International Journal of Informatics and Computation (IJICOM)
Vol. 1, No.1, August 2019
ISSN: 2685-8711, E-ISSN: 2714-5263 DOI: 10.35842/ijicom

A Survey of Intrusion Detection System

Putra Wanda[1], Huang J. Jie[2]

Abstract

Nowadays, the evolution of internet and use of computer systems has resulted in huge electronic transformation of data which experienced multiple problems such security, privacy and confidentiality of information. A significant progress has been made in term of improving computer systems security. However, security, privacy and confidentiality of electronic systems are potentially major problems in computer systems. In this paper, we presented a survey on intrusion detection systems (IDS) in several areas. It consist of Web Application, Cloud Environment, Internet of Things (IoT), Mobile Ad-Hoc Network (MANET), Wireless Sensor Network (WSN) and Voice over Internet Protocol (VOIP).

Keywords

Survey, IDS, Network Security.

1. Introduction

Currently, the evolution of internet and use of computer systems has resulted in huge electronic transformation of data which experienced multiple problems such security, privacy and confidentiality of information. A significant progress has been made in term of improving computer systems security. However, security, privacy and confidentiality of electronic systems are potentially major problems in computer systems. In fact, no system currently available in the world is 100% secure. A computer network is a set of computers connected together for the purpose of sharing resources. A network attack can be perpetrated by an insider or by an outsider. In the “inside attack", the attack is initiated by an entity inside the security perimeter, the person who has complete authorization involves in the vulnerable activities, that is, the attacker tries to access some system resources for which he is not having the authorization. It is very tough to find out this type of persons [1].

Hardware threats are easy to detect and also it causes harm only to the device rather than the data. The Hardware threats are of four types: Physical, Electrical, Environmental and Maintenance. If the attack is in software, mainly it harms the data. Previously, only the persons with high programming skills were involved in writing of hacking programs. But now, a person who has a little knowledge of programming may become a hacker just by downloading hacking tools from the internet. Attack scenarios. Basically, if a new signature is found on the database of signatures, then the behavior will be Vulnerabilities in most computer systems. And, it can be exploited by either non authorized or authorized users. Having said that, several tools are being designed and implemented for a variety of exploitations in diverse range of security attacks. Among these tools is the intrusion detection systems (IDS) which allow us to monitor a range of computer systems: an information system, a network or a cloud computing. These IDS detect intrusions and

[1] **Corresponding Author:** Putra Wanda, Universitas Respati Yogyakarta, Indonesia (wpwawan@gmail.com)
1 Putra Wanda, Universitas Respati Yogyakarta, Indonesia (wpwawan@gmail.com)
2 Huang J,Jie, Harbin University of Science & Technology, China (jjie.huang@hrbust.edu.cn).

defined as attempts to break the security objectives such as confidentiality, integrity and availability and nonrepudiation. considered as an attack [1, 2].

An attack may be an active or passive attack. In “Active attack”, the attacker will undergo some actions which may alter the system resources like breaking or bypassing the secured systems. Mostly it results in revealing sensitive information, modification of data or the maximum, loss of data completely. Trojan horses, viruses, worms, inserting malicious code, penetrating network data, stealing login information are some of the examples for the active attack. This type of attack is very harmful to the system. The types of active attacks are: Masquerade, Session Replay, Modification of message and Denial of service [3].

Intrusion Detection can be defined as "the act of detecting actions that attempt to compromise the confidentiality, integrity or availability of a resource”. An IDS is a device or software application that monitors a network or systems for malicious activity or policy violation. Any detected activity or violation is reported either to an administrator or it will be collected centrally using a Security Information and Event Management (SIEM) system [3].

This SIEM combines all the outputs from multiple sources, and uses alarm filtering techniques to distinguish malicious activity from false alarms. Though the Firewalls and IDS both relate to network security, an IDS differs from a firewall in that a firewall looks outwardly for intrusions in order to stop them from happening. Firewall limits access between networks to prevent intrusion. IDS can be classified based on where detection takes place (network or host) and the detection method that is employed [4][5].

2. Type of IDS

2.1 Anomaly Recognition

Recognition method is to deliver a profile for every gathering of the clients in framework. These profiles can be produced consequently or physically both. Gradual instructions to make these profiles are not essential if these profiles are displaying the elements precisely for every gathering of the client over the system. These sorts of profiles are used as the benchmark to show ordinary client's activity. In an event that any action of the system may contrast from this given gauge, then the movement deliver a caution [6, 7].

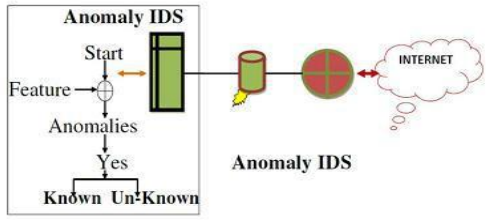

Fig. 1 Anomaly Recognition

The inconsistency recognition frameworks may give few benefits. Towards the starting, anomaly IDS can recognize insider-assaults or record burglary effortlessly. On the off chance that, genuine client or any other person is expending the stolen-account, begins doing the activities that are outer to the ordinary profile of the client, it then delivers a caution. After that, since framework depends on redid profiles, along these lines it is troublesome for assailant to acknowledge with affirmation, what activity can be stolen out without setting- away caution. Evidently significant advantage of meddling activity is not in view of particular kind of movement that displays the notable meddling activity as inside the mark subordinate IDS [6, 7].

2.2 Misuse Recognition

Another real classification of IDS-activating is alluding as misuse recognition. The misuse recognition in Fig 2 is likewise alluded as the mark based-identification consider figure to be alerts are delivered in view of certain assault marks [8, 9].

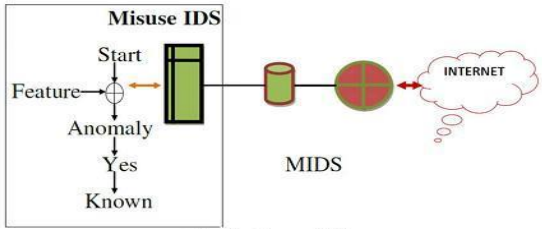

Fig. 2 Misuse Recognition

These assault marks comprise of particular activity or movement that depends on known meddling activity. The misuse discovery permits many advantages. One of them is the mark definitions which are created on known meddling activity. Furthermore, the client can manage the mark database, and investigate that misuse recognition framework is customized for meddling action [8]. Last legitimacy is that the framework is effectively learned. On the off chance the client can relate specifically to certain sort of activity over the system [9].

2.3 Location Based IDS

A. **Host Based IDS**

Host-based IDS shows the checking of framework which looks for data at nearby host or the working framework. This might be accomplished by a confounded framework which decides the correct framework call or it might be straightforward, for example, essentially inspecting framework log documents [10, 11]. Few of these methodologies may precisely hold the assaults before they may succeed, while the others just provide details regarding what has happened already. The main advantage of the host-based observing framework is the accomplishment of assault which can be analyzed. The system subordinate framework can create caution on the nearness of any prominent action; however they can't generally affirm the achievement or disappointment of these assaults [10, 11].

B. **Network Based IDS**

Set up of looking for unobtrusive movement at host-level, the system based-monitoring systems decide the correct bundles of nodes which are going around the system. The framework decides this movement for the known images of the informative action. Since these frameworks are watching node movement, any assault marks identified may succeed or come up short. A system based observing framework has preferred standpoint of organizing and seeing the assaults which are establishing around the entire system effortlessly. Seeing assaults against the whole arrangement, gives a perfect sign of range to which the system get attacked [11].

3. Literature Survey

A paper stated that when the Intrusion Detection System protects the network from the network attack, it produces a huge number of false, redundant or unimportant alerts. It is a major drawback of it. The results showed that the system could reduce the number of alerts by 94.32% [12]. A technique is suggested to find out whether a webpage is malicious or benign. First the static content of webpages using a self-developed JAVA program is taken to process the signatures with regular expressions to accelerate the analyzing process, then a honeypot system to browse web pages and finally it is concluded with the type of webpage [13].

Another study confirmed that Advanced Persistent Threat (APT) uses different attack methods to access the unauthorized system in initial stage and then slowly spread throughout the network. This proposed approach is designed to extend any" packet-level" IDS systems to improve their results. The model is built with Search-Patterns (P), Event Classes(C), Hypothesis(H) and Rules(R) [14]. A paper suggested that Web Anomaly Misuse Intrusion Detection (WAMID) framework which works with the combination of misuse and anomaly detection algorithms to detect SQL injection attack. First, in training phase, a profile is created for legitimate database behavior extracted from applying association rules on XML file containing SQL queries submitted from application to the database [15].

Botnet is a collection of hosts(bots) and it is controlled by a bot master through a command and control (C&C) channel. So, this detection mechanism detects the attack during C&C stage, that is in advance to the botnet attack. The IRC traffic patterns in an organization network was considered for the testing. The similarity measurement and the periodic characteristics were noted down. This system can find out the malicious network traffic by normal IRC clients [16].

Another article adopted a technique for SQL injection attack which is a stealing of sensitive information from the back-end database, such as credit card numbers. They proposed an IDS-SQLiDDS(SQL Injection Detection using Query Transformation and Document Similarity) to detect various types of SQL Injection attacks. Only the portion of queries after the WHERE keyword were considered. For the testing, five honeypot web applications were developed using PHP and MySQL [17].

Honeypot is nothing but a fake server that provides emulated services similar to the real services running on the actual server. So, whenever attacker tries to attack actual server, attacker is redirected to this fake server and eventually gets trapped. Honeypot then gives the valuable information regarding the intruders. This paper suggested a new honeypot system. IDS service with two components namely Analyzer and Alert System [18]. If the users make use of any web application, all the activities of the users are automatically appended into the web log files. This system basically concentrated on these log entries and suggested a preventive technique to protect them from. the most common attacks namely denial of service and brute force attacks. And it provides a secure platform for sharing of files. This system is capable of distinguishing the malicious and the non-malicious users [19].

Another attack is Cross-Site Scripting attack (XSS) is a code injection attack performed to exploit the vulnerabilities existing in the web application by injecting html tag / java script functions. They presented different types of XSS attacks. This system works in two steps: First is to trace out the cross-site scripting vulnerabilities in the web application. A website in PHP is newly created, hosted on the local host (XAMPP server) and the experiments have been performed on modern browsers (Google Chrome49, IE11, Opera15 and Firefox44.0.2) to exploit XSS vulnerabilities [20].

Another study suggested a new approach to form an IDS with various IDSs to detect network attacks by processing data from core network components using the properties of OpenFlow in an SDN environment. OpenFlow is capable of raising an event or update a flow counter at arrival time of a packet depending on a match or mismatch with respect to an existing or non-existing flow. If multiple Intrusion Detection System (IDSs) exist, traffic redirection is mainly based on subnets or IP addresses [21].

3.1 **Intrusion Detection for Web Application**

Web servers are considered as an important test environment for intrusion detection. The reason being is that because of their importance and universality of the HTTP protocol [8] and the number of striking vulnerabilities. While researchers are still exploring the signature and behavior of intrusion detection approaches, there are a lot of companies who develop commercial tools to protect web application using different techniques as well. For this reason, we will present different and specific web IDS based on their detection approach.

A. Signature Approaches

The majority of signatures specific web IDS are host IDS (HIDS) in the application level. McHugh and Proctor adopt the principle of this approach, which is based on the use of learning techniques of known attacks and define their signatures. Once the signatures are defined [22] [23]. A regular expression or pattern matching are used to recognize attacks in query waves. It should be noted also that the work by Vigna et al. [24] was within the scope of the intrusion detection scenarios and led to the development of an IDS called Web STAT. In the framework of STAT the attacks are initially modeled in a high level language, and then automatically compiled to be used as the signature of the intrusion detection [12].

B. Behavioral approaches

This approach does not use any internal information of the program. The reference model of behavior in these approaches can be defined by the application specifications or by conclusion of learning from the execution of the application. The approach proposed processing the successive system calls of processes while running on external information in the program. The experiment result showed that short system call sequences generate a stable signature to model the normal behavior of a process according to its environment [25] [26].

Network intrusion detection systems: Network Intrusion Detection systems (NIDS) are placed at a tactical point or points within the network to monitor the traffic on the network. It accomplishes an analysis of passing traffic on the entire subnet and matches the traffic which is passed on the subnets to the collection of known attacks. If an attack is caught or any abnormal behavior is sensed, the alert can be sent to the administrator. Similarly, a gray box approach is based on the sequences of system calls as well. It extracts additional information from the process while using the memory. Gao et al experiment show that the presence of an attack is often happened during the arguments of system calls [27].

3.2 Intrusion Detection System in Cloud Environment

In this section, we will present different CIDS and classify them into three categories based on the intrusion detection technique used by each system. The categories are Signature based, Anomaly based and Hybrid. We have studied systems from each

category and analyzed them to evaluate whether or not they meet the security requirements of cloud.

A. Signature Based Detection

A paper integrated a signature Apriorism based NIDS to Cloud. Signature Apriori takes network packets and known attack signatures as input and generates new derived rules that are updated in the Snort. Therefore, Snort is able to detect known attacks and derivative of known attacks in the Cloud. This approach improves the efficiency of Snort. However, it cannot detect unknown attacks [28].

Another article proposed an Intrusion Detection System as a Service (IDSaaS), which enables consumers to protect their virtual machines against internal and external attacks in public clouds. IDSaaS is a network and signature-based IDS, and it targets the Infrastructure-as-a-Service level of the cloud. It is OnDemand, elastic, portable, controllable by the cloud consumer and available through the pay-per-use cost model of the cloud [29].

Another article presented a framework based on secure mobile agents (Bee-Gent Mobile agent) for detecting distributed intrusions and repairing the vulnerabilities in hybrid cloud. The operating of this framework is divided into three successive phases: those are Detect distributed attacks, Evaluate the attacks risks, and Repair attacks [29]. A virtual host based intrusion detection system was placed between router and Cloud host. The developed IDS consists of three components namely: Event Auditor, IDS service (combination of analyze system and Alert system) and CIDD (Cloud Intrusion Detection Data Sets). The analyzer system examines the content of packet against the cloud intrusion datasets signatures stored in CIDD by means of pattern matching [30].

Another paper build an architecture which provides implementation of Sericata IDS as network IDS in the backend of Cloud environment. The aim of Sericata IDS is to secure the virtualized servers on hypervisors in the cloud platform from attackers and various threats. The main function of Sericata IDS in the network is capturing of all coming packets from external users and destined to virtualized servers, analyzing these packets and finally sending alert if a packet is matching one of rules stored into Sericata configuration file [31][32].

B. Anomaly Based Detection

A study proposed an approach to detect malicious program executions at client VM's in Cloud environment, with the use of a new technique of Immediate System Call signature detection. In this approach, for every unique System Call (user program or system program), the list of all Immediate System Calls following it is identified, and created from its normal execution logs, and such signatures are stored and then used as baseline for anomalous program detection [33]. Anomaly detection system at the hypervisor layer named Hypervisor Detector is proposed as solution. It uses a hybrid algorithm which is a mixture of Fuzzy C-Means clustering algorithm and Artificial Neural Network (FCM-ANN) to improve the accuracy of intrusion detection system FCMANN approach has the following three phases. In the first phase, a fuzzy clustering technique is used to divide the large dataset into small clusters or training subsets [34].

Another paper presented an Intelligent Intrusion Detection System for Private Cloud Environment to satisfy the security and the performance issues of cloud computing. The proposed IDS combine combining hardware and an application to detect intrusion. The software component is implemented within virtualized servers such web server to detect intrusions, without influencing the performance of the servers. The hardware component is used to store intrusions traces and parameters of the IDS [35] or using a Signature based

Semantic Intrusion Detection System on Cloud, which concentrates on the application level to detect application specific attacks [36].

Another study proposed an anomaly intrusion detection model to deal with attacks and security violations in cloud environment. The proposed approach consists of Hopefield Artificial Network and Simulating Annealing as aggregator. The framework for anomaly IDS is divided into three stages: Dataset Grouping, Hopfield Artificial Neural Network (HANN) and Simulating Annealing aggregator [37].

C. Hybrid Based Detection

A hybrid-network intrusion detection system (H-NIDS) deployed on each host machine, to detect internal and external network attacks in Cloud Computing environment. The architecture of proposed H-NIDS consists of mainly seven successive modules; Packet capture, Signature based detection, Anomaly detection, Score function, Alert system and Central log. Signature based detection module uses Snort and signature Apriorism algorithm, which generates derived attack rules, thereby, Snorts can detect known attacks and derivative attacks [38].

Another study established an Intrusion Detection System for protecting the Cloud environment against intrusions, based on the collaboration of multithreaded Network Intrusion Detection System (NIDS) and Host Intrusion Detection System (HIDS). The multithreaded NDIS is placed at the bottleneck position of the Cloud, to monitor the requests send by the Cloud users [39]. An article developed an Intelligent Intrusion Detection System (I-IDS) to improve the security of virtual machine (VM), which is the base for cloud computing model. The proposed model works at virtualization layer, it improves security of VM by creating VM profiling, packet flow monitoring and conducting centralized periodic automated vulnerability scans for infected VMs [40].

A novel Collaborative IDS (CIDS) framework is proposed for cloud, to defend network accessible Cloud resources and services from various threats and attacks. The proposed NIDS is integrated in each cloud cluster, and a correlation Unit (CU) provides collaboration between all cluster NIDSs, is placed in any one cluster. Bully election algorithm is used to elect one best cluster for placement of CU on the basis of workload. The hybrid NIDS use Snort to detect the known stealthy attacks using signature matching, and to detect unknown attacks, anomaly detection system (ADS) is built using Decision Tree Classifier and Support Vector Machine (SVM) [41].

3.3 Intrusion Detection in Internet of Things

A. IDS with Higher Interaction Ability Values

Tim Bass suggested a holistic cross-platform approach for detecting unauthorized access in the whole cyberspace should involve evaluating inferences from multi-perspectives. A deployment metric of an IDS, was used to rank the level of the holistic detection intelligence of the reviewed IDSs. It provides a multi-perspective view of the IDSs interaction with the following TCP/IP suite's four network service layers: Network Interface, Internet, Transport, and Application layers [42]. Moreover, the TCP/IP layers can be mapped to functionally similar ZigBee WSN standards and as an encapsulation or otherwise in 6LoWPAN [43].

At the beginning of 2011, the ideology of IDSs began to change as the research began to not target individual or related components, but the whole IoT. In one of these experiments, Liu et al., applied the mechanisms of artificial immune systems to IDSs3 in the IoT [44].

More recently, there has been a proposal for Computational Intelligence (CI) based systems which are adaptable and react to new situations by applying reasoning without relying on users. Examples are artificial neural networks, evolutionary computation, artificial immune systems, swarm intelligence, and fuzzy logic. Using a three tier architecture for monitoring, applying computational intelligence, and reporting intrusions, the IDS tracks the IP addresses of the source messages and stores it against their network or system patterns [45].

Another approach addressed the issue of integrating non IP networks by assigning unique identifiers to every object [46]. The ID-based communication in heterogeneous networks named the Identity Sublayer was embedded in the transmission layer for better real-time performance than traditional IDS. Another study developed a Complex Event Processing (CEP) engine for real-time pattern detection amongst the different components in the IoT. It was benchmarked against an IDS that first stores, and then matches the data with a rule. They found that their approach was more CPU intensive, but consumed less memory. Effectively it proved better real-time performance [47].

B. IDS with Lower Interaction Ability Values

The Internet (Network) layer is an ideal place for a holistic approach to a rule-based detection engine because the lower layers depend on the hardware, and are less abstracted. The following is a review of two different IDSs operating at the network layer. The first work utilizes the traditional TCP/IP suite. A paper proposed a type of service orientated architecture embedded in the TCP/IP Internet layer to enable object communication irrespective of their hardware or software platforms. An important technique utilized involved registration of services and objects in order to search and deliver the information related to them. It avoided overload by using hierarchical designated routers to filter only necessary information to the parent node [49].

Another promising DoS detection framework for IoT intrusion detection and security integrated was an open-source IDS named Suricata modified for a IPv6 over low power personal area network (6LoWPAN). It was to modify the originally open-source code to integrate an advanced event monitoring system [50].

3.4 Intrusion Detection in Wireless Sensor Networks (WSN)

In a network, intruder type is grouped into two categories. These categories are internal intruder (selfish or malicious node) and external intruder (An outside attacker trying to reach the system) [51].

A. Anomaly Detection Approaches in WSN

Anomalies of WSN can be grouped as Network Anomalies, Node Anomalies, Data Anomalies and Other Anomalies. Additional to types of WSN anomalies, approaches detecting WSN anomalies is important too. These approaches are used to implement an IDS in WSN as a detecting solution and they can be combined with each other. These approaches can be sorted as statistical based, artificial immune system based, machine learning based, data mining based and game theory based [52].

In A Game-Theoretic Framework for Robust Optimal Intrusion Detection in Wireless Sensor Networks, it is claimed that instead of approaches using heuristic and ad-hoc solutions, there is an increase to use analytical approaches for security issues in WSN. Hence authors propose a non-zero sum discounted robust stochastic game framework to

analyze intrusion detection problem in WSN. Game' s parameters are modelled by features of WSN and environment [53]

Another approach has been proposed an anomaly detection solution specifically designed for the ultrawideband (UWB) technology. In the paper, it is described that UWB is a key solution to serve low power consumption while wireless connectivity. To identify intrusions, a rule-based approach is accepted and performance of the proposed algorithm is studied by simulations. The algorithm proposed a round-based approach towards cluster structure and rule-based anomaly detection. The test results shown in paper point out a successful detection accuracy [54].

Another study proposed that the application using data mining approaches for intrusion detection system in wireless sensor network and proposed system can perform both anomaly detection technique and misuse detection technique. The IDS consists of a Central Agent and several Local Agents, which are placed on the sensors and carry out intrusion detection activities. Data mining approach is used on each agent (Local Agents, Central Agents). The test results show that high detection accuracy is obtained while keeping an acceptable, but not negligible false positives rate [55].

B. Misuse Detection Approaches in WSN

Misuse Detection Approaches is also known as signature-based IDS and is successful to detect known attacks. It's drawback is that it cannot detect new unknown attacks or attacks having not predefined rules. Using misuse detection technique is a complex task for WSN because of constraints of WSN. For instance, keeping signatures of attacks is very difficult and is less effective. In the literature it is seen that a few studies use misuse detection technique and they propose watchdog approach and mobile agent approach [56].

In Intrusion Detection in Wireless Sensor Networks Using Watchdog Based Clonal Selection Algorithm - 2013, the watchdog approach is used to detect whether a node has abnormal behavior while forwarding data. All nodes in the WSN are responsible for monitoring the neighbors and transferring the information about behavior. Misbehavior of nodes affect performance of WSN negatively. With using watchdog based clonal selection algorithm it is aimed that detect malicious and selfish nodes of WSN [57].

C. Hybrid Detection Approaches in WSN

Some specification-based solutions have been proposed and the main drawback of this solution is that the development of protocol specifications is created by human. Security protocols of WSN is defined by administrator manually. Author describes this approach with three techniques and hybrid detection is involved in this classification as third subtitle [56]. Another approach is aimed that combining anomaly detection based and misuse (signature) based approaches in order to achieve a more accurate intrusion detection system. The anomaly detection uses a distributed learning algorithm for the training of a SVM to solve the two- class problem (distinguish between normal and anomalous activities). The goal of this study is described as to save the energy [58]

3.5 Intrusion Detection in Mobile Ad-Hoc Networks (MANET)

A study developed a secure routing approach called Resiliency Oriented Secure (ROS) which include the detection phase in routing to detect the malicious node. To detect the malicious node, they employed a number of updates field in the routing table and set some threshold value for it. Whenever any node receives a routing packet that has an update in its routing table, it increments the number of update field by one. When the count values cross the threshold values it triggers alarm signal [59].

Another paper proposed a model which does not perform any change in underlying protocol and used additional security component to detect fabrication attack, resource consumption attack and packet dropping attack [20]. Using an extended architecture, IDSX is a cluster- based solution and it acts as a second line of defense. Any IDS solution could be implemented by individual nodes. The solution IDSX is compatible with any IDS solution acting as the first line of defense. The IDSX hardly produced any false positives according to the simulation results. This is because it forms a consensus of the responses from different individual IDS solutions implemented in the nodes. Anomaly-based intrusion detection schemes could be implemented as the first line of defense. The IDSX works within preset boundaries [60].

Another solution is proposed called eSOM is described using the concept of unsupervised learning in Artificial Neural Networks using Self-Organizing Maps. The technique used a data structure called U-matrix which is used to represent data classes. These regions represent malicious information and are watermarked using the Block-Wise method. The regions representing the benign data class are marked using the Lattice method. When a new attack is initiated, it causes changes in the pixel values [61].

An article proposed two intrusion detection techniques for mobile ad- hoc networks, which use collaborative efforts of nodes in a neighborhood to detect a malicious node in that neighborhood. The first technique is proposed for detection of malicious nodes in a neighborhood of nodes in which each pair of nodes in the neighborhood are within radio range of each other and such a neighborhood of nodes is known as a clique [62]. Another study proposed Intrusion Detection System (G-IDS) that employs the basic principles of the Grid computing and apply them to the intrusion detection mechanisms, in order to define a new process capable to protect networks characterized by the constantly changing of the topology [63]. they used a distributed traffic analyzer that acting in real-time feedback sharing the results between the neighboring nodes of the network [63].

In mobile IDS, a paper proposed a mobile Intrusion Detection System for multi-hop ad-hoc wireless network in their work. The authors define the monitor node which detects misbehaving node. They also presented the algorithm for detecting the packet dropping and packet delaying attack [64]. A leader election model for IDS in MANET based on the Vicky, Clarke and Groves (VCG) model was proposed. The model requires every node to be as honest as possible and leaders are selected in a way which results in optimal resource utilization. For participating honestly in the election process, leaders are positively rewarded. A higher effective lifetime of the nodes was achieved by balancing the resource consumption amongst the nodes [65].

Another approach to the IDS called HIDS has been proposed. This technique is based on reputation or trust or honesty values of the mobile nodes. Depending on its behavior, the trust value of a node is dynamically increased or decreased. If a node behaves normally, it is positively rewarded; malicious activity results in negative rewards for that node. The trust on a node is recalculated based on the rewards that it has earned, and its current honesty rate [66].

Another paper evoked the problem of increasing the effectiveness of an intrusion detection system (IDS) for a cluster of nodes in ad hoc networks. To reduce the performance overhead of the IDS, a leader node is usually elected to perform the intrusion detection service on behalf of the whole cluster. To increase the effectiveness of an IDS in MANET, they introduce a unified framework that is able to Balance the resource consumption among all the nodes and thus increase the overall lifetime of a cluster by electing truthfully and efficiently [67].

Another study presented grammatical evolution approach to intrusion detection on mobile ad hoc networks. They employ artificial intelligence-based learning technique to explore design space. The grammatical evolution technique inspired by natural evolution is used to detect known attacks on MANETs such as DOS attacks and route disruption

attacks. Intrusion detection programs are evolved for each attack and distributed to each node [68].

A hybrid solution described in combines the Watchdog and Pathrater scheme has been proposed by Marti et al. and SCAN [70]. Nevertheless, neither SCAN nor Watchdog and Path-raters address the mobility issue that well. Also, this hybrid solution suffers from the same problems. There are no fixed nodes which can behave as umpires. There must be some kind of a leader election model that runs in every node to select the Umpire nodes [69].

Another approach aims to use one of the danger theory intrusion detection algorithms, namely, the dendritic cell algorithm (DCA) to detect the sleep deprivation attack over MANET. DCA is plugged in a proposed mobile dendritic cell algorithm called MOCA which represented through a designed MDCA architecture. Each node in MANET should protect itself from danger locally without using mobile agents. At the beginning, the algorithm controls each entered packet's ID in the memory. If that packet ID found in the detected list, this indicates it comes from an attacker detected before, the algorithm rejects the packet directly, deletes its information from the routing table and sends an alarm message for the second time for that packet TD [71].

Other researchers elaborated a dynamic hybrid approach based on the artificial bee colony (ABC) and negative selection (NS) algorithms, named BeeID, for intrusion detection in AOOV-based MANETs. The approach designed of three phases: training, detection, and updating. In the training phase, a niching artificial bee colony algorithm, called NicheNABC, runs a negative selection algorithm multiple times to generate a set of mature negative detectors to cover the non-self-space. In the detection phase, mature negative detectors are employed to discriminate between normal and malicious network activities. In the updating phase, the set of mature negative detectors is updated by one of two techniques of partial updating or total updating [72][73].

3.6 Intrusion Detection in Voice Over Internet Protocol (VOIP)

The VolP security issues and solutions are increasingly important for the success of VoIP services, especially in the domain of intrusions and intrusion detections. In targeting an effective, flexible and holistic approach to VolP security management. we propose the use of a suitable mobile agent system in an integrated framework which can be applied specifically to VoIP as well as to modem network management in general. VoIP applications would face security threats inherited from IP networks. A comprehensive survey of Internet intrusions can be Sound in. They classified the Internet infrastmcture attacks into Sour categories: DNS hacking, routing table poisoning, packet mistreatment and DoS, and discusses the impact of these kinds of intrusions on the Internet [74].

Furthermore, the development of the intelligent network using SS7 (Signaling System No.7) provides greater flexibility to the network through the introduction of new services It, however, increases its vulnerability to the misuse of those services because certain services allow users access to management information. Free phone service is an example. Mobile technology also impacts telephone security [75]. VolP relies on various protocols to address different aspects of a "call". IP telephony- related protocols are not initially designed with security as a prime design goal. Although some of these protocols have added security features in their recent versions, security mechanisms are not secure enough or are still impractical. This section discusses the security characteristics of the VolP standards that are currently used in building VolP systems including SIGTRAN [76]. H.323. Session Initiation Protocol (SIP), and Megaco [77].

4. Conclusion

Intrusion Detection can be defined as the act of detecting actions that attempt to compromise the confidentiality, integrity or availability of a resource . An IDS is a device or software application that monitors a network or systems for malicious activity or policy violation. In the Internet, the outside attackers may be amateur pranksters or organized criminals or international terrorists or even hostile governments. A computer network consists of two components namely hardware and software. Both of these components may have their own risks and vulnerabilities. In this paper, we provided various approaches in Intrusion Detection including problem, techniques and application in various industries.

We have surveyed various types of Intrusion Detection Model in different cases. This paper presented intrusion detection systems (IDS) in several areas. It consists of Web Application, Cloud Environment, Internet of Things (IoT), Mobile Ad-Hoc Network (MANET), Wireless Sensor Network (WSN) and Voice over Internet Protocol (VOIP). We have found that IDS is a significant part in security system of the networks.

Acknowledgment

The research was conducted with the Harbin University of Science & Technology support in providing research facilities.

References

[1] H. Debar, M. Dacier, and A. Wespi, "A revised taxonomy for intrusion detection systems," Annales des Télécommunications, vol. 55, pp. 361-378, 2000.

[2] Y. Deswarte, "Chapitre 1: La sécurité des systèmes d'information et de communication," in Sécurité des réseaux et des systèmes répartis, Y. Deswarte and L. Mé, Eds., Traité IC2, Hermès, ISBN 2-7462-0770-2, pp. 15-65, Oct. 2003.

[3] A. Lazarevic, V. Kumar, and J. Srivastava, "Intrusion detection: A survey," in Managing Cyber Threats, Springer US, 2005, pp. 19-78.

[4] M. S. Hoque, M. Mukit, and A. Naser, "An implementation of intrusion detection system using genetic algorithm," Int. J. Netw. Secur. Appl. (IJNSA), vol. 4, no. 2, pp. 109-120, Mar. 2012.

[5] R. K. Deka, K. P. Kalita, D. K. Bhattacharya, and J. K. Kalita, "Network defense: Approaches, methods and techniques," J. Netw. Comput. Appl., vol. 57, pp. 71-84, Nov. 2015.

[6] A. Kartit, A. Saidi, F. Bezzazi, M. El Marraki, and A. Radi, "A new approach to intrusion detection system," J. Theor. Appl. Inf. Technol., vol. 36, no. 2, pp. 284-289, 2012.

[7] P. Garcia-Teodoro, J. Diaz-Verdejo, G. Maciá-Fernández, and E. Vázquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges," Comput. Secur., vol. 28, nos. 1-2, pp. 18-28, 2009.

[8] A. Garg and P. Maheshwari, "A hybrid intrusion detection system: A review," in 2016 10th Int. Conf. Intell. Syst. Control (ISCO), 2016, pp. 1-5.

[9] A. Garg and P. Maheshwari, "Identifying anomalies in network traffic using hybrid Intrusion Detection System," in 2016 3rd Int. Conf. Adv. Comput. Commun. Syst. (ICACCS), 2016, vol. 1, pp. 1-6.

[10] A. Jacobus and A. A. E. Sinsuw, "Network packet data online processing for intrusion detection system," in 2015 1st Int. Conf. Wireless Telecommun. (ICWT), 2015, pp. 1-4.

[11] M. El Ajjouri, S. Benhadou, and H. Medromi, "New collaborative intrusion detection architecture based on multi-agent systems," in 2015 Int. Conf. Wireless Netw. Mobile Commun. (WINCOM), 2015, pp. 1-6.
[12] M. N. Barghi, J. Hosseinkhani, and S. Keikhaee, "An effective web mining-based approach to improve the detection of alerts in intrusion detection systems," Int. J. Adv. Comput. Sci. Inf. Technol. (IJACSIT), vol. 4, no. 1, pp. 38-45, 2015.
[13] T. M. Koo, H. C. Chang, Y. T. Hsu, and H. Y. Lin, "Malicious website detection based on honeypot systems," in 2nd Int. Conf. Adv. Comput. Sci. Eng. (CSE 2013), Jul. 2013.
[14] I. Friedberg, F. Skopik, G. Settanni, and R. Fiedler, "Combating advanced persistent threats: From network event correlation to incident detection," Comput. Secur., vol. 48, pp. 35-57, Feb. 2015.
[15] S. E. Salama, M. I. Marie, L. M. El-Fangary, and Y. K. Helmy, "Web anomaly misuse intrusion detection framework for SQL injection detection," Int. J. Adv. Comput. Sci. Appl. (IJACSA), vol. 3, no. 3, pp. 123-129, Mar. 2012.
[16] C. M. Chen and H. C. Lin, "Detecting botnet by anomalous traffic," J. Inf. Secur. Appl., vol. 21, pp. 42-51, Apr. 2015.
[17] D. Kar, S. Panigrahi, and S. Sundararajan, "SQLiDDS: SQL injection detection using query transformation and document similarity," in Int. Conf. Distrib. Comput. Internet Technol., Springer, 2015, pp. 377-390.
[18] A. A. Somwanshi and S. A. Joshi, "Implementation of honeypots for server security," Int. Res. J. Eng. Technol. (IRJET), vol. 3, no. 3, pp. 285-288, Mar. 2016.
[19] J. Kaur, R. Singh, and P. Kaur, "Prevention of DDoS and brute force attacks on web log files using combination of genetic algorithm and feedforward backpropagation neural network," Int. J. Comput. Appl., vol. 120, no. 23, pp. 10-13, Jun. 2015.
[20] H. Kour and L. S. Sharma, "Tracing out cross-site scripting vulnerabilities in modern scripts," Int. J. Adv. Netw. Appl., vol. 7, no. 5, pp. 2862-2867, Mar. 2016.
[21] S. Seeber and G. D. Rodosek, "Towards an adaptive and effective IDS using OpenFlow," in IFIP Int. Conf. Autonomous Infrastruct., Manage. Secur., Springer, Jun. 2015, pp. 134-139.
[22] J. McHugh, "Testing intrusion detection systems: A critique of the 1998 and 1999 DARPA intrusion detection system evaluations as performed by Lincoln Laboratory," ACM Trans. Inf. Syst. Secur., vol. 3, no. 4, pp. 262-294, 2000.
[23] P. Proctor, "Practical Intrusion Detection Handbook," Upper Saddle River, NJ: Prentice-Hall, 2001.
[24] G. Vigna, W. Robertson, V. Kher, and R. A. Kemmerer, "A stateful intrusion detection system for worldwide web servers," in Proc. Annu. Comput. Secur. Appl. Conf. (ACSAC 2003), Las Vegas, NV, Dec. 2003, pp. 34-43.
[25] S. Forrest, S.-A. Hofmeyr, A. Somayaji, and T.-A. Longstaff, "A sense of self for Unix processes," in Proc. IEEE Symp. Res. Secur. Privacy, IEEE Comput. Soc. Press, May 1996, pp. 120-128.
[26] S.-A. Hofmeyr, S. Forrest, and A. Somayaji, "Intrusion detection using sequences of system calls," J. Comput. Secur., 1998.
[27] D. Gao, M.-K. Reiter, and D. Song, "Gray-box extraction of execution graphs for anomaly detection," in Proc. 11th ACM Conf. Comput. Commun. Secur., 2004, pp. 318-329.
[28] C. N. Modi, D. R. Patel, A. Patel, and M. Rajarajan, "Integrating signature Apriori-based network intrusion detection system (NIDS) in cloud computing," in 2nd Int. Conf. Commun. Comput. Secur., 2012, pp. 905-912.
[29] T. Alharkan and P. Martin, "IDSaaS: Intrusion Detection System as a Service in Public Clouds," in Proc. 12th IEEE/ACM Int. Symp. Cluster, Cloud Grid Comput. (CCGrid), 2012, pp. 686-687.
[30] A. Khaldi, K. Karoui, and H. Ben Ghezala, "Framework to detect and repair distributed intrusions based on mobile agent in hybrid cloud," in Int. Conf. Parallel Distrib. Process. Technol. Appl. (PDPTA'14), 2014, pp. 471-476.
[31] S. M. Manthira and M. Rajeswari, "Virtual host-based intrusion detection system for cloud," Int. J. Eng. Technol. (IJET), vol. 5, 2014, pp. 5023-5029.
[32] J. K. Khatri and G. Khilari, "Advancement in virtualization-based intrusion detection system in cloud environment," Int. J. Sci. Eng. Technol. Res. (IJSETR), vol. 4, 2015, pp. 1510-1514.
[33] S. Gupta and P. Kumar, "Immediate system call sequence-based approach for detecting malicious program executions in cloud environment," Wireless Pers. Commun., vol. 81, 2015, pp. 405-425.

[34] N. Pandeeswari and G. Kumar, "Anomaly detection system in cloud environment using fuzzy clustering-based ANN," Mobile Netw. Appl., 2015, pp. 1-12.
[35] B. Muthukumar and P. K. Rajendran, "Intelligent intrusion detection system for private cloud environment," Commun. Comput. Inf. Sci., vol. 536, 2015, pp. 54-65.
[36] S. Sangeetha, B. G. Devi, R. Ramya, M. K. Dharani, and P. Sathya, "Signature-based semantic intrusion detection system on cloud," in Inf. Syst. Des. Intell. Appl., vol. 339 of the series Adv. Intell. Syst. Comput., 2015, pp. 657-666.
[37] B. Al-Shdaifat, W. S. Alsharafat, and M. El-bashir, "Applying Hopfield artificial network and simulating annealing for cloud intrusion detection," J. Inf. Secur. Res., vol. 6, 2015, pp. 49-53.
[38] C. N. Modi and D. Patel, "A novel hybrid-network intrusion detection system (H-NIDS) in cloud computing," in IEEE Symp. Comput. Intell. Cyber Secur. (CICS), 2013, pp. 23-30.
[39] P. Ghosh, A. K. Mandal, and R. Kumar, "An efficient network intrusion detection system," in Inf. Syst. Des. Intell. Appl., vol. 339 of the series Adv. Intell. Syst. Comput., 2015, pp. 91-99.
[40] C. Ambikavathi and S. K. Srivatsa, "Improving virtual machine security through intelligent intrusion detection system," Indian J. Comput. Sci. Eng. (IJCSE), vol. 6, 2015, pp. 39.
[41] D. Singh, D. Patel, B. Borisaniya, and C. Modi, "Collaborative IDS framework for cloud," Int. J. Netw. Secur., vol. 18, 2016, pp. 699-709.
[42] S. A. Shaikh, H. Chivers, P. Nobles, J. A. Clark, and H. Chen, "A deployment value model for intrusion detection sensors," in Lecture Notes Comput. Sci., in 3rd Int. Conf. Inf. Secur. Assurance, vol. 5576, pp. 250-259, Jun. 2009.
[43] Z. Shelby and C. Bormann, 7LoWPAN: The Wireless Embedded Internet, 1st ed. Chichester, UK: Wiley, 2009.
[44] M. T. Dlamini, M. M. Eloff, and J. H. P. Eloff, "Internet of things: Emerging and future scenarios from an information security perspective," Southern Afr. Telecommun. Netw. Appl. Conf., Aug. 2009.
[45] C. Li, J. Yang, Y. Zhang, R. Chen, and J. Zeng, "Research on immunity-based intrusion detection technology for the internet of things," in Natural Comput. (ICNC), 2011 7th Int. Conf., vol. 1, IEEE, 2011, pp. 212-216.
[46] A. Gupta, O. J. Pandey, M. Shukla, A. Dadhich, S. Mathur, and A. Ingle, "Computational intelligence-based intrusion detection systems for wireless communication and pervasive computing networks," in Comput. Intell. Comput. Res. (ICCIC), 2013 IEEE Int. Conf., IEEE, 2013, pp. 1-7.
[47] V. P. Kafle, Y. Fukushima, and H. Harai, "Dynamic mobile sensor network platform for ID-based communication," in ITU Kaleidoscope Acad. Conf.: Living Converged World, IEEE, 2014, pp. 153-159.
[48] J. M. Batalla and P. Krawiec, "Conception of ID layer performance at the network level for Internet of Things," Pers. Ubiquitous Comput., vol. 18, pp. 465-480, Feb. 2014.
[49] P. Kasinathan, C. Pastrone, M. A. Spirito, and M. Vinkovits, "Denial-of-service detection in 6LoWPAN-based Internet of Things," in 2013 IEEE 9th Int. Conf. Wireless Mobile Comput., Netw. Commun. (WiMob'2013), Lyon, France, Oct. 2013.
[50] P. Kasinathan, G. Costamagna, H. Khaleel, C. Pastrone, and M. A. Spirito, "An IDS framework for Internet of Things empowered by 6LoWPAN," in 2013 ACM SIGSAC Conf. Comput. Commun. Secur., 2013, pp. 1337-1340.
[51] A. H. Farooqi and F. A. Khan, "A survey of intrusion detection systems for wireless sensor networks," Int. J. Ad Hoc Ubiquitous Comput., vol. 9, no. 2, pp. 69-83, 2012.
[52] R. Jurdak, X. R. Wang, O. Obst, and P. Valencia, "Wireless sensor network anomalies: Diagnosis and detection strategies," in Intell.-Based Syst. Eng., Springer, 2011, pp. 309-325.
[53] H. Moosavi and F. Bui, "A game-theoretic framework for robust optimal intrusion detection in wireless sensor networks," 2014.
[54] E. Karapistoli and A. A. Economides, "Anomaly detection and localization in UWB wireless sensor networks," in Pers. Indoor Mobile Radio Commun. (PIMRC), 2013 IEEE 24th Int. Symp., IEEE, 2013, pp. 2326-2330.

[55] L. Coppolino, S. D'Antonio, A. Garofalo, and L. Romano, "Applying data mining techniques to intrusion detection in wireless sensor networks," in P2P, Parallel, Grid, Cloud Internet Comput. (3PGCIC), 2013 8th Int. Conf., IEEE, 2013, pp. 247-254.
[56] A. Abduvaliyev, A.-S. K. Pathan, J. Zhou, R. Roman, and W.-C. Wong, "On the vital areas of intrusion detection systems in wireless sensor networks," IEEE Commun. Surv. Tutor., vol. 15, no. 3, pp. 1223-1237, 2013.
[57] S. Nishanthi and T. Virudhunagar, "Intrusion detection in wireless sensor networks using watchdog-based clonal selection algorithm," 2013.
[58] H. Sedjelmaci and M. Feham, "Novel hybrid intrusion detection system for clustered wireless sensor network," arXiv preprint arXiv:1108.2656, 2011.
[59] M. L. Manickam and S. Shanmugavel, "Resiliency-oriented secure routing protocol for malicious mobile ad hoc networks," in Int. Joint Conf. TSSA WSSA, Indonesia, 2006.
[60] R. Ranjana and M. Rajaram, "Detecting intrusion attacks in ad-hoc networks," Asian J. Inf. Technol., vol. 6, no. 7, pp. 758-761, 2007.
[61] R. Chaki and N. Chaki, "IDSX: A cluster-based collaborative intrusion detection algorithm for mobile ad hoc network," in Proc. IEEE Int. Conf. Comput. Inf. Syst. Ind. Manage. Appl. (CISIM), 2007.
[62] A. Mitrokotsa, N. Komninos, and C. Douligeris, "Intrusion detection with neural networks and watermarking techniques for MANET," in Int. Conf. Pervasive Serv., IEEE, 2007.