IJEE 0973-7383 Volume-9 • Number-1 Jan -June 2017 pp. 125-137 available online at www.csjournals.com
UGC Recommended Journal http://ugc.ac.in/journallist

# A Review on Foundation of Network Intrusion Detection and Prevention Systems (NIDPS)

Aaruni Goel, Dr. Ashok Kumar Vasishtha
[1]Research Scholar, [2]Research Supervisor
Mewar University, Chittorgarh, INDIA

**Abstract:** Intrusion detection is the way toward checking the occasions happening in a PC or network framework and scrutinizes them for indications of feasible events, which are breach or approaching dangers of infringement of computer or network security strategies. Occurrences have many causes, for example, malwares, attackers increasing unlawful access to devices from the Internet, and permitted clients of network who abuse their benefits or try to get extra benefits for which they are not permitted.
**Keywords:** Sensors; intrusion detection and prevention; inline sensors.

## 1. Introduction

An intrusion detection system (IDS) is a sort of programming or configuration of security software(s) that captures the any type of intrusion detection. An Intrusion Prevention System (IPS) is like the IDS but with the abilities to attempt to stop possible malicious events too. Jointly they are known as IDPS (Intrusion Detection & Prevention Systems).

IDPSs are principally centered on recognizing feasible events. For instance, an IDPS could recognize when an attacker has effectively overwhelmed the network by abusing its weakness. The IDPS could then report the occurrence to Network Administrator (NA), who could rapidly start incident response activities to minimize the harm brought about by that event. The IDPS could likewise log information that could be utilized by the incident handlers. Numerous IDPSs can likewise be arranged to identifyviolation of security approaches. For instance, some IDPSs can be arranged with firewall rule-set like settings, permitting them to distinguish network activity that violates the security policy of the organization. Additionally, some IDPSs can screen record file transfer activities and recognize ones that may be suspicious, for example, duplicating an extensive database onto a client's system.

Numerous IDPSs can likewise recognize supervision action, which may show that an assault is up and coming. For instance, some assault tools and types of malware, especially worms, perform scanning exercises (port scans for resulting consequent attacks). An IDPS may have the capacity to stop reconnaissance and alert NA, who can take measures if necessary to modify other security controls to probable related events.

## 2. Types of IDPS Technologies

There are some sorts of IDPS which are new innovations and discussed as under:

*Wireless Intrusion Detection and Prevention System (WIDPS)*, screens wireless data movement and examines wireless networking protocols to distinguish doubtful deed including the protocol conventions themselves. It cannot distinguish distrustful doings in the application or higher-layer protocols (e.g., TCP, UDP) that the wireless network activity is exchanging [1].

*Host based Intrusion Detection and Prevention System (HIDPS)*, scrutinizes the attributes of a single host and the incidents happening inside that host for suspicious movement. Such system examines data traffic movement (just for

that host), host logs, running processes, applications status, access control, permissions and system files activity pertaining to associated host. Such IDPSs are most used in public access servers and on the servers which are dealing with sensitive information [2].

This thesis work will focus on only *Network Intrusion Detection and Prevention System (NIDPS)*, which screens data traffic for specific network partitions or devices and investigates the system and application protocol to recognize suspicious action. It can distinguish a wide range of sorts of incidents that NA has to pay attention timely.

## 3. Intrusion Detection Approaches

In this subsequent section different commonly used intrusion detection techniques are discussed on which packets are inspected [3].

### 3.1Signature-Based Detection

A signature is an instance that relates to a known danger in terms of cyber security. Signature-based detection is the way toward distinct marks against observed incidents with recognizes probable events or which is an infringement of an security approach of organization. Signature-based recognition is exceptionally powerful at distinguishing known dangers strategy since it just matches the present unit of movement, to a real data packet or log traces, to a list of signatures using string comparison operations. But such discovery generally insufficient at identifying already ambiguous dangers or zero day impacts, masked evasion by the utilization of sophisticated avoidance tools, and numerous variations of known dangers. This is the major drawback where the signature based strategy is totally failed.

### 3.2 Anomaly-Based Detection

Anomaly-based detection is the way toward matching of what movement is viewed as ordinary against inspected incidents to distinguish critical abnormalities. ANIDPS utilizing anomaly-based detection has profiles like inbuilt biometrics design identification that speak to the general typical response of such things as clients, hosts, organize associations, or applications. The profiles are produced by observing the qualities of usual action over a given time frame. The NIDPS then uses statistical techniques to match the qualities of current action with features identified with the previous recorded profile. Profiles can be created for some behavioral characteristics, for example, the number of messages sent by a client or total number of uploads and downloads etc... The significant advantage of anomaly-based detection techniques is that they can be useful to identify the zero days' attacks. Another issue with building profiles is that it can be exceptionally tough now and again to make them exact, in light of the fact that figuring effort can be very difficult.

In anomaly-based detection the profiles can either be static or element. Once produced, a static profile is unaltered unless the NIDPS is particularly forced to create another profile. Since networks and systems change after some span of time, the relating measures of usual behavior is additionally varied; thereby a static profile will in the long run get to be distinctly incorrect, so it should be renewed intermittently. A dynamic profile is balanced always according to the supplementary incidents are monitored. Dynamic profiles do not have this issue; however they are many time vulnerable to evasions techniques from aggressors. For instance, an assailant can perform little measures of malevolent effort every so often, and then gradually raise the repetition and amount of action. In the event that the

rate of progress is adequately moderate, the NIDPS may think the malicious drive is familiar conduct and include it in its profile. It should also be now worth full to notify that malicious action can also be recorded during the time of creation of profiles. At last anomaly-based NIDPS products often produce many false positives because of benign activity that deviates significantly from profiles, especially in more diverse or dynamic environments. Furthermore, it is often difficult for analysts to determine why a particular alert was generated and to validate that an alert is accurate and not a false positive [4].

### 3.3 Stateful Protocol Analysis

It is also termed as deep packet inspection. It is the way toward looking at matching previously recorded profiles for every protocol state against examined instances to recognize deviations. Different from anomaly-based recognition, which utilizes host or system particular profiles, deep packet inspection depends on manufacturer created general profiles that determine how specific protocols is to and is not be utilized [5].

The deep packet investigation implies that the NIDPS is fit for talent to scrutinize the packets on the basis of network, transport, and application conventions and protocols. For instance, when a client begins a File Transfer Protocol (FTP) session, the session is at first in the unauthenticated state. After using proper username and password client pairing requests with responses will be generated, the NIDPS can determine the result is positive after effectively discovery the status code and the connection becomes authenticated. It should be noted that performing the vast majority of the commands while in the unauthenticated state would be viewed as distrustful, yet in the authenticated state performing a large portion of them is viewed as genuine. The only problem in this scheme is that it is much time consuming as each and every packet is scrutinized [6][7].

## 4. Internal Modules of IDPS

This segment depicts the real parts of NIDPS arrangements and shows the most well-known system architectures for this section.

### 4.1 Tools and Devices

The main components that are contained in NIDPS solution are describes as below. More or less all are almost necessary for effective use of NIDPS in an organization [8].

*Sensor:* The main function of sensor is to monitor the activity along with its analyzing. The point for which sensor is termed for sensing so is that it is being taken in use for NIDPSs which make a use of monitoring the networks. They can be either of any format-hardware based or software based. A hardware based sensor is included for specific hardware and sensors. These structures are predictably boosted for sensor utilization, including particular NIC and associated drivers for effective capture of every packets (i.e. promiscuous mode) or other tools that support in investigation. Hardware sensors frequently utilize adapted operating system(OS) that NAs are not suggested getting openly. On the other hand software based sensor vendors distributed dedicated programmed software without dedicated physical hardware's. NAs can execute the software in their servers or systems that come across out with certain updates. The sensor is programmed to install that may incorporate a adapted OS, or it may be introduced in to a generally used OS usually as whatever different application would.

*Management Server:* Over characterizing it might said that a management server is a centralized machine that gets information from the sensors then and administers the collected information. A few management servers perform examination on the on-going happenings information received from the sensors and use to classify incidents that those specific sensors cannot. Facilitating the status of event(s) information is starting with diverse sensors or operators, for example, finding incidents actuated by those same IP (Internet Protocol Address) locations is known as correlation. For large organization multiple management servers are generally used to cope with heavy data traffic.

*Database Server:* It is defined as storehouse of information from the event that has been reported by sensors or a management server. The support to database servers is provided by many NIDPSs. It is used to help in creating rule set if ambiguity occurs and for analyzing the unforeseen events by NAs.

*Console:* A console is that is called a program which gives an interface to the NIDPS's clients and NAs. This particular is usually mounted on a PC or laptop computers. A few consoles are utilized for NIDPS management, just, for example, configuring and updating sensors, while other types are used for management and investigation purposes [9].

**4.2 Deployment of Sensors**

The choosing the appropriate network for the components, administrators also need to decide where the NIDPS sensors should be located. There are two types of sensor deployment-*inline* and *passive.*

An inline sensor is implemented so that the system activity which this implementation is examining must go through it, much like the data traffic linked with a firewall. As far as the technology is concerned, a number of inline sensors are mixed firewall/NIDPS devices, while others are just NIDPSs.

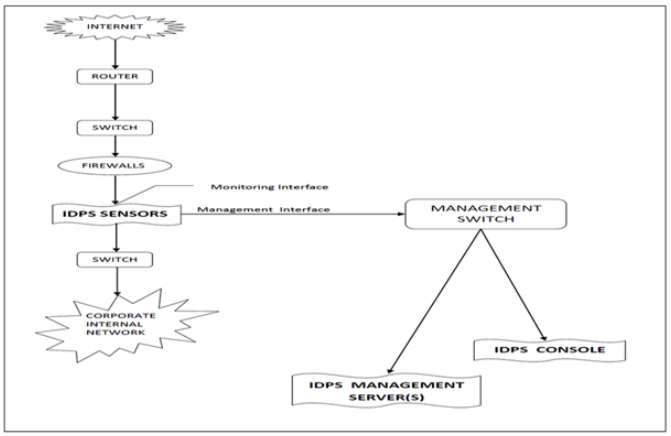


**Figure:1 Deployments of Inline Sensors**

The essential inspiration for sending NIDPS sensors inline is to empower them to stop assaults by choking network data traffic as per the rule-set in real time. Inline sensors are regularly put where network firewalls and other network security tools would likely to be set i.e. at the divisions between networks, for example, links with outside systems and borders between distinctive internal LANs that have to be isolated. Inline sensors that are not mixed

firewall/IDPS devices are regularly positioned on the more secure side of a network separation with the goal that they have less activity to prepare[10][11].

Figure: 1 shows such an organization. Sensors can likewise be put on the less secure side of a system separation to give physical prevention and decline the load on the isolating tool, for example, a firewall. This figure also depicts that the sensors one interface is always connected to management server through management switch for analyzing the network activities by the said server.

The passive sensors put across so it keeps an eye on a duplicate of the genuine data traffic across the network; no real traffic really goes through the sensor. The passive are normally sent so they can examine key network parts, for example, the separations amongst systems, and vital network sections, for example, movement on a Demilitarized Zone (DMZ) subnet. Figure: 2 shows the implementation of passive ports. Passive sensors can scrutinize the network traffic activity through different techniques, including the accompanying of spanning ports, network tap and ID load balancer. They are briefly discussed in this section.

Many switches have an option ofmultiple spanning ports, which is a port that can see all network activity related to data traffic which passes through the switch. Linking a sensor to a spanning port can permit it to observe the data traffic movement going to and from many be sited users. In spite of the fact that this checking technique is generally simple and cheap, it can likewise be dangerous [10].

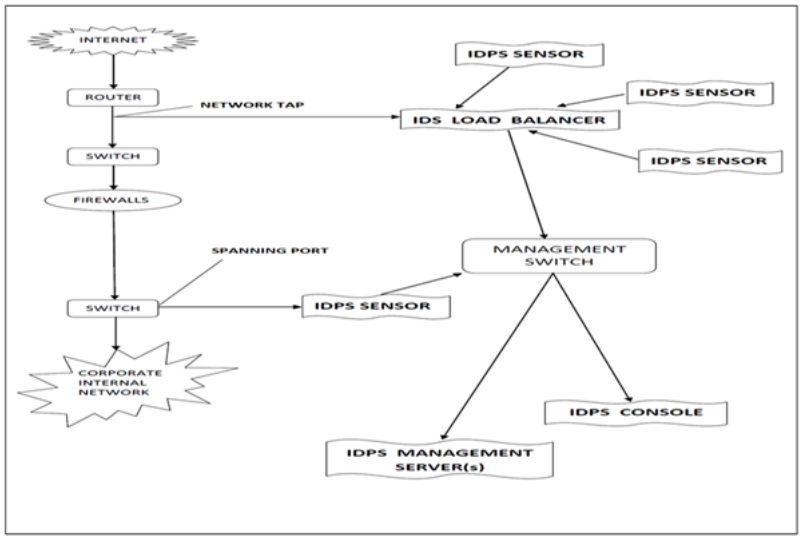


**Figure: 2 Deployments of Passive Sensors**

The problem with passive sensors depends upon switch and heavy data traffic load. If switch is supposed to not configured properly the over spanning port does not have the capacity to see all the movement of data traffic. Also under heavy data traffic load spanning ports are also not able to watch all the traffic. This may cause the hang state for switch also. Additionally, many switches have just a single spanning port, and there is regularly a need different advancements, for example, network forensic tools, network management tools which work upon the similar activity an relies on spanning port.

A network tap is an immediate joining together a sensor and the physical network media itself, for example, a fiber optic link. The tap gives the sensor a duplicate of all physical network activity being passed on the media. Introducing a tap by and large includes some network downtime, and issues with a tap could bring about extra downtime. Likewise, not at all like spanning ports, which are legitimately at hand due to presence of switches everywhere networks taps are to be acquired by paying price for it [11].

A NIDPS load balancer is a widget that accumulates and straight directly steer the movement of data traffic to inspecting frameworks, including NIDPS sensors. A load balancer can get duplicates of data traffic from at least one spanning ports or network taps and whole data traffic activity from various networks (e.g., rebuild a session that was part between two systems). The load balancer then dispenses duplicates of the activity to at least one listening devices, including NIDPS sensors, in view of a rule set created by NA. The set of rules tell the load balancer which kind of network traffic is to given to every listening device. Normal designs incorporate the accompanying:

- Send all data traffic activity to various NIDPS sensors. This should be possible for high accessibility or to have various sorts of NIDPS sensors perform simultaneous examination of a similar action.
- It divides among multiple NIDPS sensors the network traffic with great flexibility with respect to data traffic volume. This is normally done to perform load adjustment so that no sensor is left with the measure of movement of data traffic and relating examination.
-It also breaks up the data traffic activity among different NIDPS sensors in view of IP locations, protocols, or on the basis of upon different parameters. This should be possible for load adjusting purposes, for example, having one IDPS sensor committed to Web action activity and another IDPS sensor is checking all other data movement. This break up of data traffic should likewise be possible to perform more thorough examination of specific sorts of traffic activity (e.g., action including the most significant users).

Most methods for having a sensor counteract intrusions require that the sensor be sent in inline mode, not passive. Since passive mode screen a duplicate of the movement, they normally give no dependable route to a sensor to prevent the activity from achieving its goal. Thereby in long run corporate should implement inline mode if they need advantages of IPS too. Passive sensors are of no use if one wants to need IPS as this mode only observes the duplicate packets [9][11].

## 1. Modus operandi of IDPS

The working of IDPS depends upon various parameters like its security aspects, logging manner, detection and prevention measures and so on. Each one is thoroughly discussed in this section.

### 5.1 Security Procedures

Network based IDPS objects give a wide range of security abilities. Parts 4.4.1.1 through 4.4.1.4 depict regular security abilities, partitioned into four classifications: data gathering, logging, attack recognition and protection, separately.

5.1.1 Security ability

*Recognizing hosts:* ANIDPS sensor is being in the charge of capacity to make the record of all hosts present on the physical network on the basis of IP address or MAC address. The storage of such record can be utilized as a profile to recognize new users on the network [12].

*Classifying Operating Systems:* A NIDPS sensor may have the capacity to recognize the OSs and OS versions utilized by the organization users through different strategies. It is achieved as the sensor could track which ports are utilized on every host, which could show a specific OS or OS family (e.g., Windows, Unix, Mac). An alternate procedure is to break down packet headers for certain asymmetrical qualities or fusions of attributes that are shown by specific OSs (also termed as passive fingerprinting). A few sensors can likewise recognize application versions which now and again conclude which OS is being used. Knowing which OSs or OSvariants are being used can be useful in recognizing the possibility of vulnerability it has [13]**.**

*Distinguishing applications:* For some applications, IDPS sensors can distinguish the application versions being used. It is done by tracing which ports are utilized and checking certain attributes of use correspondences. For instance, when a client machine builds a very first communication with a server during the establishment of session, the server may tell the client what application server programming version it is running, and the other way around. Data on application versions can be utilized to recognize possibly weak applications, and unlicensed utilization of a few applications[12].

*Identifying network characteristics:* A few NIDPS sensors gather general data about data traffic movement identified with the design of system appliances and hosts, for example, the number of hops between client and server. This data can be utilized to recognize changes to the network structure [14].

5.1.2 Logging Capabilities

IDPSs normally perform comprehensive logging of data identified with distinguished incidents. This information can be utilized to affirm the legitimacy of alerts, examine events, and to logically link incidents between the IDPS and other logging sources. IDPS advancements normally allow NAs to store logs by local principles and send duplicates of logs to brought together logging servers (e.g., syslog, mysql and so forth.).Network based IDPS logging may be incorporated with the following fields:

- Time Stamp: At what day and what time particular event was occurred.
- Session ID: A distinctive number generated during the establishment of each TCP connection.
- Alert type: In terms of priority, severity or confidence which shows the impact of event on network.
- Protocols used: The communication between source and destination is dealing with which type of protocol i.e. Network Layer, Transport Layer and /or Application Layer.
- Location: Source and Destination socket addresses
- Packets count: Number of packets (or bytes) transmitted during the session establishment and termination.
- State related information: For instance, authentication of username

Most network based IDPSs can likewise perform packet exclusion. Normally this is done once an alarm has happened, either to list down resulting action in the session or to record the whole session if the IDPS has been incidentally putting away the past packets.

The logs are extremely important in terms of research for new attacks, defense strategy and forensics analysis.

5.1.3 Detection Strategy

Network based IDPSs ordinarily offer wide recognition abilities. Most objects utilize a blend of signature based, anomaly based and stateful based examination procedures to perform inside and

out investigation. The said such examination techniques are generally firmly tightened.

Another noteworthy question which may arise what are the detection capacity of an NIDPS? The answer is simple and states that detection competence of an NIDPS include- Kinds of incidents detected, detection exactness, fine-tuning and customization accordingly and its limitations. Kinds of incidents include malicious reconnaissance activities against- application layer protocols in the form of attacks (i.e. banner grabbing, buffer overflows, format string attacks, cracking password, malware diffusion), transport layer protocols (i.e. port scanning, abnormal packet fragmentation, SYN floods, DDoS), network layer protocol (spoofed IP addresses, illicit IP header values), unexpected application services(i.e. tunneled protocols, backdoors, hosts running unauthorized application services)and at last policy violations (i.e. use of wrong Web sites, use of banned application protocols). NIDPS sensors are usually designed to stop assaults regardless of whether they are probably going to be successful, however an NIDPS may in any case log the action with various precedence levels relying upon what its result most likely would have been if not blocked.

Detection exactness is determined on the basis of false positive and false negative impacts. More current advancements utilize a blend of identification techniques to build exactness and the extent of recognition, and by and large the rates of false positives and false negatives have declined. False positives and false negatives for system based NIDPS sensors can be diminished fairly due to the multifaceted complications during incidents are being checked. A dedicated sensor is frequently observing activity including hundreds or a huge number of inside and outside hosts. The number and versions of OSs and applications being used over the surveillance network can be tremendous; likewise, OSs and applications are always being changed [15].

This makes unfeasible to compile all the activities for a sensor that it watches. Far more dreadful, sensors need to view actions for a wide range of mixes of web servers and clients. There are numerous many web servers associated with several versions that use to interact with numerous web browsers and their versions. Every joint effort of web browser and server could have distinctive communication characteristics (e.g., sequence of commands and corresponding response codes) that could affect the exactness of investigation. Because it is like a count calculated in terms of permutation between the communication of different web servers and web browsers. Likewise, security control parameters between servers and firewalls, varied configurations setups and customizations could bring about extra challenges for sensors.

Still sensors do their jobs at their work but it is more needed that reduce the load of sensors for better results. Therefore the tuning and customization techniques are the process to improve the detection rate. Network based NIDPSs normally require comprehensive tuning and customization to enhance their detection exactness. Illustrations of tuning and customization abilities are thresholds (a boundary between normal and abnormal behavior expressed in the form of value. It is the maximum suitable value, for example, maximum unsuccessful login efforts in a given set of time, or maximum number of length of password) for port scans and application authorization efforts,

blacklists (it is nothing but the object that involves in malevolent activity like TCP, UDP port numbers, ICMP codes, Specific IP addresses etc…) and whitelists (this is just simple list of objects that are considered genuine like TCP, UDP port numbers, ICMP codes, specific IP addresses etc…) for host IP addresses and usernames, and alert ready situations. The NIDPSs can utilize data with respect to the organization's hosts to enhance recognition exactness. For instance, an NIDPS may permit NAs to determine the IP addresses utilized by the premises' web servers, mail servers, and other normal sorts of hosts of organization and additionally indicate the sorts of administrations gave by every host (the kind and versions of web server application running by every Web server). This permits the IDPS to better organize alerts. Some network based NIDPSs can likewise import the outcomes of weakness outputs and utilize them to figure out which assaults would likely be effective if not blocked. This permits the NIDPS to make better choices in terms of prevention activities and organize alerts all the more exactly [16].

5.1.4 Prevention Approach

Network based IDPS sensors proposed different prevention capacities, including the accompanying (clustered by kind of sensor) [5]: Working of both the inline and passive modes are as under:

- Passive Mode- A passive sensor can effort to close a current TCP session by directing TCP reset packets to both source and destination.The objective is for one of the endpoints to terminate the link before an assault can succeed. But, much of the time the reset packets are not got in time on the grounds that the attack activity must be checked and blocked, the assault identified, and the packets sent over systems to the endpoints. Likewise, since this method is just pertinent to TCP, it can't be utilized for attacks taken for different kinds of packets, including UDP and ICMP. Session killing is definitely not generally utilized any more on the grounds that other, recent innovated prevention capacities are more viable.
- Inline Mode - Most inline IDPS sensors offer firewall capacities that can be used to drop or reject suspicious network traffic.If there is chance that a specific protocol is being utilized improperly, for example, for a DoS assault, malware transmission, or data sharing, some inline IDPS sensors can confine the rate of network data transfer capacity that the protocol can utilize. This movement keeps away adversely affecting data transfer capacity utilization for different resources. Some inline IDPS sensors can clean part of a packet, which implies that infected matter is supplanted with genuine content and the purified packet sent to its goal.

Some sensors that goes about as an intermediary like a proxy may perform programmed standardization of all activity, for example, repackaging application payloads in new packets. This has the impact of disinfecting many assaults including packet headers and some application headers, regardless of whether the IDPS has recognized an assault. A few sensors can likewise strip tampered parts in the form of attachments from e-messages and expel other discrete bits of malevolent content from network traffic.

Most NIDPS advancements additionally offer characteristics that make up for the utilization of normal evasion methods. Evasion is altering the configuration or timing of deleterious actions so that its appearance changes however its impact is the same. Attackers utilize evasions to attempt to keep NIDPS skills from recognizing their assaults. For instance, an attacker could encode content characters especially, realizing that the target comprehends the encoding and trusting that any observing NIDPSs do not. Most NIDPS advancements can defeat regular

avoidance strategies by copying unique handling performed by the objectives. In the event that the NIDPS can watch the action similarly that the destination would, then evasion techniques will for the most part be unsuccessful at masking attacks. Most NIDPS sensors permit NAs to indicate the prevention capacity, that is, a type of arrangement for every sort of alarm. This more often than excludes allowing or disallowing counteractive action, and determining which expected ability ought to be utilized.

**5.2 Supervision over IDPS**

Once a network based IDPS component has been chosen, the NAs need to outline engineering, performNIDPS testing, secure the NIDPS parts, and after that implement them.

About all NIDPS items are intended to be worked and kept up through a graphical user interface (GUI), otherwise called the console. The console ordinarily allows NAs to arrange and redesign the sensors and management servers, and also examine their status (e.g., sensor failure, packet dropping). NA can likewise administer client accounts, alter reports, and perform numerous different capacities utilizing the console. NIDPS clients can likewise perform many capacities through the console, including observing and scrutinizing the NIDPS information and producing reports. A few NIDPS items additionally give better access control, for example, determining for which sensors specific clients can examine information then again produce reports or specific NAs can adjust arrangements. This permits an extensive NIDPS implementation to be separated into logical blocks for operational purposes [11].

A few NIDPS items likewise deal with command line interfaces (CLI). Not at all like GUI consoles, which are normally utilized for remote administration of sensors and management servers, CLIs are normally utilized for local administration of those parts. Some of the time a CLI can be come to remotely through encrypted scheme set up through secure shell (SSH) or different means. Another thing to be noticed is about up gradation of IDPS. There are two sorts of NIDPS upgrades i.e. software upgrades and signature redesigns. Software upgrades settle bugs in the NIDPS software or include new innovations, while signature upgrade on the other hand include new identification capacities or refine existing discovery abilities (e.g., lessening false positives). For some NIDPSs, signature upgrades cause program code to be modified or supplanted, so they are truly a specific type of software upgrade.

**5.3 Combination of different Tools**

Numerous organizations utilize various NIDPS solutions; ordinarily from various manufacturers (most suppliers make items in just a single kind of NIDPS innovation). As a matter of course, these solutions work totally autonomously of each other. This has some prominent advantages, for example, minimizing the effect that a failure of one has on the other different NIDPS solution. But the solutions are most certainly not coordinated in any capacity; the suitability of the whole NIDPS usage might be to some degree constrained. Data and information cannot be shared by these solutions, and NIDPS clients and NAs may need to consume additional strength to examine and deal with numerous arrangements of solutions. NIDPS items can be specifically unified, for example, one solution nourishing alert code to another solution, or they can be combined somewhat indirectly in a way, for example, every one of the IDPS solutions sustaining alert code into a Security Information and Event Management system (SIEM).

Thereby indirect NIDPS combination is generally performed with SIEM software. SIEM programming is intended to import data from different security-related logs and correlate incidents among them. Log types normally

strengthened by SIEM programming and incorporate IDPSs, firewalls, anti-malwares, and other security software's; OSs (e.g., audit logs); application servers (e.g. Web servers, email servers).

Another option to utilizing SIEM programming for integrated logging is to utilize the syslog protocol. Syslog gives a basic system to logging, log storage, and log transmission that any NIDPS could utilize if intended to do as such. Some NIDPSs offer components that permit their log designs to be changed over to syslog layout. Syslog is extremely adaptable for log sources, on the grounds that each syslog passage contains a content field into which logging sources can put data in any configuration. But this adaptability makes examination of the log information difficult. Every NIDPS may utilize various configurations for its log messages, so a strong investigation program would be acquainted with every layout and have the capacity to separate the significance of the information inside the fields of every organization [10].

## 2. Conclusion

IDPS behavior of network needs a specialized and expertise security expert in framing the rule set. A little error in rule set can proved to be a major security breach. In future by developing user friendly and authentic programs one might be easily configure rule set and less expertise is needed but till date no such genuine programs are available. Furthermore the work on automation of rule set is under process which in near future can be a big boon for small and medium industries that are not able to pay employ security expert.

It has been seen whenever we work on IDS\IPS and related package over server, the speed of server becomes slow however the implementation of snort provides minimum disturbance to any host in the network.There are large sets of rules with the help of which all the different types are attacks are diagnosed. Thus information processing and related correlation of attacks and rules takes some time to identify properly the genuine data traffic.

The analysis and correlation of the facts to identify the suspicious nature of data traffic in a network is really a big issue. This issue does not only affect the speed of the machine of the monitoring host but also give birth to other production disputes. As we have seen during the study of different approaches of intrusion detection in section 3, signature based approach has its own advantage that it detects the attacks very fast without raising false alarms. The drawback lies that it is incompetent in handling new attacks. Thereby, it can be said that if NAs create signatures in large amount then the chances of signatures contradiction and problem of correlation will likely to increase. The Zero day attacks again have a chance to be narrow escaped. If we compare the above discussion with anomaly based approach then no doubt it can provide the possibility to detect of zero day attacks by identifying uncommon patterns which further can be transformed to outline new signatures but again this approach produces too much false alarms that it is quite problematic for NAs to find out whether the present activity is anomalous or not. In the anomaly approach making profiles is also a much tough and challenging task because the behavior of user and his activities changes over time and also this behavioral style varies from one user to another. Furthermore in different time segments as per the job assigned to user his view point and behavior again changes. Here we can surely say that anomaly based approach is also not the perfect solution because many signatures will be created to identify the anomalous nature of a single user as well and need to be modified time to time. The last approach is the deep packet inspection methodology. This is well suited approach to identify all the attacks related to networks because it not

only analyses the packets on the basis of renowned authentic protocols but it also checks out the proper implementation of such networking protocols. But this inspection method takes long time to analyses the data packets which are not appropriate during busy office hours. Further in this method it is also to be considered that sometimes during vigorous attack on high speed network can make the situation vulnerable because packets may be dropped and data traffic is not thoroughly analyzed. In precise we can say that the performance of snort is really a major aspect that has to consider at all levels.

Due to the said facts the designers should concentrate on hybrid approaches to identify the attacks and to optimize the performance. Various algorithms have been devised and being devising for improving network performance of NIDPS. With the help such high performance algorithms and recent technological paradigms systems it can be expected that in coming time are easily handle multi gigabits of input. On this basis it is the speculation that in future this is not a big deal to create hybrid models for checking intrusions along with optimizing the networks of the organizations.

Last and not least the intrusions over the network are also taken place by mysterious and choked bandwidth, misused services on the network, connection through proxy websites or proxy softwares or unidentified misconfigured networks or unsolved log entries. The said notifications are primarily focused any type network intrusions as in case of ours. Beside this there are many other symptoms which prelude any type of network intrusions and are not limited to modification or deletion of softwares or logs, automatic rebooting of system, unusual hang state, unknown accounts, new login accounts, anomalous nature of users.

The aforesaid mentioned are all the conclusions are based mainly on computer and network security in terms of hardwares and softwares. But as said earlier we should not forget physical security in this too as it is the infrastructure by itself which protect us first from outsider.

This review has demonstrated that both the intrusion detection and prevention frameworks still should be enhanced to guarantee an unfailing security for a system

**References**

[1] Hutchison, K., Wireless Intrusion Detection Systems, SANS Institute InfoSec Reading Room, A White paper, 2005. Online Available: https://www.sans.org/reading-room/whitepapers/wireless/wireless-intrusion-detection-systems-1543

[2] Giovanni, V. and Kruegel, C., Host-Based Intrusion Detection, Reliable Software Group, Technical University Vienna, 2005.

[3] Ghorbani, A.A., Lu, W. and Tavallaaee, M., Network Intrusion Detection and Prevention Concepts and Techniques, Springer, 2010.

[4] Bahrololum, M., and Khaleghi, M., Anomaly Intrusion Detection System Using Hierarchical Gaussian Mixture Model IJCSNS International Journal of Computer Science and Network Security, Vol.8, issue 8, August 2008.

[5] FangluGuo and Tzi-ckerChiueh, Traffic Analysis: From Stateful Firewall to Network Intrusion Detection System, Computer Science Department, Stony Brook University, NY 2005.

[6] Check Point, Stateful Inspection Technology Tech Note. Online Available:

http://www.checkpoint.com/products/security/whitepapers/firewall-1_statefulinspection.pdf. March 2002

[7] Guido van Rooji, Real Stateful TCP Packet Filtering in IP Filter. Online Available: http://www.iae.nl/users/guido/papers/tcp filtering.ps.gz

[8] Tiwari N., Singh, S. R. and Singh, P. G., Intrusion Detection and Prevention System (IDPS) Technology-Network Behavior Analysis System (NBAS), International Science Congress Association , pp. 51-56, 2012.

[9] Scarfone, K., Mell, P., Guide to Intrusion detection and prevention systems (IDPS), NIST, pp. 1-127, 2007. Online Available: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf

[10] Chen, H. *et al*., A Multi-objective Optimization Approach to IDS Placement, Springer,2009. Online Available: http://link.springer.com/chapter/10.1007%2F978- 3-642-04091-7_13#page-1.

[11] Kent, K., Chevailer, S., Grance T. and Dang, H. , NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response. Online Available: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf

[12] Bejtlich, R., The Tao of Network Security Monitoring: Beyond Intrusion Detection, Addison-Wesley, 2004.

[13] Marchette, D., Computer Intrusion Detection and Network Monitoring: A Statistical Viewpoint, Springer, 2001.

[14] Crothers, T., Implementing Intrusion Detection Systems: A Hands-On Guide for Securing the Network, 2002

[15] Vacca, J. R., Computer and information security handbook: Morgan Kaufmann Series in Computer Security, First edition, May 4, 2009.

[16] Godbole, N., Information systems security: Security Management, Metrics, Frameworks and Best Practices, John Wiely Publishers, All Chapters, 2009.