will need more computing and storage resources to keep up with the load.
Dynamic Reconfiguration	Individual components may be reconfigured and restarted without affecting the rest of the intrusion detection system.	A small number of components analyze all the data. Reconfiguring them likely requires the intrusion detection system to be restarted.
Overload	Impose little overhead on the systems because the components running on them are smaller. However, the extra load is imposed on most of the systems being monitored.	Impose little or no overhead on the systems, except for the ones where the analysis components run, where a large load is imposed. Those hosts may need to be dedicated to the analysis task.
Execution	Harder because a larger number of components need to be kept running.	A relatively small number of components need to be kept running.
Resist subversion	A larger number of components need to be monitored. However, because of the larger number, components can cross-check each other. The components are also usually smaller and less complex.	A smaller number of components need to be monitored. However, these components are larger and more complex, making them more difficult to monitor.

6.1. Distributed or De-centralized IDS

A distributed intrusion detection system is one where the analysis of the data is performed in a number of locations proportional to the number of hosts that are being monitored. We only consider the locations and number of the data analysis components, not the data collection components. Some intrusion detection systems that we classify as distributed are: DIDS [70], GrIDS [71], EMERALD [72] and AAFID [73].

6.2. Centralized IDS

A centralized intrusion detection system is one where the analysis of the data is performed in a fixed number of locations, independent of how many hosts are being monitored. Same in the case of Dcentralized IDS, we do not consider the location of the data collection components, only the location of the analysis components. Some intrusion detection systems that we classify as centralized are: IDES [66], IDIOT [67], NADIR [68] and NSM [69].

Comparison between Decentralized and Centralized intrusion detection systems with respect to given condition, is described in Table 3.

7. IDS Classification: Based on Reaction or Response

Based on Reaction or Response, IDS can be classified as: Active Response and Passive Response.

7.1. Passive Response

In a passive system, the IDS detect a potential security breach, log the information and signal an alert. Passive-response intrusion detection does not actively attempts to stop the intrusion. It merely logs the intrusion and notifies someone, by email or pager. Several passive response IDS products allow plug-ins for communication with a central management console. This allows you to use the passive response product in a decentralized active response system, in which the passive IDS reports to the central console, which in turn can actively control involved network devices and systems. Modern IDSs offer a wide range of options to send notifications of intrusions, including pager, cell phone, email, SNMP trap messages, or simply a message box on the administrator’s PC. It is important to make sure that the notifications are send in a secure manner to prevent the attacker from intercepting or altering them.

Passive attack includes observation or monitoring of communication. A passive attack attempts to learn or make use of information from the system but does not affect system resources. The goal of the opponent is to obtain information that is being transmitted [2].

7.2. Active Response

An active attack attempts to alter system resources or affect their operation. It involves some modification of the data stream or the creation of a false stream [2]. A common active response is increasing the sensitivity level of the IDS to collect additional information about the attack and the attacker. Active-response IDSs automatically take action in response to a detected intrusion. The exact action differs per product and depends on the severity and type of attack. Another possible active response is making changes to the configuration of systems or network devices such as routers and firewalls to stop the intrusion and block the attacker. This could involve blocking the source address of the attacker, restarting a server or service, closing connections or ports, and resetting TCP sessions.

The paper [88] proposes an active network programming model. Comparing to a traditional network, active network gives the nodes programmable ability. It adopts the active network technology. The response, service deployment and service update schemes rely on this technology. The proposed intrusion detection and response system (WRS) can stop attacks at the first line and respond as fast as possible to reduce the damage caused by intruders. It provides the abilities of detection, report and response. The proposed prototype system adopts the novel data mining technology-support vector machine to enhance the detection function.

8. IDS Classification: Based on Detection Methods

Based on Detection Methods, IDS can be classified as: Anomaly detection, Signature Detection or Misuse Detection and Stateful Protocol Analysis Detection.

8.1. Anomaly Detection

Anomaly detection is concerned with identifying events that appear to be anomalous with respect to normal system behavior. The most appealing feature of anomaly detection systems is their ability to identify new and previously unseen attacks. A wide variety of techniques including statistical modeling, neural networks, and hidden Markov models have been explored as different ways to approach the anomaly detection problem. Each of these anomaly-based approaches fundamentally relies upon the same principles: anomalous activity is indicative of an attempted attack and the correct set of characteristics can sufficiently differentiate anomalies from normal system usage.

In anomaly detection, the system administrator defines the baseline, or normal, state of the network's traffic load, breakdown, protocol, and typical packet size. The anomaly detector monitors network segments to compare their state to the normal baseline and look for anomalies. Such system involves first establishing a baseline model that represents normal system behavior and against which anomalous events can be distinguished. The system then analyzes an event by considering it within this model and classifying it as anomalous or normal based on whether it falls within a certain threshold of the range of normal behavior. Because the process of establishing a baseline model of normal behavior is usually automated, anomaly systems also do not require expert knowledge of computer attacks. This approach is not without its handicaps;

however, as anomaly detection may fail to detect even attacks that are very well-known and understood if these attacks do not differ significantly from what the system establishes to be normal behavior. Anomaly based systems are also prone to higher numbers of false positives, as all anomalous events are assumed to be intrusive although in reality a variety of other factors can produce behavior that appears anomalous (e.g., implementation errors).

J. Song et al. in [38], have proposed a novel anomaly detection method which can be tuned and optimize automatically without pre-defining them. Moreover, evaluate this method via real traffic data achieved from Kyoto University honeypots as a dataset. It is still difficult to deploy many IDS methods into real network environments due to the fact that they need several factors during their process. Moreover, IDS managers and operators suffer from optimizing and tuning the need factors according to the alternative of their network characteristics. The experimental results illustrate that the proposed method is greater than the Song's method from the aspect of the accuracy performance. This method is not beneficial and difficult to apply on various network environments. This method also poor in experiments due to auteurs didn't effort in more real traffic data and superior range. The proposed method required training and testing in maximum databases and apply in various real network environments.

Catania et al. in [43], proposed an approach for autonomous labeling algorithm of normal traffic in the network. This algorithm is applied to the SVM algorithm, when the class distribution is not imbalanced. The current proposed methods using SVM in IDS are accurate when the normal traffic has hugely been more than the number of attacks on the dataset; while this situation cannot be always accrued. The main advantage of using the proposed approaches is, when the training dataset which contains normal traffic and number of attacks, the approach can depict the normal traffic. The SbSVM is not evaluated for the real time situation. It is important to evaluate and improve the ability of applying this approach for real time applications.

The paper [80] demonstrates that a hardware (HW) implementation of network security algorithms can significantly reduce their energy consumption compared to an equivalent software (SW) version. The paper has four main contributions: (i) a new feature extraction algorithm, with low processing demands and suitable for hardware implementation; (ii) a feature selection method with two objectives - accuracy and energy consumption; (iii) detailed energy measurements of the feature extraction engine and three machine learning (ML) classifiers implemented in SW and HW - Decision Tree (DT), Naive-Bayes (NB), and k-Nearest Neighbors (kNN); and (iv) a detailed analysis of the tradeoffs in implementing the feature extractor and ML classifiers in SW and HW [80]. The new feature extractor demands significantly less computational power, memory, and energy. Its SW implementation consumes only 22% of the energy used by a commercial product and its HW implementation only 12%. The dual-objective feature selection enabled an energy saving of up to 93%. Comparing the most energy-efficient SW implementation (new extractor and DT classifier) with an equivalent HW implementation, the HW version consumes only 5.7% of the energy used by the SW version [80].

Identification of anomalous activity in computer network is first step in identifying the threat to information system. Paper [81] focuses on Genetic algorithm (GA) based anomaly detection technique, as GA is one of the most effective evolutionary techniques for machine learning. In this paper Genetic algorithm is applied for network intrusion detection. Author mainly improves optimization specifically focusing on false positive rate. Reduction in false positive rate also improves accuracy and performance. The limitation of other techniques of accuracy, false positive rates has been addressed in this paper. Experimental results show the efficient detection rates based on KDD99cup datasets [81].

8.2. Signature Detection or Misuse Detection

The concept behind signature detection or misuse detection scheme is that it stores the sequence of pattern, signature of attack or intrusion etc. into the database. When an attacker tries to attack or when intrusion occurs then IDS matches the signatures of intrusion with the predefined signature that are already stored in database. On successful match the system generates alarm. In misuse detection, the IDS analyzes the information it gathers and compares it to large databases of attack signatures. Essentially, the IDS looks for a specific attack that has already been documented. Like a virus detection system, detection software is only as good as the database of intrusion signatures that it uses to compare packets against.

The essence of misuse detection centers around using an expert system to identify intrusions based on a predetermined knowledge base. As a result, misuse systems are capable of attaining high levels of accuracy in identifying even very subtle intrusions that are represented in their expert knowledge base; similarly, if this expert knowledge base is crafted carefully, misuse systems produce a minimal number of false positives. A less fortunate ramification of this architecture results from the fact that a misuse detection system is incapable of detecting intrusions that are not represented in its knowledge base. Subtle variations of known attacks may also evade analysis if a misuse system is not properly constructed. Therefore, the efficacy of the system relies heavily on the thorough and correct construction of this knowledge base, a task that traditionally requires human domain experts.

S. Araki et al. in [41], using multistage OC-SVM and feature extraction represented a method to detect unknown attacks. The unknown attacks cannot be detected using signature-based IDS. Since the detecting unknown attacks, IDS is applied; yet, this method cannot completely distinguish between sophisticated attacks and known attack. Furthermore, for evaluating the proposed method used Kyoto2006+ as data set. This represents a method achieve unknown attacks that in the archive have not been stored. This method is poor in second stage classifier to a detection rate of unknown attacks. For solving that poorness can extract more viable features at reflect exclusive behavior of unknown attacks, and also can perform clustering and filtering in order to decrease an effect of noisy data.

A. H. Sung et al. in [47], used a method for feature deleting at each time employ to SVM and ANN, after that the features are ranked and for five different classes in DARPA intrusion data, efficient features are demonstrated. But, since the unimportant and/or pointless inputs cause a complex problem, slower and less accurate detection results. Author used data in their own experiments that initiate from MIT's Lincoln Lab. This technique considered a benchmark for evaluating and creating an intrusion detection system by DARPA. Using the importance features gives the most significant performance as far as training time. Using 2 classifiers are time consuming and hard task to trigger them.

Authors in [42], proposed a combining IG feather selection and SVM classifier in IDS model, but selection of suitable parameters effect on performance of SVM. This paper use NSL-KDD as a dataset. Results illustrate this model can give a lower false alarm and higher detection rate toward regular SVM. The limitation of this paper is limited experiments; just two swarm intelligence algorithms. Proposed algorithms can be used other kinds of swarm intelligence algorithms.

Paper [77] focuses on deploying high interaction honeypot system coupled with intrusion detection system on different operating system flavors which work as clients. Clients collect URLs by specifically crafted web links crawler [4]. These URLs are then visited by application needed to visit these URLs. Finally, if these URLs are malicious and exploit the application software, an alert is triggered by signature based intrusion detection system deployed on the machine. Based on these alerts, URLs are stored in a black list of malicious URLs.

Polymorphic worm signature extraction is a critical part of signature-based intrusion detection. Since the classical Hierarchical Multi-Sequence Alignment(HMSA) algorithm has bad time performance in extracting signatures when multiple sequences alignment was used and the extracted signatures were not precise enough, a new method called antMSA was proposed based on the improved ant optimal algorithm. The search strategy of the ant group was improved and introduced to the Contiguous Matches Encouraging Needleman-Wunsch(CMENW) algorithm to get a better solution quickly in global range by using the rapid convergence ability of the ant colony algorithm. The signature fragments were extracted and converted into the standard rules of the intrusion detection systems for subsequence defense [78].

A new software-based pattern matching algorithm that modifies Wu-Manber pattern matching algorithm using Bloom filters is introduced in [79]. The Bloom filter acts as an exclusion filter to reduce the number of searches to the large HASH table. The HASH table is accessed if there is a probable match represented by a shift value of zero. On average the HASH table search is skipped 10.6% of the time with a worst case average running time speedup over Wu-Manber of 33%. The maximum overhead incurred on preprocessing time is 1.1% and the worst case increase in memory usage was limited to 0.33%.

8.3. Stateful Protocol Analysis Detection

This method identifies deviations of protocol states by comparing observed events with “predetermined profiles of generally accepted definitions of benign activity [8].

9. IPS: Intrusion Prevention System

Intrusion prevention systems (IPS), also known as *intrusion detection and prevention systems* (IDPS), are network security appliances that monitor network or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, report it and attempt to block or stop it [24]. Figure 4 shows the idea about types of IPS System.

9.1 IPS vs. IDS: Similarity and Difference

IPSs are considered extensions of IDS because they both monitor network traffic and/or system activities for malicious activity. The main differences are, unlike intrusion detection systems, intrusion prevention systems are placed in-line and are able to actively prevent or block intrusions that are detected [8,25]. IPS can take such actions as sending an alarm, dropping detected malicious packets, resetting a connection or blocking traffic from the offending IP address [26]. An IPS also can correct cyclic redundancy check (CRC) errors, defragment packet streams, mitigate TCP sequencing issues, and clean up unwanted transport and network layer options[25,27].

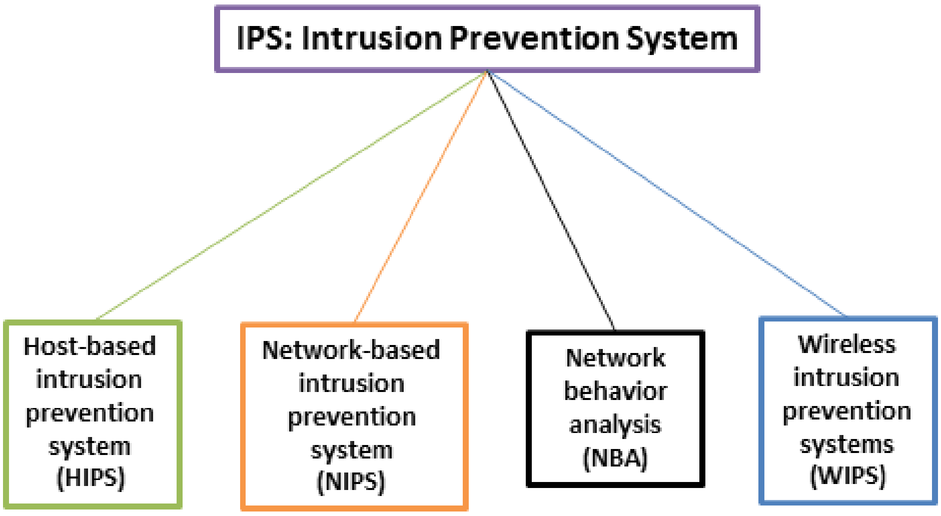
IPS: Intrusion Prevention System
Host-based intrusion prevention system (HIPS)
Network-based intrusion prevention system (NIPS)
Network behavior analysis (NBA)
Wireless intrusion prevention systems (WIPS)

Figure 4. Types of IPS System

9.2. Types of IPS

Intrusion prevention systems (IPSs) can be classified into four different types as shown in Figure 4.

Host-based intrusion prevention system (HIPS): A Host Intrusion Prevention System (HIPS) aims to stop malware by monitoring the behavior of code. This makes it possible to help keep the system secure without depending on a specific threat to be added to a detection update. It is an installed software package which monitors a single host for suspicious activity by analyzing events occurring within that host. The normal method of a HIPS is runtime detection. It intercepts actions when they occur, but some HIPS also offer pre-execution detection. This means that the nature of an executable is analyzed before it runs, to check for suspicious behavior.

Idea given in [37] provides a multilayer approach in IDPS to monitor a single host. Multilayer approach consists of three layers. File Analyzer, System Resource Analyzer and Connection Analyzer. The advantage of this technique [37] is that it provides both signatures based and anomaly based detection and prevention. The drawback in Multilayer approach is that the IDPS require a large amount of memory to store the data of the system and network traffic. Paper [61] introduce a four tier host based IPS that uses data mining technique, namely decision tree, as a detecting mechanism. The input parameters for the prior decision tree algorithm are the most infected or targeted computer resources by intruders, instead of a static signature database.

Network-based intrusion prevention system (NIPS): The NIPS monitors the network for malicious activity or suspicious traffic by analyzing the protocol activity. Once the NIPS is installed in a network, it is used to create physical security zones. This, in turn, makes the network intelligent and quickly discerns good traffic from bad traffic. In other words, the NIPS becomes like a prison for hostile traffic such as Trojans, worms, viruses, and polymorphic threats. NIPS are reported to have a high rate of false positives but have blocked thousands of known attacks.

NIPSs are manufactured using high-speed application-specific integrated circuits (ASICs) and network processors, which are used for high-speed network traffic since they are designed to execute tens of thousands of instructions and comparisons in parallel, unlike a microprocessor, which executes one instruction at a time. The majority of NIPSs utilize one of the three detection methods: Signature-based detection, Anomaly-based detection, and Protocol state analysis detection.

There are many existing approaches for IDPS, in which SNORT [32] is an open source intrusion prevention system capable of real-time traffic analysis and packet logging. Snort has three primary uses: a straight packet sniffer like tcpdump, a packet logger (useful for network traffic debugging, etc), or a full-blown network intrusion prevention system [32].

Wi-Fi technology is vulnerable to many attacks due to the lack of security, limitation of capability, power limitations, resource handling etc. Security is more and more important, and wireless monitoring and shielding are of prime importance for network security [65]. In order to satisfy secure communication between all nodes, this paper proposes Advanced Technique for Monitoring and Shielding in Wi-Fi Technology. Idea proposed in [65] explores various security issues of IEEE 802.11 based wireless network and analyzes numerous problems in implementing the wireless monitoring and shielding system. To protect from attack, the system analyzes wireless network protocols efficiently and flexibly, reveals rich information of the IEEE 802.11 protocol such as traffic distribution and different IP connections, and graphically displays later.

Network behavior analysis (NBA): Network behavior analysis (NBA) is a way to enhance the security of a proprietary network by monitoring traffic and noting unusual actions or departures from normal operation. Conventional intrusion prevention system solutions defend a network's perimeter by using packet inspection, signature detection and real-time blocking. NBA solutions watch what's happening inside the network, aggregating data from many points to support offline analysis. CAMNEP is a NBA tool which uses several anomaly detection algorithms to classify legitimate and malicious traffic.

A good NBA program can help a network administrator minimize the time and labor involved in locating and resolving problems. It should be used as an enhancement to the protection provided by the network's firewall, intrusion detection system, antivirus software and spyware-detection program. After establishing a benchmark for normal traffic, the NBA program passively monitors network activity and flags unknown, new or unusual patterns that might indicate the presence of a threat. The program can also monitor and record trends in bandwidth and protocol use. Network behavior analysis is particularly good for spotting new malware and zero day exploits.

Wireless intrusion prevention systems (WIPS): Wireless intrusion prevention system (WIPS) is a network device that monitors the radio spectrum for the presence of unauthorized access points (intrusion detection), and can automatically take countermeasures (intrusion prevention). The primary purpose of a WIPS is to prevent unauthorized network access to local area networks and other information assets by wireless devices. These systems are typically implemented as an overlay to an existing Wireless LAN infrastructure, although they may be deployed standalone to enforce no-wireless policies within an organization. Some advanced wireless infrastructure has integrated WIPS capabilities.

Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, and reporting attempts. In addition, organizations use IDPSes for other purposes, such as identifying problems with security policies, documenting existing threats and deterring individuals from violating security policies. IDPSes have become a necessary addition to the security infrastructure of nearly every organization [28]. IDPSes typically record information related to observed events notify security administrators of important observed events and produce reports. Many IDPSes can also respond to a detected threat by attempting to prevent it from succeeding. They use several response techniques, which involve the IDPS stopping the attack itself, changing the security environment (e.g. reconfiguring a firewall) or changing the attack's content [28].

Table 4. IDPS using SVM as Classifier

Approach	Working Idea	Detection Rate %	False Alarm %
Unsupervised anomaly detection system [38]	Tune and optimize automatically the values of parameters without pre-defining them. Dataset: Data achieved from Kyoto University honeypot	-	-
Multiclass SVM [40]	Attributes are optimized using k-fold cross validation. This technique can be used to decrease the rate of False-Negatives in the IDS. Dataset: Self	-	-
OC-SVM One-Class SVM [41]	Multistage OC-SVM and feature extraction represents a method to detect unknown attacks. Method is poor in second stage classifier to detection rate of unknown attacks. Dataset: From Kyoto	80.00	20.94
IG-ABC-SVM Information Gain- Artificial Bee Colony [42]	A combining IG feature selection and SVM classifier in IDS model is proposed Experiments using just two swarm intelligence algorithms. Dataset: NSL-KDD	98.53	0.03
SbSVM [43]	autonomous labeling algorithm of normal traffic (when the class distribution is not imbalanced) Not evaluated for real time case Dataset: DARPA	99	5.5
RS-ISVM- reserved set -Incremental SVM [44]	An incremental SVM training algorithms is used, hybrid with modifying kernel function U-RBF Foreseeing attacks, specifically for attacks of U2R and R2L may not tolerate but oscillation problem solved Dataset: KDD Cup 1999	89.17	4.9
SVM-GA [45]	Hybrid model by combining (GA and SVM) Dataset: KDD CUP 1999	98.33	0.50
SVM -GPC-10 Genetic principal Component [46]	Subset selection using GA and PCA. Dataset: KDD cup	99.96	0.49
SVM and NN [47]	Hybrid process Most significant performance as far as training time but time consuming and hard task to trigger Dataset: DARPA	99.87	-
N-KPCA-GA-SVM kernel principal component analysis-genetic algorithm (GA)-SVM [74]	Hybrid of KPCA, SVM and GA algorithms. Faster convergence speed. Performs higher predictive accuracy and better generalization But have complex structure and have latency for real time application. Dataset: KDD CUP99	96.37	0.95
CSV-ISVM Candidate Support Vector - Incremental SVM [75]	Improved learning algorithm Better recognize rate and false alarm rate than usual classification Dataset: KDD Cup 1999	90.14	2.31

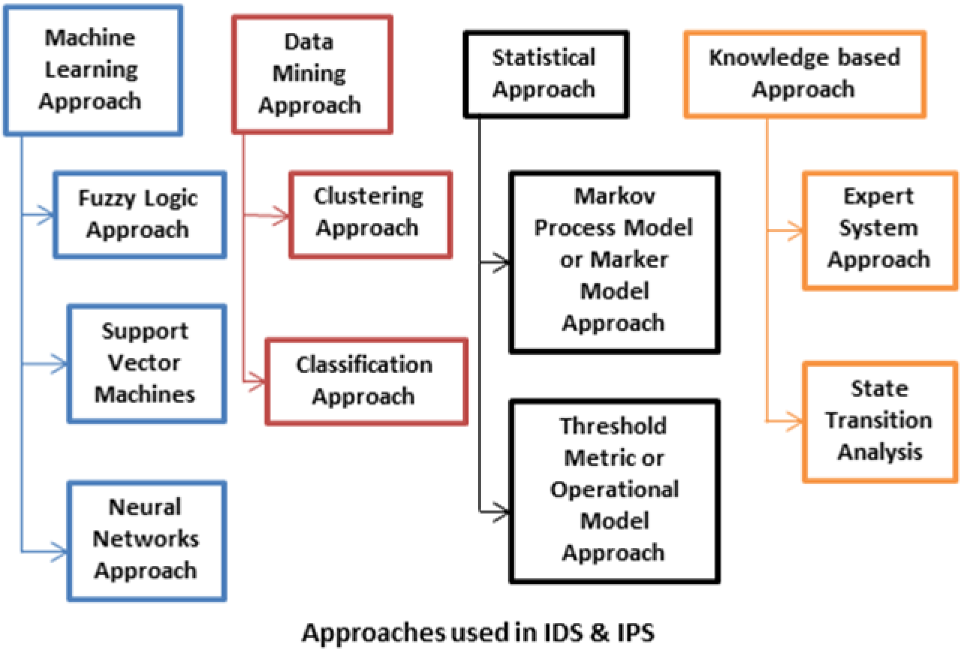

Figure 5. Approaches for Network Security

In order to provide sufficient protection against increasingly sophisticated cyber-attacks, intrusion prevention system (IPS) is explored. But in some cases, common IPS cannot provide timely protection ideally for moveable end-users in a public open network environment. Secure Vault: An Intrusion Prevention Model for Ender-Users is presented in [60]. In this model, an end-user in Internet can connect a network-based IPS engine conveniently. Model mainly consists of two parts: vault sensor and secure manor. Because of secure manor introduced, all sophisticated traffics of user are protected in a close operating environment and go on in security. A wide analysis of different approaches for IDPS using SVM as Classifier is shown in Table 4.

10. Approaches Used for IDS and IPS

This section reviews the approaches which are useful for IDS as well as IPS. Figure 5 shows the overview of used approach for network security.

10.1. Machine Learning Approach

Machine learning is a technique which can be defined as the ability of the program and/or a system to learn and improve their performance for certain tasks or a group of tasks over time. It primarily concentrates on establishing a system for improving the performance on the basis of previous result it means that machine learning has the ability to alter the execution strategy based on newly acquired information. This characteristic makes this technique to use in various situations, but the drawback is their recourse expensive nature. In many instances, the machine learning technique coincides with that of the statistical techniques and data mining techniques [49]. This technique can further classify as:

Fuzzy Logic Approach: The fuzzy logic system is highly responsible for both handling the large number of input parameters and dealing with the inexactness of the input data. As if fuzzy logic is combined with data mining technique, it reduces the size of input data set and selects features that focus as an anomaly. Dickerson et al. Developed the Fuzzy Intrusion Recognition Engine (FIRE) using fuzzy sets and fuzzy rules [50].

Support Vector Machines: The working of Support Vector Machines (SVM) is as, firstly it maps the input vector into comparatively higher dimensional feature space and after that obtain the optimal separating hyper-plane in higher dimensional feature space. Besides, a decision boundary, i.e. the separating hyper-plane, is determined by support vectors rather than the whole training samples and therefore is extremely strong to outliers. Especially, an SVM classifier is designed for binary classification. Eskin et al. [51] and Honig et al. [52] used an SVM along with their clustering method for unsupervised learning. The obtained performance was comparatively better than both of their previous clustering method. A detail analysis of different approaches for IDPS using SVM as Classifier is shown at Table 4 in Section 9.2.

Neural Networks Approach: Neural Networks have been largely employed with success for complex problems such as Pattern Recognition, hand-written character recognition, Statistical Analysis. The basic idea of neural network is that, the system learns to look for the next command based on a sequence of previous commands by a specific user. It provides a better solution to the problem of modeling the user behavior in anomaly detection because they do not require any explicit user model. Ghosh et al [53] found that a “well trained, pure feed forward, back propagation neural network” which performed comparably on a basic signature matching system. There are many neural networks that can be used for ABIDS like Multilayer Perceptron’s, Radial Basis Function-Based etc. To protect from attack, the paper [54] introduces a Model for Cryptosystem Using Neural Network, which is of high security and low cost. Based on this model separate Encryption and Decryption Algorithm is presented. Also Training Algorithm for Multi-layered Neural Network is provided to hold secure multimedia data. The proposed work finds its application in medical imaging systems, military image database communication and confidential video conferencing, and similar such application [54].

With the Neural Network approach, false alarms were reduced by two orders of magnitude (to roughly one false alarm per day) and they increased the detection rate to roughly 80 % with the DARPA data base. System could detect old as well as new attacks not included in the training data, and in a lesser extent attacks distributed across multiple sessions. Two types of architecture of Neural Networks can be distinguished:

1) **Supervised training algorithms**, where in the learning phase, the network learns the desired output for a given input or pattern. The well-known architecture of supervised neural network is the Multi-Level Perceptron (MLP); the MLP is employed for Pattern Recognition problems.
2) **Unsupervised training algorithms**, where in the learning phase, the network learns without specifying desired output. Self-Organizing Maps (SOM) are popular unsupervised training algorithms; a SOM tries to find a topological mapping from the input space to clusters. SOM are employed for classification problems.

Intrusion detection system modeling based on neural networks and fuzzy logic is proposed in [59]. In this research, training data preparation is implemented as a preprocessing block composed of Self-Organizing Map (SOMs). Several networks with different characteristics are linked cascade and parallel for the purpose of creating SOM block. This block is used for reduction of training data through process of clustering data in smaller subsets. Training data are divided in clusters and used for training of ANFIS (Adaptive Network Based Inference System) components of the system. IDS hybrid structure consists of SOM block cascade linked with fuzzy system. The proposed hybrid structure is trained, tested and validated using KDD CUP 99 data set.

10.2. Data Mining Approach

Data mining can be better solution for IDS at its best to “pattern finding” and is defined [4] as the process of extracting useful and previously ignored models or pattern from the large data store. The data mining process is likely to reduce the amount of data that must be reserved for historical comparison of network activity, creating data that more meaningful to anomaly detection. Certain advantages of data mining technique that, it removes normal activity from alarm data to allow analysts to focus on real attacks. Identify false alarm generators and “bad” sensor signatures and find anomalous activity that uncovers a real attack. The data mining based approach can further be classified into following techniques:

Clustering Approach: Cluster analysis or clustering is the task of grouping a set of objects in such a way that objects in the same group (called a cluster) are more similar (in some sense or another) to each other than to those in other groups (clusters). It is a main task of exploratory data mining, and a common technique for statistical data analysis, used in many fields, including machine learning, pattern recognition, image analysis, information retrieval, and bioinformatics [4]. Clustering is an unsupervised technique for discovery of pattern in unlabeled data with many dimensions. Generally k-mean clustering is used to find natural grouping of similar instances. The records that are at a long distance from any one of this cluster indicate an unusual activity that may considered as new attack [55].

Classification Approach: The primary goal of classification is to learn from the class-labeled training instances for calculating classes of new or previously unseen data and new data is classified on the basis of the training set. Advantages of Classification-Based Techniques [56], especially the multi-class techniques, it uses the powerful algorithms that can distinguish between instances belonging to different classes. The testing phase of classification-based techniques are fast, subsequently each test case needs to be compared against the pre computed model.

10.3. Statistical Approach

Statistical modeling is among latest technique used for detection intrusion in electronic systems. Statistical based anomaly detection techniques use statistical properties and statistical test to ascertain whether the observed behavior deviate considerably from expected behavior [58]. There are two main steps in SABIDS process: First it creates behavior profiles for the normal activities and current activities. These profiles are matched based on several techniques to detect any kind of deviation from the normal behavior. SABIDS can further be classified into following categories:

Markov Process Model or Marker Model Approach: The Markovian model is used with the event counter metric to determine the regularity of particular events, on the basis of event which preceded it. This model characterized each observation as a specific state and utilizes a state transition matrix to determine if the probability of the event is high or normal, based on preceding events. It is useful when sequence of activities is particularly important. Markov chain keeps track of an intrusion by examining the system at fixed intervals and maintains the records of its state. If the state change takes place it computes the probability for that state at a given time interval and if this probability is low at that time interval then that event is counted as an anomalous [58].

Threshold Metric or Operational Model Approach: This particular model is based on the assumption that identification of anomaly by comparing the observation with a predefined limit. On the basis of cardinality of observation that observed over a certain period of time an alarm is generated. The operating model is most applicable to metrics where experience has shown that certain values are often associated with intrusions. For example an event counters for the number of password failure during a brief period, where more than suppose 10, suggest a failed log-in [58].

10.4. Knowledge based Approach

It collects knowledge about the specific attacks and system vulnerabilities and then applies this knowledge to exploit the attack and vulnerabilities to generate the alert. Any other event that the system is unable to recognize as an attack is accepted and hence the accuracy of the knowledge based IDS is considered good. However their main requirement is that their knowledge of the attacks be updated regularly [57]. The knowledge based detection technique can be used for both SBIDS and ABIDS.

Accuracy of this technique is good and it has a very low false alarm rate. A certain problem occurs while using this system as, completeness of this technique requires that their knowledge of the attacks be updated regularly. The knowledge based detection technique can further be classified as:

Expert System Approach: Expert systems are used mainly by knowledge-based IDS. For describing attacks it contains set of rules. Audit events are then translated into facts carrying their semantic significance in the expert system, and this rule and facts help inference engine for drawing conclusions. This method increases the abstraction level of the audit data by attaching semantic to it. The expert system can be used for both SBIDS as well as ABIDS.

State Transition Analysis: This technique is conceptually identical to model based reasoning, define the attacks with a set of goals and transitions and represent them as a state transition diagram. State transition diagram is a graphical representation of actions performed by an intruder to archive a system compromise. In this technique, an intrusion is considered as a sequence of action performed by an intruder those pointers from some initial state of a computer system to a target cooperated state. State transition analysis diagrams recognize the demands and the compromise of the penetration. They make lists of key actions that have to occur for the successful completion of an intrusion.

11. Conclusion and Future Work

Network threats are a security risk which can be met on a daily basis. Because of this, it is important today to consider more complex security options than just ordinary firewall systems. This paper deals about various types of attack on networks, the advantages and disadvantages of the solution called Intrusion Detection System (IDS) and Intrusion Prevention System (IPS), various classification of IDS and IPS, and used approaches for IDPS. This paper finds out the problem associated with secure communication over the networks.

Some intrusion detection systems have become very advanced, the data produced by software and the methods of the attackers are also becoming more complex all the time. This makes it hard to distinguish legitimate use of a system from a possible intrusion. When an IDS incorrectly identifies an activity as a possible intrusion it will results in a false alarm, also referred to as a false positive. Especially badly configured IDSs and behavior-based IDSs in particular can produce many false positives. In case of passive-response IDS, this could result in an excessive administrative load (getting paged for a false alarm every 3 minutes becomes annoying very quickly). In case of active-response IDS, this may even create a DoS situation. If the IDS would mistakenly block a legitimate user’s IP address. Therefore, it takes careful planning and consideration before implementing an IDS. Paper extracts the issues and focuses on why is there need of IDS and IPS for achieving secure service over the networks?

Since security is one of the key requirements to enable privacy. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure of data. In the future, work can be done on system design, algorithm design for secure communication over the complex networks.

References

[1] Shyam Nandan Kumar, “Cryptography during Data Sharing and Accessing Over Cloud.” International Transaction of Electrical and Computer Engineers System, vol. 3, no. 1 (2015): 12-18.

[2] Shyam Nandan Kumar, “DecenCrypto Cloud: Decentralized Cryptography Technique for Secure Communication over the Clouds.” Journal of Computer Sciences and Applications, vol. 3, no. 3 (2015): 73-78.

[3] Shyam Nandan Kumar, “Review on Network Security and Cryptography.” International Transaction of Electrical and Computer Engineers System, vol. 3, no. 1 (2015): 1-11.

[4] Shyam Nandan Kumar, “World towards Advance Web Mining: A Review.” American Journal of Systems and Software, vol. 3, no. 2 (2015): 44-61.

[5] Mark Handley, Vern Paxson, and Christian Kreibich, “Network Intrusion Detection: Evasion, Traffic Normalization, and End-to-End Protocol Semantics", 10th USENIX Security Symposium, Washington, D.C., pp.13-17, August 2001.

[6] Vern Paxson, “Bro: A System for Detecting Network Intruders in Real-Time," Computer Networks, 31, pp. 2435-2463, Dec. 1999.

[7] Y. Yasami and S. P. Mozaffari, "A novel unsupervised classification approach for network anomaly detection by k-Means clustering and ID3 decision tree learning methods," The Journal of Supercomputing, vol. 53, pp. 231-245, 2010.

[8] Michael E. Whitman; Herbert J. Mattord, “Principles of Information Security”, Cengage Learning EMEA, 2009.

[9] Intrusion Detection System, Wikipedia, https://en.wikipedia.org/wiki/Intrusion_detection_system#Network_intrusion_detection_systems, Oct-2016.

[10] Jeong H, Hyun W, Lim J, You I, “Anomaly teletraffic intrusion detection systems on hadoop-based platforms: A survey of some problems and solutions” (NBiS), 15th international conference on. IEEE, Melbourne, Australia, pp. 766-770.

[11] Cheon J, Choe T-Y, “Distributed processing of snort alert log using hadoop”, Int J Eng Technol(0975-4024) 2013, 5(3): 2685-2690.

[12] Lee Y, Lee Y, “Toward scalable internet traffic measurement and analysis with hadoop”, ACM SIGCOMM Comput Commun Rev, vol. 43(1), pp. 5-13.

[13] Bass T, “Intrusion detection systems and multisensor data fusion”, Commun ACM 2000, 43(4), pp. 99-105.

[14] Rouse M, “Security information and event management (SIEM), 2012.

[15] K. Das, “Protocol anomaly detection for network-based intrusion detection”, GSEC Practical Assignment Version 1.2f SANS Institute, 2001.

[16] F.N. Sabri, N.M. Norwawi, K. Seman, “Identifying false alarm rates for intrusion detection system with Data Mining”, IJCSNS International Journal of Computer Science and Network Security, vol.11, 2011.

[17] S.X. Wu, W. Banzhaf, “The use of computational intelligence in intrusion detection systems: A Review”, Applied Soft Computing Journal 10, 2010.

[18] S. Wu, E. Yen, “Data mining-based intrusion detectors”, Expert Systems with Applications 36, 2009.

[19] Jelena Mirkovic, Sven Dietrich, David Dittrich and Peter Reiher, “Internet Denial of Service: Attack and Defense Mechanisms”, Prentice Hall PTR, 2005.

[20] FBI agents bust 'Botmaster', Reuters News Service, November 4, 2005.

[21] Alex Lam, "New IPS to Boost Security, Reliability and Performance of the Campus Network," Newsletter of Computing Services Center, 2005.

[22] Y. F. Jou, F. Gong, C. Sargor, X. Wu, S. Wu, H. Chang, and F. Wang, “Design and Implementation of a Scalable Intrusion Detection System for the Protection of Networks Infrastructure," Proceedings of DARPA Information Survivability Conference and Exposition, vol. 2, pp. 69-83, January 2000.

[23] E. Y. K. Chan et al., “IDR: An Intrusion Detection Router for Defending against Distributed Denial-of-Service (DDoS) Attacks," 7th International Symposium on Parallel Architectures, Algorithms and Networks (ISPAN'04), pp. 581-586, May 2004.

[24] "NIST – Guide to Intrusion Detection and Prevention Systems (IDPS)", February 2007.

[25] Robert C. Newman, “Computer Security: Protecting Digital Resources”, Jones & Bartlett Learning, 2009.

[26] Tim Boyles, “CCNA Security Study Guide: Exam 640-553”, John Wiley and Sons, pp. 249, 2010.

[27] Harold F. Tipton, Micki Krause, “Information Security Management Handbook”, CRC Press, pp. 1000, 2007.

[28] Scarfone, Karen; Mell, Peter, “"Guide to Intrusion Detection and Prevention Systems (IDPS)", Computer Security Resource Center, National Institute of Standards and Technology (800-94), 2007.

[29] OSSEC, http://ossec.github.io/, Oct-20116.

[30] OSSEC, Wikipedia, https://en.wikipedia.org/wiki/OSSEC, Oct-2016.

[31] Open Source Tripwire, Wikipedia, https://en.wikipedia.org/wiki/Open_Source_Tripwire, Oct-2016.

[32] SNORT-Network Intrusion Detection & Prevention System, https://www.snort.org/, Oct-2016.

[33] SMART Watch, http://www.timberlinetechnologies.com/products/intrusiondtct.html, Oct-2016.

[34] BRO, Wikipedia, https://en.wikipedia.org/wiki/Bro_(software), Oct-2016.

[35] Prelude Hybrid IDS, Wikipedia, https://en.wikipedia.org/wiki/Prelude_SIEM_(Intrusion_Detection_System), Oct-2016.

[36] Suricata, https://suricata-ids.org/, Oct-2016.

[37] Oludele Awodele, Sunday Idowu, Omotola Anjorin, and Vincent J. Joshua, “A Multi-Layered Approach to the Design of Intelligent Intrusion Detection and Prevention System (IIDPS)”, Babcock University, vol. 6, 2009.

[38] Song, J., Takakura, H., Okabe, Y., & Nakao, K., “Toward a more practical unsupervised anomaly detection system, Information Sciences”, 231, pp. 4-14, 2013.

[39] Chopra, V., Saini, S., & Choudhary, A. K., “A Novel Approach for Intrusion Detection”, IJCSI, vol 8. Issue 4, pp. 294-297, 2011.

[40] Zhao, G., Song, J., & Song, J., “Analysis about Performance of Multiclass SVM Applying in IDS”, International Conference on Information, Business and Education Technology (ICIBET 2013). Atlantis Press, 2013.

[41] Araki, S., Yamaguchi, Y., Shimada, H., & Takakura, H., “Unknown Attack Detection by Multistage One-Class SVM

Focusing on Communication Interval", In Neural Information Processing, pp. 325-332, 2014, Springer International Publishing.

[42] Enache, A. C., & Patriciu, V. V., "Intrusions detection based on Support Vector Machine optimized with swarm intelligence", 9th International Symposium on Applied Computational Intelligence and Informatics (SACI), pp. 153-158, 2014, IEEE.

[43] Catania, C. A., Bromberg, F., & Garino, C. G., "An autonomous labeling approach to support vector machines algorithms for network traffic anomaly detection", Expert Systems with Applications, 39(2), pp. 1822-1829, 2012.

[44] Yi, Y., Wu, J., & Xu, W., "Incremental SVM based on reserved set for network intrusion detection", Expert Systems with Applications, 38(6), pp.7698-7707, 2011.

[45] Atefi, K., Yahya, S., Dak, A. Y., and Atefi, A., "A hybrid intrusion detection system based on different machine learning algorithms", 4th International Conference on Computing and Informatics, Sarawak, Malaysia, pp. 312-320, 2013.

[46] Ahmad, I., Hussain, M., Alghamdi, A., and Alelaiwi, A., "Enhancing SVM performance in intrusion detection using optimal feature subset selection based on genetic principal components" Neural Computing and Applications, 24(7-8), pp.1671-1682, 2014.

[47] Sung, A. H., & Mukkamala, S., "Identifying important features for intrusion detection using support vector machines and neural networks, Symposium on Applications and the Internet, pp. 209-216, 2003, IEEE.

[48] Y. Yasami and S. P. Mozaffari, "A novel unsupervised classification approach for network anomaly detection by k-Means clustering and ID3 decision tree learning methods," The Journal of Supercomputing, vol. 53, pp. 231-245, 2010.

[49] Garcia-Teodoro, Pedro, J. Diaz-Verdejo, Gabriel M.; Enrique V., "Anomaly-based network intrusion detection: Techniques, systems and challenges" computers & security, vol.28, no. 1, pp. 18, 28, 2009.

[50] Dickerson; John E., Julie D., "Fuzzy network profiling for intrusion detection", 19th International Conference of the North American Fuzzy Information Processing Society (NAFIPS), Atlanta, GA, pp. 301, 306, 2000.

[51] Eskin; Eleazar, Andrew A., Michael P., Leonid P., Sal S.,"A geometric framework for unsupervised anomaly detection: Detecting intrusions in unlabeled data", D. Barbar and S. Jajodia (Eds.), Data Mining for Security Applications, Boston: Kluwer Academic Publishers, May 2002.

[52] Honig; Andrew, Andrew H., Eleazar E., Salvatore S., "Adaptive model generation: An architecture for the deployment of data mining based intrusion detection systems", D. Barbar and S. Jajodia (Eds.), Data Mining for Security Applications. Boston, Kluwer Academic Publishers, May 2002.

[53] Ghosh; Anup K., Aaron S., Michael S., "Learning program behavior profiles for intrusion detection", 1st USENIX, 9-12 Apr. 1999.

[54] Shyam Nandan Kumar, "Technique for Security of Multimedia using Neural Network", International Journal of Research in Engineering Technology and Management, vol. 2, issue 5, pp.1-7, 2014.

[55] Jian P., Shambhu U., Faisal F., Venugopal G., "Data Mining for Intrusion Detection – Techniques, Applications and Systems", Data Mining Techniques for Intrusion Detection and Computer Security, University at Buffalo, New York, 2004.

[56] Varun C, Arindam B., Vipin K., "Anomaly Detection: A Survey", ACM Computing Surveys, Vol. 41, No. 3, Article 15, July 2009.

[57] Herve D., Marc D., Andreas W., "Towards a Taxonomy of Intrusion Detection Systems", Computer Networks, Elsevier, vol. 31, pp. 805, 822, 1999.

[58] Qayyum, A., Islam, M.H., Jamil, M., "Taxonomy of statistical based anomaly detection techniques for intrusion detection" IEEE Symposium on Emerging Technologies, pp. 270,276, 17-18 Sept. 2005.

[59] A. Midzic, Z. Avdagic, and S. Omanovic, "Intrusion detection system modeling based on neural networks and fuzzy logic", IEEE 20th Jubilee International Conference on Intelligent Engineering Systems (INES), 2016.

[60] Lijun Dong, Min Du, Shengsheng Yu, and Rongtao Liao, "Secure Vault: An Intrusion Prevention Model for Ender-Users", International Conference on Computational Intelligence and Security Workshops, CISW 2007.

[61] Alaa Al-hamami, and Tahani Alawneh, "Developing a Host Intrusion Prevention System by Using Data Mining", International Conference on Advanced Computer Science Applications and Technologies (ACSAT-2012).

[62] Satomi Honda, Yuki Unno, Koji Maruhashi, Masahiko Takenaka, and Satoru Torii, "TOPASE: Detection of brute force attacks used disciplined IPs from IDS log", IFIP/IEEE International Symposium on Integrated Network Management (IM), 2015.

[63] Shyam Nandan Kumar, and Amit Vajpayee, "A Survey on Secure Cloud: Security and Privacy in Cloud Computing", American Journal of Systems and Software, vol. 4, no. 1, pp. 14-26, 2016

[64] Shyam Nandan Kumar, and Amit Vajpayee, "ASP: Advanced Security Protocol for Security and Privacy in Cloud Computing." American Journal of Information Systems, vol. 4, no. 2, pp. 17-31. 2016.

[65] Shyam Nandan Kumar, "Advanced Technique for Monitoring and Shielding in Wi-Fi Technology", International Journal of Research in Engineering Technology and Management, vol. 2, issue 3, pp. 1-6, 2014.

[66] T.F. Lunt, A. Tamaru, F. Gilham, R. Jagannathan, P.G. Neumann, H.S. Javitz, A. Valdes, T.D. Garvey, "A realtime intrusion detection expert system (IDES) - Final Technical Report, Technical Report", SRI Computer Science Laboratory, SRI International, Melno Park, CA, February 1992.

[67] M. Crosbie, B. Dole, T. Ellis, I. Irsul, E. SpaffSord, "IDIOT - Users Guide", COAST Laboratory, Purdue University, 1398 Computer Science Building, West Lafayette, IN 47907-1398, September 1996.

[68] J. Hochberg, K. Jackson, C. Stallings, J.F. McClary, D. DuBois, J. Ford, "NADIR: an automated system for detecting network intrusion and misuse", Computers and Security vol. 12 (3), pp.235-248, 1993.

[69] L. Heberlein, G. Dias, K. Levitt, B. Mukherjee, J. Wood, D. Wolber, "A network security monitor", IEEE Symposium on Research in Security and Privacy, May 1990.

[70] S.R. Snapp, S. Smaha, D.M. Teal, T. Grance, "The DIDS (distributed intrusion detection system) prototype", USENIX Summer 1992 Technical Conference, San Antonio, TX, June 1992.

[71] S. Cheung, R. Crawford, M. Dilger, J. Frank, J. Hoagland, K. Levitt, J. Rowe, S. Staniford-Chen, R. Yip, D. Zerkle, "The design of GrIDS: a graph-based intrusion detection system", Technical Report CSE-99-2, Department of Computer Science, University of California at Davis, Davis, CA, January 1999.

[72] P.A. Porras, P.G. Neumann, "EMERALD: Event monitoring enabling responses to anomalous live disturbances", 20th National Information Systems Security Conference, National Institute of Standards and Technology, 1997.

[73] J.S. Balasubramaniyan, J.O. Garcia-Fernandez, E. Spafford, D. Zamboni, "An architecture for intrusion detection using autonomous agents", Technical Report 98-05, COAST Laboratory, Purdue University, May 1998.

[74] Kuang, F., Xu, W., and Zhang, S., "A novel hybrid KPCA and SVM with GA model for intrusion detection", Applied Soft Computing, vol. 18, pp.178-184, 2014.

[75] Chitrakar, R., and Huang, C., "Selection of Candidate Support Vectors in incremental SVM for network intrusion detection", Computers & Security, vol. 45, pp. 231-241, 2014.

[76] Tavallaee M, Bagheri E, Lu W, Ghorbani AA, "A detailed analysis of the kdd cup 99 data set", Second IEEE international conference on Computational intelligence for security and defense applications, IEEE Press, Piscataway, NJ, USA, CISDA'09, pp 53-58.

[77] Rohit Shukla, and Maninder Singh, "PythonHoneyMonkey: Detecting malicious web URLs on client side honeypot systems", 3rd International Conference on Reliability, Infocom Technologies and Optimization (ICRITO), 2014.

[78] Wan YuWen, You JinXin, Guo Fan, and Xu ShuFang, "Polymorphic worms signature extraction based-on improved ant colony algorithm", 9th International Conference on Computer Science & Education (ICCSE), 2014.

[79] Monther Aldwairi, and Koloud Al-Khamaiseh, "Exhaust: Optimizing Wu-Manber pattern matching for intrusion detection using Bloom filters", 2nd World Symposium on Web Applications and Networking (WSWAN), 2015.

[80] Eduardo Viegas, Altair Santin, Andre Franca, Ricardo Jasinski, Volnei Pedroni, and Luiz Oliveira, "Towards an Energy-Efficient

Anomaly-Based Intrusion Detection Engine for Embedded Systems", IEEE Transactions on Computers, vol: PP, Issue: 99, pp.1-1, 2016.

[81] Dipika Narsingyani, and Ompriya Kale, "Optimizing false positive in anomaly based intrusion detection using Genetic algorithm", IEEE 3rd International Conference on MOOCs, Innovation and Technology in Education (MITE), 2015.

[82] Manu Bijone, and Jitendra Dangra, "A Survey of Signature Based & Statistical Based Intrusion Detection Techniques", IJSRD - International Journal for Scientific Research & Development, Vol. 4, Issue 08, pp. 583-585, 2016.

[83] Geethapriya Thamilarasu, and Zhiyuan Ma, "Autonomous mobile agent based intrusion detection framework in wireless body area networks", IEEE 16th International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2015.

[84] N Santosh, R Saranyan, kumar P Senthil, and V. Vetriselvi, "16th International Conference on Advanced Computing and Communications, ADCOM 2008.

[85] Hisham A. Kholidy, Abdelkarim Erradi, Sherif Abdelwahed, and Fabrizio Baiardi, "HA-CIDS: A Hierarchical and Autonomous IDS for Cloud Systems", 2013 Fifth International Conference on Computational Intelligence, Communication Systems and Networks (CICSyN), IEEE.

[86] Hisham A. Kholidy, Abdelkarim Erradi, Sherif Abdelwahed, and Fabrizio Baiardi, "A hierarchical, autonomous, and forecasting cloud IDS", International Conference on Modelling, Identification & Control (ICMIC), 2013, IEEE.

[87] I-Hsuan Huang, and Cheng-Zen Yang, "Design of an Active Intrusion Monitor System", IEEE 37th Annual 2003 International Carnahan Conference on Security Technology.

[88] Han-Pang Huang, and Chia-Ming Chang, "An active network-based intrusion detection and response systems", IEEE International Conference on Networking, Sensing and Control, 2004.

[89] Khattab M. Ali Alheeti, and Klaus McDonald-Maier, "Hybrid intrusion detection in connected self-driving vehicles", 22nd International Conference on Automation and Computing (ICAC), 2016, IEEE.

[90] Iftikhar Ahmad, Azween B Abdullah, and Abdullah S Alghamdi, "Remote to Local attack detection using supervised neural network", International Conference for Internet Technology and Secured Transactions (ICITST), 2010, IEEE.

[91] Zorana Bankovic, Slobodan Bojanic, Octavio Nieto-Taladriz, and Atta Badii, "Increasing Detection Rate of User-to-Root Attacks Using Genetic Algorithms", International Conference on Emerging Security Information, Systems, and Technologies, IEEE, 2007.