IJCSE International Journal of Computer Sciences and Engineering Open Access

Review Paper Volume-3, Issue-12 E-ISSN: 2347-2693

A Taxonomy of Network Intrusion Detection System for Wireless Communication

R. Karthik[1*] and B.L. Shivakumar[2]

[1*]*Department of Information Technology, Kongunadu Arts and Science College, India*
[2]*Department of Computer Applications, Sri Ramakrishna Engineering College, India*

www.ijcseonline.org

Received: 29/Nov/2015 Revised:07/Dec/2015 Accepted:20/Dec/2015 Published: 31/Dec/21015

***Abstract*—**Nowadays, it is essential to give a high-level security to protect highly sensitive and private information. Network Technology and Internet Application sector plays a vital role in today's trend. Over a few years, we are able to see a tremendous growth towards the network technology. With the help of internet facility, we are able to carry out different tasks such as internet banking, online education, social networking and so on, which make our life more comfortable. Numbers of clients are being connected with the technology day by day. Despite being hacked by unwanted intruder or malicious.This cause a great damage to the documents, software and the confidential data's. Terms such as worms, viruses and Trojans create fear in the internet clients. Because of security and safety against these acts, it can be done only with our system, which will be able to sense and reply these attack or penetration. A very helpful tool in this is Intrusion Detection System (IDS), which detects the attacks and analysis it to take appropriate decision against it. Intrusion Detection System has a great impact on cyber security and network vulnerability. Once the detection is marked, the corresponding action could be taken by IDS. Intrusion detection system is a softwareand hardware device. This paper will illustrate us an overview of IDS and to create a secure zone in the sector of networking. Furthermore, appropriate problems and challenges in this field are consequently illustrated and discussed.

Keywords—Security Signature, Intrusion detection, Network Attacks, Prevention System, Analyzer, DOS,Misuse detection, Anomaly detection.

I. INTRODUCTION

Every computer system is constantly at risk for unauthorized and intrusion, however, with sensitive and confidential in sequence are at a higher risk. Intrusion Detection System is a method in information security, which plays a vital role in detecting different types of attacks and protects the network system. An IDS is the process of observing and analyzing the events arising in a computer system or network system to spot all security problems. Network intrusion detection systems support the most widely deployed system. A Network Intrusion Detection System (NIDS) attempts to spot malicious activities such as denial-of-service (DOS) attacks, port scans and observing the network traffic attacks. However, they stay entirely unsuccessful against those attacks that are so far unfamiliar and these can be combated just once they are detected physically and a signature is produced for them [1]. Network security has received a wide attention due to the supporting security concerns in networks.

A network-based Intrusion Detection System generally consists of a network application with a Network Interface Card (NIC). A wide mixture of algorithms have been planned which can detect and conflict with these security risks. With these proposals signatures based network intrusion detection system has been a commercial winner and have seen a widespread acceptance. There are two general approaches of NIDS implementation: Signature based system, Anomaly detection based system. These approaches expand the basis of several currently present intrusion detection techniques. Now almost anyone can exploit the vulnerabilities, analyze data integrity, and more on a desktop system due to the wide accessibility of attack tools. The predictable method for securing desktop systems is to create security mechanisms, such as firewalls, verification mechanisms, 'Virtual Private Networks' (VPN) which form a protective "shield" around them.

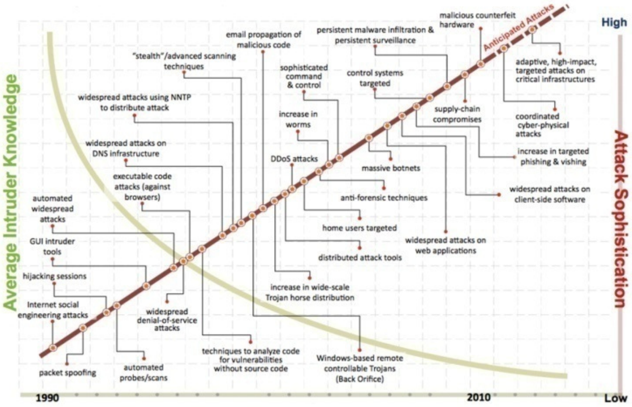

Figure 1: Attack Sophistication vs. Intruder Technical Knowledge [2].

The figure 1 illustrates the Attack sophistication vs. Intruder technical knowledge. During the 1990's the intruder attacks on the network, hacking was high but in the coming up years with the increasing techniques, the intruders have decreased relatively.

There are three functions in IDS: monitoring, detecting and generating an alert. IDS are frequently considered as the functionality of the firewall. However, there are variations between them. A firewall must be considered as a boundary that protects the information flow and prevent intrusions where as IDS detects if the network is under attack or if the security required by the firewall has been entered. Mutually firewall and IDS develop the security of the network. This section is called intrusion detection and it is complementary to predictable security mechanisms [3]. In this paper the efficiency, various techniques, types of IDS, role of NIDS, types of attacks, taxonomy of IDS, and a real time analyzer tool has been discussed.

II. LITERATURE REVIEW

Intrusion detection theory was established in early 1980's after the development of internet with observation end monitoring the threat [4]. There was a rapid increase in status and integration in security infrastructure. As mainframe, PCs were common and all clients were limited to it, early IDS were largely host based. In such cases, intrusion detection was alerted on insider threats and with the outside world was unusual. Security threat events were reported eventually when information were collected at the mainframe and analyzed. The development of computer networks provides an enhancing focus on IDS. Initial attempts in a networking atmosphere were made on enabling interaction between host based IDS and network-based IDS then swapping information moreover through a raw audit trace over the network or to issue the alarms generated by local analysis [5]. Nowadays, many systems provide an integrated tool by combining network-based and host-based variants which are typically called as hybrid IDS. For example in the distributed IDS developed by Snapp et al., Haystack is used for the entire host to detect neighboring attacks and Network Security Monitoring (NSM) monitors the network. Both send information to the Distributed Intrusion Detection System (DIDS) director to perform final analysis. Network/host based IDS are incapable to detect unauthorized use of particular applications, which in turn paved way for application based IDS. This IDS spotlights on monitoring interactions between a user and particular applications. Recent year's intrusion detection researcher's focus on identifying attacks in wireless environment therefore wireless network population is increasing [6]. As wireless networks, are highly sensitive and insecure, eavesdropping and congestion attacks are easy, thus extra security policies and précised intrusion detection techniques are needed.

III. EFFICIENCY OF INTRUSION DETECTION SYSTEMS

Some preferred uniqueness of intrusion detection systems has been recognized.

A. Prediction Performance

In IDS, easy performances are been calculated such as prediction accuracy is not sufficient. For example, the network intrusion representing the entire network traffic by a very small percentage and achieving 99% accuracy by unimportant IDS that normally tags all the network traffic. The ability to correctly identify intrusions and the inability in identifying legitimate action as an intrusion results in showing a good prediction performance. The predictive performance measures to evaluate IDs comprise detection rate and copied alarm rate. Detection rate is labeled as the part of numbers, suitably detected attacks and the entire number of attacks as the false alarm, false positive rate is the ratio of numbers, which are classified incorrectly as attacks of common connections. Generally, it is hard to calculate these two actions, as it is typically impracticable to have universal data of all attacks [7]. Whereas detection rate and false alarm rate are regularly in, different estimation of IDS is also executed using Receiver Operating Characteristics analysis.

B.Time Performance

The entire time required for the IDS to detect an intrusion refers to the time performance of IDS. The processing time and the propagation time are also combined in this. The processing time is dependent on the processing speeds of the IDS, which in turn is rated at the processes audit events. The processing of real-time security incidents may not be adequate if the rate gained is not sufficiently high. The propagation time is the time essential-for processing data to propagate to the security analyst [8]. The minimum rate of both these times permit the security analysis adequate time for reacting towards an attack and to end an attacker from changing audit data or shifting the IDS before causing much damage.

C. Fault Tolerance

An IDS must be able to provide a secure service and recuperate swiftly from successful attacks and it must be reliable, strong and resistant to attacks. This case is very common in large DOS attacks, deliberate attacks and buffer overflow attacks which can collapse the computer system, in turn the IDS and can shut down too. This feature plays an important role in appropriate functioning of IDS. While the majority of commercial IDS run on OS and group of systems, which can be easily, attacked. In addition, IDS should be alert in preventing huge number of false or confusing alarms that are caused by adversaries [9]. Such that alarms may simply have a harmful collision on the accessibility of the system, and IDS should be rapidly conquering these barriers.

IV. INTRUSION DETECTION SYSTEM TECHNIQUES

The different methods used for completing the preferable elements of IDS are:

A.Misuse Detection

Misuse Detection is derived from widespread information of well-known attacks with flaw in a system given by the computer professional. Uses of the misuse detection are to detect the hackers that they try to execute the attacks as well as to utilize the recognized flaws of the data. It is precised in identifying recognized attacks; it cannot spot the unidentified attacks with increasing computer-generated threats to the data [10]. It is the frequent method implemented in intrusion detection system in recent days. The benefit of this method is that it has the capability to produce precised outcome with less fake alarms. The drawback is that it will spot only the identified attacks.

i) Signature Based IDS

Signature based Intrusion Detection System uses a set of rules to recognize intrusion by surveillance for model of events exactly to identified and recognized attacks. The mentioned signatures are utilized to resolve the data transmit or receive the different streams crossing in the course of network connection; As soon as the stream equalizes a signature, suitable act is preceded. Usually, a security signature has been classified as a string, port and header condition signature. Signature descriptions are been stocked up in the database required to be precise so that differences of the famous attacks will not be losed. It can be leaded in constructing large databases, which occupies a block of memory.

ii) String Signatures

String signature seeks a series of ASCII symbols, which denote a possible attack. An example, of string signature is "cat + +" > /. rhosts” for UNIX which, carry out might cause the system turn out to be exceptionally vulnerable to set of connection attacks. Simple strings can guide to numerous false positives, so it is essential to clear the string signature; in favor of this reason they can utilize a compound string signature. A familiar Web server attack of a compound string signature can be “CGI-Bin” (Common Gateway Interface), “aglimpse” and “IFS” (Integrated File System).

iii) Port Signatures

Port signatures frequently utilized for the link setup, which tries to familiar, and repeatedly attacked ports. An example, of these ports consist of Telnet (Transfer Control Protocol port 23), FTP (Transfer Control Protocol port 21/20), SUNRPC (Transfer Control Protocol /User Datagram Protocol port 111), and IMAP (Transfer Control Protocol port 143). The incoming packets to these ports are unimpressed, and then any of these ports are not used in this site.

iv) Header Signatures

Header signatures observe for unsafe or illegal mixture within packet header fields. The prominent instance of packet’s port field is Urgent pointer, Network BIOS port as well as the Out Of Band data pointer is set. In previous edition of Windows Operating system, this outcome would be in BSOD (blue screen of death). TCP packet is a well-known header signature in which mutually SYN (synchronize) and FIN (finish) flags are set and is sent to a precised host. This shows that the creator is trying to begin and end a relationship concurrently [11].

B. Anomaly Based

Anomaly based watches over the network congestion and contrasts it besides the well-known baseline of the usual congestion profile. A basic characteristics for the set of connections is basically the usual bandwidth consumption for regular protocols utilized to evaluate the grouping of port numbers, devices, which aware the supervisor or client abnormal congestion be, noticed which to be considerably differed from the baseline of “normal” behavior and “anomaly”.Anomaly based is personalized to select what will be examined usual behavior with anomaly, but broadly established act of thumb is that, a few events, which take places at a rate better than two standard deviations as of the statistical norms, must be examined doubtful.

Some Examples of Anomaly based:

1. A client turns on and off a system 30 occasions within a day as an alternative of the usual way of 2 to 4 occasions a day.
2. A computer is being used by the user around 3:00 AM, which is not of the business hours.
3. A Network IDS will be able to examine the client samples for instance summarizing the set of instructions, which are frequently implemented. When a client in the managerial section quickly initiates to implement the set of instructions as of the engineering partition else it starts to assemble a key followed by the system will be able to quickly aware the administrator. For instance, anomaly based IDS can guide towards a large pace of fake detection that is termed as false/fake positives.

In general, it is hard to maintain low fake positives into any system, which sets to forceful approach to identify anomalies. For instance, it is hard to differentiate flash group from a DDoS attack, so a system can increase fake alarm in a flash group action guessing which is named asDDoS attack. Likewise, set of connections remodel and temporary crash, which might quickly alter the congestion profile, which wrongly raises an alarm. Following test relates by the statement completed with these systems which attacks at all times be anomalous, that is not essentially right. The intellectual attacker might build up intrusion systems that reason for nominal disturbance within the vital congestion that might go off invisible.

In designing the system deals by the accessibility of a collection of related sets, which will be the usual type of congestion [12]. Reasonably, the guessing which stays alive from attack-free set of information's for guidance, a detector external is used to replicated the set of information's which will not give an exact guessing. Standard set of connected systems congestion has a huge amount of scans, DOS attacks, and backscatter and worm action. If it is not cautious, this activity will turn out to be a part of usual state for an anomaly detector.

V. TYPES OF INTRUSION DETECTION SYSTEM

A. Host Based IDS

Host based IDS, which is capable of working with high quality data; investigate client's actions & behaviors on a specified machine. Host Based IDS deals with intrusion detection, which takes place on a single server system. The information is gathered from a single server system. The Host Based IDS representative monitors actions for example reliability of the system, application, activity, document changes, server based network congestion, as well as system records. By means of using the regular hashing tools, file timestamps, system records, as well as monitors the system calls and the local network connections give the representative coming to the status of the local server. If here in some prohibited modification or action is spotted, it alerts the client through a notification message, which notifies the central management server, restricts the activity, or else a mixture of the mentioned three. The conclusion must depend on the guideline, which is established on the local system. These types of host-based IDS process are examined as passivecomponent [13].

i) System Commands

Host based IDS employs useful source of information such as system commands for detecting malicious users. With the help of analyzing user's system command, which is possible, to build their user profiles, which describes the user's characteristics and common behavior? Logged system controls examples within ps are UNIX, pstat, vmstat, get limit. The information given by these controls are about different events is extremely accurate as well as useful. The preprocessing of review information that is gathered as informal data, which is needed before analysis.

ii) System Accounting

Operating systems such as both 'Windows' and 'UNIX' have the availability of system accounting. There are no possible numbers of intrusion detection methods in spite of increasing attention for system accounting in windows circumstances. The common use of system accounting UNIX environment is used to gather information on system actions, which comprises of utilization of mutual assets by user of the system [13]. The invention of data from system accounting is able to serve like a precious as well as stable cause of information for IDS.

B. Network Intrusion Detection Systems

Network Intrusion Detection System checks whether there is any intruders in the incoming and outgoing network traffic. NIDS are placed in the network hubs and taps [14]. NIDS check for a doubtful pattern of package to determine as an intruder. NIDS scans the incoming and the outgoing traffic to avoid the internal intruder. One of the disadvantages of NIDS is that it slows down the network speed.

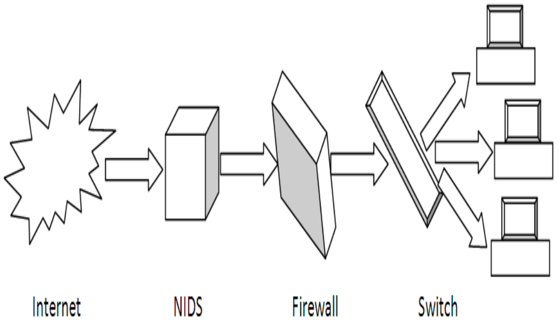

Figure 2: Network Based IDS [15]

The figure 2 illustrates that Network intrusion is been monitored by Network Intrusion Detection System (NIDS) are located at the key network points like routers and switches. All the traffic exceeds through the NIDS. It observes the network traffic and checks the packets whether it holds any malicious data.

C.Distributed Intrusion Detection Systems

Distributed Intrusion Detection System consists of numerous IDS with a huge network, which interacts with each other, or a single server that provides with the advanced network monitoring. DIDS contains Network Intrusion Detection System and Host based Intrusion Detection System. DIDS is a unique mechanism where the intruders are being deducted across the subnet and several host. The server takes the authority and makes it vulnerable to the attacks. DIDS collect audit information and identify attacks from multiple hosts and maybe the network that connects the hosts [16].

VI. WIRELESS NETWORKS

A Wireless LAN is an easy data communication system applied as an expansion to or as an option for, a wired LAN. Wireless set of connected systems have turn out to be famous in recent times due to simplicity of their mechanism and protection. Wireless networks use high frequency radio waves rather than wires to communicate between network – enabled systems devices. The utility of a wireless set of connection that allows endeavor to let alone the expensive method of launching of cables into constructions or as a link between various equipment places. Physical layer in wireless networks is a broadcast medium and it is fewer in security in permanent set of connected computers. For instance, using radio frequencies communication take place "through the air", the threat of interception is high than wired networks. The attacker can study it, if the point is not encrypted, or encrypted with a weak algorithm, so it compromising privacy. The overall security remains the same as with wired networks: preserving secrecy, ensuring integrity, and maintaining accessibility in sequence. They are not given explicit traffic attentive points therefore packets will be supervised in order that every single portable node must run with IDS. Division among standard and anomalous traffic is frequently not cleared in ad-hoc wireless set of connections [17]. For time being, the variation of either compromised or false node is beyond synchronization, which is appropriate to unpredictable physical movement.

VII. ROLE OF NIDS AND TYPES OF ATTACKS

A Network Intrusion Detection System is assigned to supervise set of connected systems on behalf of attacks otherwise intrusions as well as collected information of these intrusions towards the administrator in turn to acquire serious steps. A huge Network Intrusion Detection System server is like an essential network watches the entire congestion; else, minor systems will be able to group up to look after the congestion on behalf of an isolated server, switch, gateway, or a router. We have to check the attacks as well as IDS guides to spot the intrusions. To check every network activity, without a NIDS it results in irreparable harm to an organization’s network Intrusion attack are those in which an attacker pass in to your network to read, break, or take your information.

A. Scanning Attack

Attackers sending a variety of packets for investigating whether a network or system is being exploited. When the investigation packets are reaching the target system, the system responds it and these replies are being examined towards finding the features of the targeted system, and there will be vulnerabilities. Therefore, scanning attack identifies a potential victim. Port, network, vulnerability scanners, etc. are used to yield information [18].

B.Denialof Service Attack

A DOS attack tries to collapse an objective thus to disrupt the service reject the access of genuine as well as certified clients. Thus, these types of attacks are usual in the Web where collections of servers, which are regularly utilized to attack World Wide Web servers with, fake appeal. They will drastically change the financial harm to Electronic Commerce by rejecting the clients approach

C.Flooding DOS Attacks

In flooding DOS attack, an attacker delivers additional appeals to an objective than it can manage. It can also consume the processing ability or consume the network bandwidth leading to a DOS to new users. DOS (Denial of Service) attacks are difficult to conflict these do not use the data and even the most protected system will be spotted. An additional unsafe edition of DOS attack is named DDOS attack, where the large pool of system is being targeted to a specified individually targeted server. Botmaster will be able to begin a DDoS attack via utilizing the vulnerability within any system, and takes command, by creating a DDoS controller [19]. The trespasser utilizes the controller to speak over with additional bots (system). Compromising a large amount of servers, instructed in a single command, the trespasser allows controller to open the flood attack against the particular object.

D.Penetration Attacks

In this attack, the hacker increases an illegal control and modifications of the system, reading the system documents, etc. Commonly, these types of attacks destroy the software, which allows the hacker to establish malware and viruses in the system.

The classification of penetration attacks are

(i) Client to root

A local client acquires the complete admission to all the section of the system.

(ii) Remote to client

A client over the network increases a client account and the linked controls.

(iii) Remote to root

A client over the network increases the total control of the system.

(iv) Remote disk reads

A hacker connected to the network increases admission to the remote document, which accumulates locally on the server.

(v) Remote disk, writes:

A hacker connected to the network neither only gains admission to the remote document which accumulates locally on the server, other than it modifies them.

VIII. HACKING ATTACK DETECTED

Hackers in countries like Europe and China effectively bust into PCs at almost 2,500enterprises and administration groups for the past 72 weeks in a corresponding worldwide attack, which show huge number of individual and commercial private affairs to robbery. The maximum awareness is in Egypt, Mexico, Saudi Arabia, Turkey and the U.S.

IX.BOTNET

A botnet is a set of computers linked in a corresponding method for malicious purposes. Each computer in a botnet is called as bot. These bots design a network of compromised computers, which is managed by a third party and used to dispatch malware or Spam, or to introduce attacks. A botnet can also be known as a zombie army. The largest botnet consists of 12.7 million hosts of more than 190 countries, including systems in businesses, universities, government agencies and in homes. The dead stolen data included 800.000 users' bank account details, user names, credit card numbers, and passwords. Featuring attack data from tipping point intrusion prevention systems, securing 6000 organizations & vulnerability data from 6.000.000 systems compiled by qaualys [20].

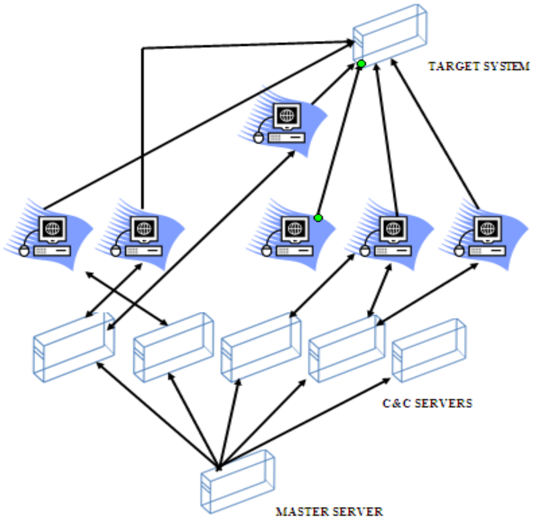

Figure 3: Botnet Intrusion prevention

The Intrusion Detection System method to security is formed on the statement, which a system would not be safe, but that abuse of security plan intrusions will be able to spot by observing and investigating system performance.

X. TAXONOMY OF INTRUSION DETECTION SYSTEMS

The definition of taxonomy is "a classification of organisms into groups based on similarities of structures in characteristics". The Intrusion Detection System looks for actions or set of actions, which are similarly predefined structure of a well-known attack, the analytical approach is known as misuse detection. The identification of intrusion is like an odd activities or a different behavior is typically termed as anomaly detection. Time elements is utilized to sort out the IDS which is keen on on-line IDS which spots intrusions in real time and off-line IDS which frequently stores the monitored information first and then investigate it in group mode for symptoms of intrusion. An IDS investigates the gathered information simply starts from the single monitored system and distributed IDS which gather information from numerous monitored systems which in turn to study worldwide, spread and synchronized attacks.

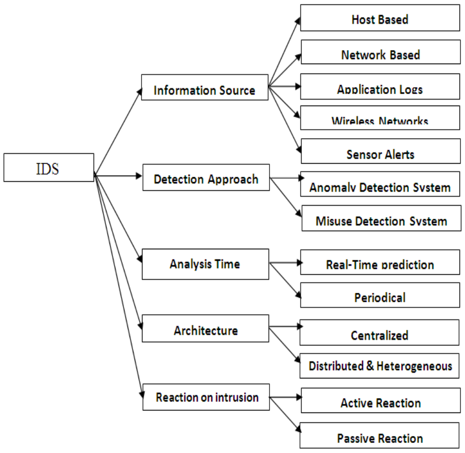

Figure 4: Characteristics classification of IDS attacks

XI. SYSTEM LOG INFORMATION

The information which is not presented at the network stage is available in system log data, such as a user's login while sending an email and file transfer details. The SYSLOG daemon performs conquering as well as gathering system record document information in a clear set-up. A major drawback in using 'SYSTEM LOG' information is not safe, as it exhibits buffer overflow exploitation. Due to the direct utilize of 'SYSTEM LOG' this information is mostly preferred by various network solutions along with applications for example login, send mails, Network File System(nfs) and Hyper Text Protocol(http). It is also employed by security linked tools sudo, klaxon, or TCP wrappers [12], which identifies tools which might show extremely precise issues.

XII. ALERTS FROM IDS

As a result of raise in a congestion level, recent trading IDS typically lean to make an extremely huge amount of false alarms. These alarms are increased mutually for definite intrusions as well as normal behavior, hence rising false alarm rate as well as irresistible security administrator. Additionally, a huge DDOS or else scanning attack may cause several alarms while numerous network links are concerned. Additionally, it raises the amount of alarms that security analysts must study [20]. In turn to reduce amount of approach for spotting intrusions is increased, which can decrease the final detection rate.

XIII. REAL TIME ANALYZER

Preliminary caution against security destruction intrusion with acquaintance based has turn out to be essential for systems, in the current scenario. Smartness and Activeness of the system be necessary in classifying and distinguishing of packet data, the curiosity and mischievousness are spotted, an alert is generated and action reply is implemented. This instrument is initiated to finish or else let procedure packet information linked by the action. By applying behavioral analysis techniques and examining various data records and prevention, demeanor recognition intrusion prevention system the attack is prevented before entering the network for obtaining preemptive protection against Zero-day attacks and malware. On the opposing, with respect from the efforts they instant a latest method for the arrangement to spot threats. Unluckily, running in the off-line system, gathering information in actual conquering except teaching along with recognizing warning is off-line. Identification and recognition investigation of packets in real-time congestion is very difficult to identify by all detection in IPS, this is one of the problems faced by IPS to.

(i) Host Based Approach

Host-based Approach are recently famous technologies which checks in favor of doubtful action starting from the host or OS level, for observing position, utilizing the representative module, which uses earlier than the host attains end of an attack. The alarm is generated as well as it offers intrusive.

(ii) Network Based Approach

This recognizes all packets that are inbound to and outbound of the set of connected systems. The mixture of 'network-based approach' and 'security modules' offers an energetic and a complete network security. Its right to use congestion will be complex than understanding it, as network architecture are constructed regularly on the bases of performance which are not visible. They are discovering to be anxious about how to find the apt path to the destination packet when transporting the packets, which are more vital than examining it. Whereas in the real set of connected systems there are issues in handling the routing of the data [21]. 'PCI interface Ethernet' has restricted performance, due to 'network scalability' and end user of the host. The beginning outcome of 'Gigabyte Ethernet card' with 33MHz secondary 'Component Interconnect' opening is a least required for its performance has turn out to be essential. Therefore, a few people generate their personal item based on 'Gigabyte Ethernet'.

XIV.NETWORK MANAGEMENT

Mostly the 'safety supervision' and 'administration', network section is provided by the theoretical break involving 'intrusion prevention' and 'segment administration'. Normally this integration collects all safety mechanisms, which supervises with single 'network management'. As of business point, there must be an ensure provided by the enterprise revealing that service level agreement provides proper treatment to business – critical application [21]. The most essential purpose of network management is the set of performance operation and network devices.

CONCLUSION

In this paper an overview of the types of IDS, lifecycle, variousdomains, types of attacks and tool has been discussed. During the last decade, drastic improvement has taken place in internet. Today internet is used in all lifestyles, safe data transmission is still a big challenge in data communication. Even though many researchers have suggested new techniques for secured data transmission, the intruders are able to break the system with ease. Therefore, a secured and efficient tool will be a big boon for data communication in today's world.

REFERENCES

[1] R. Bace and P. Mell, "Special Publication on Intrusion DetectionSystems,"Tech.Report SP 800-31, National Institute of Standards and Technology, Gaithersburg, Md., Nov **201**.

[2] David W. Cooke, Rapporteur, "The Resilience of the Electric Power Delivery System in Response to Terrorism and Natural Disasters" Summary of a workshop in National Research council. ISBN: **978-0-309-29395-2**,Page No (**1-42**).

[3] Defeng Wang, Yeung, D.S., and Tsang, E.C., "Weighted Mahalanobis Distance Kernels for Support Vector Machines", IEEE Transactions on Neural Networks, Volume-**18**, No-**5**, Page No (**1453-1462**), Sep **207**.

[4] Inella, Paul. "The Evolution of Intrusion DetectionSystems."[Online]Availablehttp://www.securityfocus.com/infocus/1514, Nov **16**, **201**.

[5] KoralIlgun, Richard A. Kemmerer, Fellow, IEEE, and Phillip A. Porras, "A State Transition Analysis: A Rule - Based Intrusion Detection Approach", IEEE Transactions on Software Engineering,Volume-**21**, No-**3**, Page No (**181 – 199**)**,** Mar **195.**

[6] L Ertoz, E. Eilertson, A. Lazarevic, P. Tan, J. Srivastava, V. Kumar and P. Dokas, "The MINDS - Minnesota Intrusion Detection System, in Data Mining", A. Joshi H. Kargupta, K. Sivakumar, Y. Yesha, "Next Generation Challenges and Future Directions", Ed., **204.**

[7] Intrusion.com, Intrusion Secure Host, white paper available at: www.intrusion.com/products/hids.asp, **203.**

[8] W. Jansen, P. Mell," Mobile Agents in Intrusion Detection and Response", In Proceedings of the 12th Annual Canadian Information Technology Security Symposium, Ottawa, Canada, Page No(**77-91**),Sep**210**.

[9] C. Kruegel, T. Toth," Distributed Pattern Detection for Intrusion Detection", In Proceedings of the Network and Distributed System Security Symposium Conference, Internet Society, Los Angeles, CA, Feb**202**.

[10] E. Eskin, A. Arnold, M. Prerau, L. Portnoy and S. Stolfo,"A Geometric Framework for Unsupervised Anomaly Detection: Detecting Intrusions in Unlabeled Data, in

Applications of Data Mining in Computer Security",**202**, S. Jajodia D. Barbara, "Advances In Information Security", Ed. Boston: Kluwer Academic Publishers, **212.**

[11] M. Esmaili, R. Safavi-Naini, B. Balachandran and Pieprzyk, J. "A Case Based Reasoning for Intrusion DetectionSystem",In Proceedings of the 12th Annual Computer Security Applications Conference, ISSN: **1063-9527**,Page No (**214 -223)**,Dec **196**.

[12] German Florez-Larrahondo, Zhen Liu, Yoginder S. Dandass, Susan M. Bridges, and Rayford Vaughn, "Integrating Intelligent Anomaly Detection Agents into Distributed Monitoring Systems", Dynamic Publishers, Inc.Journal of Information Assurance and Security.Volume-**1**, No-**1**, ISSN:**1554-1010,** Page No (**59–77)**,**206.**

[13] C. Krugel, T. Toth," A Survey on Intrusion Detection Systems", Technica lUniversity of Vienna Technical, report, Page No(**410-417**), Apr**210**, citeseerx.ist.psu.edu/viewdoc/summary?.

[14] "Network Intrusion Detection System", http://en.wikipedia.org/wiki/Network_intrusion_detection_system,Jul**1,209**.

[15] The concept of Intrusion Detection Systems", http://maltainfosec.org/archives/26.html,http://rsmus.com/what-we-do/services/risk-advisory/the-ultra-secure-network-architecture.html, **211.**

[16] N. Einwechter, "An introduction todistribut edintrusion detection systems",http://www.securityfocus.com/infocus/1532, **202**.

[17] Y. Zhang and W. Lee, "Intrusion detection in wireless adhoc networks", In Mobile Computing and Networking, MOBICOM , Boston, MA, USA, Page No(**275–283**), **200**.

[18] Ghosh and A. Schwartzbard,"A Study in Using Neural Networks for Anomaly and Misuse Detection", In Proceedings of the Eighth USENIX Security Symposium, Washington, D.C., Page No(**141-152)**, Aug **199**.

[19] Amrita Anand, Brajesh Patel," An Overview on Intrusion Detection System and Types of Attacks It Can Detect Considering Different Protocols", International Journal Of Advanced Research in Computer Science and Software Engineering, Volume-**02,**No-**08**,ISSN: **2277 128X**, Page No (**94-98**), Aug**212**.

[20] G. Helmer, J.S.K Wong, V. Honavar and L. Miller, "Intelligent Agents for Intrusion Detection", In Proceedings of the IEEE Information Technology Conference, Syracuse, NY, Page No (**121-124**), Sep **207**.

[21] DerisStiawan, Ala' Yaseen Ibrahim Shakhatreh, Mohd.Yazid Idris, Kamarulnizam Abu Bakar, Abdul Hanan Abdullah," Intrusion Prevention System: A Survey", Journal of Theoretical and Applied Information Technology, Volume-**40**, No-**1**,ISSN: **1992-8645**,Page No (**44-54)**,June**15**,**212**.

AUTHORS PROFILE

Mr.R.Karthikhas received his BCAand MCA degrees in the year 2006 and 2009 respectively from Bharathiar University, Coimbatore, Tamil Nadu, India. Before coming to the teachingprofession, hehas worked inreputedsoftware organization, Allsec Technologies, Chennai, Tamil Nadu, India. He is presently working as an ant Professor in the Dept.of Information Technology in Kongunadu Arts and Science College, Coimbatore, TamilNadu, India. He is currently working towards his PhD degree in the Area of Networks. He has published several papers in International and National level journals and conferences.

Dr.B.L.Shivakumarholds a Ph.D. in Computer Science from Bharathiar University, Coimbatore. He has more than 19 years of academic experience in various positions in reputed colleges. He has 12 years of research experience and has 47 research publications to his credit in reputed journals and conferences. He has successfully guided four research Scholars from leading Universities and presently 6 students are pursuing PhD, under his guidance. He has written 38 articles related to Computer in Tamil daily "Dina Thanthi" in Computer Jallam. He is recipient of Bharat Jyoti award conferred by The India International Friendship Society, New Delhi and NSS Best Programme Officer award by Bharathiar University. His interest includes Computer Forensic Science, Network Security and Cloud computing. He is a member in a number of Academic Bodies and Professional Societies.