© SEP 2025 | IRE Journals | Volume 9 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I3-1710550

Intrusion and Detection Systems for Wired and Wireless Network Application

OKETAYO ABIMBOLA[1], NRIAGU C.OGONNA2, ODUWOLE OLUWAKEMI O.[3]
[1, 2, 3]*National Mathematical Centre, Abuja, Nigeria*

Abstract - The proliferation of wired and wireless networks has increased the risk of cyber threats, making intrusion detection systems (IDS) crucial for network security. This research focuses on designing and developing advanced IDS for both wired and wireless network applications. We explore various machine learning and deep learning techniques to detect and prevent intrusions, including anomaly-based and signature-based detection methods. Our system aims to improve detection accuracy, reduce false positives, and enhance network security. The proposed IDS can be applied to various network environments, including IoT, cloud computing, and industrial control systems. This research contributes to the development of robust and efficient IDS for protecting wired and wireless networks from cyber threats.

Keywords: Intrusion Detection Systems, Network Security, Machine Learning, Deep Learning, Wired Networks, Wireless Networks, Cyber Threats.

I. INTRODUCTION

IDSs are the process of detecting and identifying unauthorized or unusual activity on the system.It can also be described as the process of evaluating suspicious activity that occurs in a corporate network. IDSs will help detect unauthorized activities or intrusions that may compromise the confidentiality, integrity, or availability of a resource. Heavy reliance on networked computer resources and the increasing connectivity of these networks has greatly increased the potential damage caused by attacks launched against computers from remote sources (wireless networks). It is not easy to prevent these attacks with a firewall, mechanism, or security policy due to their dynamism. Information held by Information Technology (IT) products or systems is a critical resource that enables organizations to succeed in their mission. Additionally, individuals have a reasonable expectation that their personal information contained in IT products or systems remain private, be available to them as needed, and not be subject to unauthorized modification. IT products or systems should perform their functions while exercising proper control of the information to ensure it is protected against hazards such as unwanted or unwarranted dissemination, alteration, or loss. The term IT security is used to cover prevention and mitigation of these and similar hazards (DeMara, 2004). It is very important that the security mechanisms of a system are designed to prevent unauthorized access to system resources and data. However, completely preventing breaches of security appear, at present, unrealistic. we can try to detect these intrusion attempts so that action may be taken to repair the damage now or later. This field of research is called Intrusion Detection.

The nature of mobile computing environment makes it very vulnerable to an adversary's malicious attacks. First of all, the use of wireless links renders the network susceptible to attacks ranging from passive eavesdropping to active interfering. Unlike wired networks where an adversary must gain physical access to the network wires or pass through several lines of defense at firewalls and gateways, attacks on a wireless network can come from all directions and target at any node. Damages can include leaking secret information, message contamination, and node impersonation. All these mean that a wireless network will not have a clear line of defense, and every node must be prepared for encounters with an adversary directly or indirectly.

Performances depend on factors like users, medium, hardware, and the efficacy of the software evaluated using two Matrix, throughput, and delay. Reliability on the other hand is measured by a frequency that requires a security objective or primitive. To avoid the issue of security primitive or objective being violated frequently, a detection criterion needs to be put in place and this is Intrusion Detection System (IDS). There are anti-intrusion detection techniques used in a network be it wireless or wired. Anti intrusion technique has six components: pre-emption, countermeasures, deterrence, prevention, deflection, and detection. Accurate Detection is more critical and accurate. Intrusion detection systems had a dual approach. It used a rule-based Expert System to detect known types of intrusions plus a statistical

anomaly detection component based on profiles of users, host systems, and target systems

IDS help in the detection of unauthorized activities or intrusions that may compromise the confidentiality, integrity, or availability of a resource. Investigating the future of intrusion detection systems by exploring results of research papers published between 2011 and 2016 touching IDS history, current and future on networks it is realized that IDS can be implemented in any part of the system. Results of papers published on IDS analyzed using machine learning and mathematical regression. A mathematical aspect used in IDS analysis shows that the intrusion detection system can be implemented at DTE or DCE and in any type of network regardless of the channel.

The evolution of malicious software (malware) poses a critical challenge to the design of IDS. Malicious attacks have become more sophisticated and the foremost challenge is to identify unknown and obfuscated malware, as the malware authors use different evasion techniques for information concealing to prevent detection by an IDS. In addition, there has been an increase in security threats such as zero-day attacks designed to target internet users. Therefore, computer security has become essential as the use of information technology has become part of our daily lives. As a result, various countries such as Australia and the US have been significantly impacted by the zero-day attacks. According to the 2017 Symantec Internet Security Threat Report, more than three billion zero-day attacks were reported in 2016, and the volume and intensity of the zero-day attacks were substantially greater than previously (Symantec, 2017). High profile incidents of cybercrime have demonstrated the ease with which cyber threats can spread internationally, as a simple compromise can disrupt a business' essential services or facilities. There are a large number of cybercriminals around the world motivated to steal information, illegitimately receive revenues, and find new targets. Malware is intentionally created to compromise computer systems and take advantage of any weakness in intrusion detection systems. In 2017, the Australian Cyber Security Centre (ACSC) critically examined the different levels of sophistication employed by the attackers (Australian, 2017). So there is a need to develop an efficient IDS to detect novel, sophisticated malware. The aim of an IDS is to identify different kinds of malware as early as possible, which cannot be achieved by a traditional firewall. With the increasing volume of computer malware, the development of improved IDSs has become extremely important.

When an intrusion (defined as "any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource" (R. Heady, 1990)) takes place, intrusion prevention techniques, such as encryption and authentication, are usually the first line of defense. However, intrusion prevention alone is not sufficient because as systems become ever more complex, and as security is still often the after-thought, there are always exploitable weaknesses in the systems due to design and programming errors, or various "socially engineered" penetration techniques. For example, even though they were first reported many years ago, exploitable "buffer overflow" security holes, which can lead to an unauthorized root shell, still exist in some recent system softwares.

Furthermore, as illustrated by the DDoS attacks launched against several major Internet sites where security measures were in place, the protocols and systems that are designed to provide services (to the public) are inherently subject to attacks such as DDoS. Intrusion detection can be used as a second wall to protect network systems because once an intrusion is detected, e.g., in the early stage of a DDoS attack, response can be put into place to minimize damages, gather evidence for prosecution, and even launch counter-attacks.

II. REVIEW OF RELATED WORKS

The primary assumptions of intrusion detection are: user and program activities are observable, for example via system auditing mechanisms; and more importantly, normal and intrusion activities have distinct behavior. Intrusion detection therefore involves capturing audit data and reasoning about the evidence in the data to determine whether the system is under attack. Based on the type of audit data used, IDSs can be categorized as network-based or host-based. A network-based IDS normally runs at the gateway of a network and "captures" and examines network packets that go through the network hardware interface. A host-based IDS relies on operating system audit data to monitor and analyze the events generated by programs or users on the host. Intrusion detection techniques can be

categorized into misuse detection and anomaly detection (D.E.Denning, 1987) (W.Lee, 1999).

Misuse detection systems, e.g., IDIOT (Spafford, 1995) and STAT (K. Ilgun, 1995), use patterns of well-known attacks or weak spots of the system to match and identify known intrusions. For example, a signature rule for the "guessing password attack" can be "'there are more than 4 failed login attempts within 2 minutes". The main advantage of misuse detection is that it can accurately and efficiently detect instances of known attacks. The main disadvantage is that it lacks the ability to detect the truly innovative (i.e., newly invented) attacks. Anomaly detection (sub)systems, for example, the anomaly detector in IDES (T. Lunt, 1992), flag observed activities that deviate significantly from the established normal usage problems as anomalies, i.e., possible intrusions. For example, the normal profile of a user may contain the averaged frequencies of some system commands used in his or her login sessions. If for a session that is being monitored, the frequencies are significantly lower or higher, then an anomaly alarm will be raised. The main advantage of anomaly detection is

2.1 Signature-based intrusion detection systems (SIDS)

Signature intrusion detection systems (SIDS) are based on pattern matching techniques to find a known attack; these are also known as Knowledge-based Detection or Misuse Detection (Khraisat A, 2018). In SIDS, matching methods are used to find a previous intrusion. In other words, when an intrusion signature matches with the signature of a previous intrusion that already exists in the signature database, an alarm signal is triggered. For SIDS, host's logs are inspected to find sequences of commands or actions which have previously been identified as malware. SIDS have also been labelled in the literature as Knowledge-Based Detection or Misuse Detection (C. Modi, 2013).

SIDS usually gives an excellent detection accuracy for previously known intrusions (Kreibich C, 2004). However, SIDS has difficulty in detecting zero-day attacks for the reason that no matching signature exists in the database until the signature of the new attack is extracted and stored. SIDS are employed in numerous common tools, for instance, Snort (M, 1999) and NetSTAT (Vigna G, 1999).

Traditional approaches to SIDS examine network packets and try matching against a database of signatures. But these techniques are unable to identify attacks that span several packets. As modern malware is more sophisticated it may be necessary to extract signature information over multiple packets. This requires the IDS to recall the contents of earlier packets. With regards to creating a signature for SIDS, generally, there have been a number of methods where signatures are created as state machines (C. R. Meiners, 2010), formal language string patterns or semantic conditions (Lin C, 2011).

The increasing rate of zero-day attacks (Symantec, 2017) has rendered SIDS techniques progressively less effective because no prior signature exists for any such attacks. Polymorphic variants of the malware and the rising amount of targeted attacks can further undermine the adequacy of this traditional paradigm.

2.2 Intrusion data sources

The previous two sections categorised IDS on the basis of the methods used to identify intrusions. IDS can also be classified based on the input data sources used to detect abnormal activities. In terms of data sources, there are generally two types of IDS technologies, namely Host-based IDS (HIDS) and Network-based IDS (NIDS). HIDS inspect data that originates from the host system and audit sources, such as operating system, window server logs, firewalls logs, application system audits, or database logs. HIDS can detect insider attacks that do not involve network traffic (Creech G, 2014a).

NIDS monitors the network traffic that is extracted from a network through packet capture, NetFlow, and other network data sources. NIDS can be used to monitor many computers that are joined to a network. NIDS is able to monitor the external malicious activities that could be initiated from an external threat at an earlier phase, before the threats spread to another computer system. On the other hand, NIDSs have limited ability to inspect all data in a high bandwidth network because of the volume of data passing through modern high-speed communication networks (Bhuyan MH, 2014). NIDS deployed at a number of positions within a particular network topology, together with HIDS and firewalls, can provide a concrete, resilient, and multi-tier protection against both external and insider attacks.

2.3 Anomaly detection

With the world moving towards being increasingly dependent on computers and automation, one of the main challenges in the 1980s has been to build secure applications, systems, and networks for users (Hindy, 2018). In the 1990s, IDS technology improved to address the increasing number and sophistication of network attacks. This new method, named anomaly detection, relied on identifying unusual behavioral patterns on the network and provided alerts for any identified abnormality. There are other different types of attacks like Probe attacks, Remote to Local (R2L), Dos (Denial of service), and user to remote (U2R) attacks which are detected differently. The main advantage of AIDS is the ability to identify zero-day attacks due to the fact that recognizing the abnormal user activity does not rely on a signature database (A. Alazab, 2012). AIDS triggers a danger signal when the examined behavior differs from the usual behavior. Furthermore, AIDS has various benefits. First, they have the capability to discover internal malicious activities. If an intruder starts making transactions in a stolen account that are unidentified in the typical user activity, it creates an alarm. Second, it is very difficult for a cybercriminal to recognize what is a normal user behavior without producing an alert as the system is constructed from customized profiles.

2.3.1 Wireless Security

Wireless networking increases the flexibility in the home, work place and community to connect to the internet without being tied to a single location.

With the benefits of Wi-Fi there are also some risks which users should be aware of. Without any security implemented, unauthorised users may steal data or load malicious code onto the network with the intention of creating havoc. Unlike wired networks, the radio signal produced by wireless networks can penetrate walls, ceilings, floors and are therefore not confined to a building. Hackers can effortlessly pick up these signals from the outside of the building using easily available wireless detection tools.

Many WLANs used in the home still operate with no measure of encryption. However, there does arise something of a problem for the home user when establishing a WLAN, namely which encryption protocol to use.

The majority of wireless networks use the IEEE 802.11 standard for communication. Initially the IEEE 802.11b was the de-facto security standard for wireless networking technology for small businesses and home users, with all Wireless Access Points equipped with Wired Equivalency Protocol (WEP). Flaws in WEP were soon discovered and in response to this, the 802.11i task group were developed to address the major problems with security. They addressed three main security areas: authentication, key management and data transfer privacy. The Wi-Fi Alliance developed Wi-Fi Protected Access (WPA) as a Wi-Fi standard, which accelerated the introduction of stronger security. As the security standards have evolved other wireless security options have become available which are preinstalled on devices, these include WPA and Temporal Key Integrity Protocol (TKIP).

Initially, when Wi-Fi networking was in its infancy, war-walking, war-driving and war-chalking were well publicised phenomena. Developed by Peter Shipley in April 2001, these terms describe the process used by hackers walking or driving around areas looking for unsecured wireless networks.

Symbols were left on the walls or pavements to indicate the security status of nearby Wi-Fi points. War-driving did highlight the worrying results that firstly a large proportion of Wi-Fi users do not enable any form of encryption and secondly that the standard wireless encryption protocol (Wired Equivalency Protocol - WEP) can easily be cracked.

Even after much publicity about wireless encryption and new improved protocols were made available, a survey conducted by White Hat in January 2005 J.Hart found 51% of businesses, within a one-mile radius of Bristol town centre, did not use any form of encryption. Of those who did use encryption, 25% used the default service set identifier (SSID) and therefore probably still had the factory passwords.

2.3.2 Problems of Current IDS Techniques

The vast difference between the fixed network where current intrusion detection research are taking place and the mobile network makes it very difficult to apply intrusion detection techniques developed for one environment to another. The most important difference is perhaps that the latter does not have a fixed infrastructure, and today's network-based IDSs, which rely on real-time traffic analysis, can no longer function well in the new environment.

A significant big difference is in the communication pattern in a mobile computing environment. Mobile users can be stingy about communication and often

adopt new operation modes such as disconnected operations (M. Satyanarayanan, 1993). This suggests that the anomaly models for wired network cannot be used as is. Furthermore, there may not be a clear separation between normalcy and anomaly in mobile environment. Intrusion detection may find it increasingly difficult to distinguish false alarms from real intrusions.

III. TYPES OF COMPUTER ATTACKS

Cyber-attacks can be categorized based on the activities and targets of the attacker. Each attack type can be classified into one of the following four classes (Mukkamala, 2003):

1. Denial-of-Service (DoS) attacks have the objective of blocking or restricting services delivered by the network, computer to the users.
2. Probing attacks have the objective of acquisition of information about the network or the computer system.
3. User-to-Root (U2R) attacks have the objective of a non-privileged user acquiring root or admin-user access on a specific computer or a system on which the intruder had user level access.
4. Remote-to-Local (R2L) attacks involve sending packets to the victim machine. The cybercriminal learns the user's activities and obtains privileges which an end user could have on the computer system.

3.1 IDS Evasion Techniques

1. Flooding
   The attacker begins the attack to overwhelm the detector and this causes a failure of control mechanism. When the detector fails, all traffic would be allowed (Kolias C, 2016). A popular method to create a flooding situation is spoofing the legitimate User Datagram Protocol (UDP) and Internet Control Message Protocol (ICMP). The traffic flooding is used to disguise the abnormal activities of the cybercriminal. Therefore, IDS would have extreme difficulty to find malicious packets in a huge amount of traffic.

2. Obfuscation
   Obfuscation techniques can be used to evade detection, which are the techniques of concealing an attack by making the message difficult to understand (Kim, 2017). The terminology of obfuscation means changing the program code in a way that keeps it functionally identical with the aim to reduce detectability to any kind of static analysis or reverse engineering process and making it obscure and less readable. This obfuscation of malware enables it to evade current IDS.
   Obfuscation attempts to utilize any limitations in the signature database and its capability to duplicate the way the computer host examines computer's data (Alazab A, 2016). An effective IDS should be supporting the hexadecimal encoding format or having these hexadecimal strings in its set of attack signatures (M. Cova, 2010). Unicode/UTF-8 standard permits one character to be symbolized in several various formats. Cybercriminals may also use double-encoded data, exponentially escalating the number of signatures required to detect the attack.
   SIDS relies on signature matching to identify malware where the signatures are created by human experts by translating a malware from machine code into a symbolic language such as Unicode. However, the use of code obfuscation is very valuable for cybercriminals to avoid IDSs.
3. Encryption
   Generally, encryption offers a number of security services, such as data confidentiality, integrity, and privacy. Malware authors employ these security attributes to escape detection and conceal attacks that may target a computer system. For example, attacks on encrypted protocols such as HyperText Transfer Protocol Secure (HTTPS) cannot be read by an IDS (Metke AR, 2010). The IDS cannot match the encrypted traffic to the existing Database signatures if it doesn't interpret the encrypted traffic. Therefore, examining encrypted traffic makes it difficult for detectors to detect attacks (Butun I, 2014). For example, packet content-based features have been applied extensively to identify malware from normal traffic, which cannot readily be applied if the packet is encrypted. These challenges motivate investigators to use some statistical network flow features, which do not rely on packet content (J.

Camacho, 2016). As a result of this, malware can potentially be identified from normal traffic.

3.2 Possible Security Threats

Like wired networks, wireless networks are subject to malicious attacks. The radio signals do not remain within the confines of the building, and indoor routers have a range of approximately 20-150 metres, depending on the 802.11 standard and the data rate. Therefore, the radio signal can easily be detected externally or in a neighbouring building.

This means the attacker does not need to infiltrate the building to hack the network. With the right equipment, it is possible for the radio signal to extend up to 125 miles. However, such distances can only be reached in certain environments such as deserts, which lack structures such as buildings and trees. Obstacles such as walls and distance can cause the radio signal to attenuate and the threat of attack will decrease. Wireless detection devices work in two modes, passive and active. The passive mode listens for the access points' broadcast, which may or may not contain the SSID. Whereas active mode uses the probe request and response to detect access points, which involves the access point responding to the probe request. Attacks on WLANs can be categorised as passive attacks which include War-Driving and Sniffing (via a promiscuous mode); and active attacks include Spoofing (impersonation), Denial-of-Service attacks (DoS) and Man-in-the-middle attacks.

3.2.1 Passive Attacks - Accidental users

Occasionally when trying to connect to an Access Point the computer may automati-cally connect to a different network and the user may "accidentally" use that connection without realising it belongs to a third party. However, it is illegal in Italy to use bandwidth without the consent of the owner according to articles 615 and 617 of italian penal code. This may occur in the work place when users are unfamiliar with the company's SSID and pick up a neighbouring company's unsecured network.

3.2.2 Active Attacks - Brute force attack

A brute force attack is the systematic testing of different letters, numbers and symbols until the correct password or key is guessed. There are a number of software programmes available on the Internet that can be used to recover encryption keys on wireless LANs, these include AirSnort and WEPCrack. AirSnort requires approximately 5-10 million encrypted packets to be gathered. Once enough packets have been collected, AirSnort can guess the encryption password in under a second. WEP can easily be cracked because the Initialisation Vector is sent as plaintext within the encrypted packet. This means that if anyone intercepts the data using a sniffer package, they will be able to decipher the secret key.

The newer encryption standard WPA can also be cracked using a tool called WPA Cracker that uses dictionary brute-force attack, which can check 16-18 passwords/second on a 1.4GHz notebook. It is therefore recommended that passphrases are at least 20 characters long and do not contain dictionary words.

3.2.3 Denial-of-Service attacks

A Denial-of-Service attack (DoS) can cause a network to slow down or become unusable. A DoS attack may occur if the attacker generates a lot of traffic on the network, which may block the server for hours or by attacking the resource itself. Another form of DoS attack is the use of a strong radio signal. This denies legitimate users from accessing a resource. Distributed Denial-of-Service attacks (DDoS) occurs when many computers are used against the target. A single master program can be loaded onto a commandeered computer via an insecure wireless network; the master program can communicate to "agent" computers anywhere on the Internet infected with the agent program and initiate an attack.

3.2.4 Man-in-the-middle attack

A Man-in-the-middle attack occurs when an attacker is able to read and modify communications between two parties without them being aware of the attacker's presence. An Evil Twin attack (also known as base-station cloning/access point cloning) is similar to a Man-in-the-middle attack. The term is used for fake hotspots/access points, which pretend to be a legitimate hotspot. The Evil Twin is a malicious server, which may be used to extract sensitive information such as bank details. The hacker sets up the SSID to be the same as the local hotspot or corporate wireless network. The hacker may disrupt or disconnect the access point by directing a Denial-of-Service attack against it, or by creating radio signal interception around it. The hacker may then intercept the traffic. The user is unaware that they are not using a legitimate hotspot

and may unknowingly provide their user name and password as they log on to the fake hotspot. Evil Twin networks may be avoided by enabling the WEP or WPA security, so the user is unable to join the "evil network"' as the key will not match.

3.2.5 Session High-Jacking

Session High Jacking is an attack against the integrity of a session. The attacker takes an authorized and authenticated session away from its proper owner. The target knows that it no longer has access to the session but may not be aware that the session has been taken over by an attacker. The target may attribute the session loss to a normal malfunction of the WLAN. Once the attacker owns a valid session she may use the session for whatever purposes she wants and maintain the session for an extended time. This attack occurs in real-time but can continue long after the victim thinks the session is over.

3.2.6 Intrusion Detection for WLAN

Intrusion prevention measures, such as encryption and authentication, can be used in wireless networks to reduce intrusions, but cannot eliminate them. For example, encryption and authentication cannot defend against compromised mobile nodes, which often carry the private keys. The history of security research has taught us a valuable lesson: no matter how many intrusion prevention measures are inserted in a network, there are always some weak links that one could exploit to break in. Intrusion detection presents a second wall of defense and it is a necessity in any high-survivability network. In summary, mobile computing environment has inherent vulnerabilities that are not easily preventable.

To secure mobile computing applications, we need to deploy intrusion detection and response techniques, and further research is necessary to adapt these techniques to the new environment, from their original applications in fixed wired network.

3.3 Additional Security solutions

In order to achieve a more security level to our WIDS we have to add these security features

1. Honeypot

A Honeypot is a security resource whose value lies in being probed, attacked or compromised. This means, that a honeypot is expected to get probed, attacked and potentially exploited. In fact, honeypot provides additional and valuable information about the hacker. WIDS must incorporate honeypot features, which diverts attacker to fakedAP that eventually leads to a honeypot where events are quarantined from the production network, Whith the target being deceived, it starts to record every single move made by it. Hopefully, these records can be used as a learning material and reference.

2. Address Rule Matching

This feature is necessary to detect if duplicated mac addresses are being used in our network. To understand if some client try to spoof some MAC addresses availables, we need to trace the MAC addresses that are being used in our network and compare them in our database of mac address knowns to be authorized to access our network

3. War-Driving attempts

Before connecting to a WLAN, client device must first find an AP either by listening for AP's beacon or broadcasting probe request consecutively. As stated in 802.11, AP must reply a probe respnse, as to inform its existence, to the client that issues the request to establish connection. War-Driving takes the advantage of such vulerability to scan every AP within radio signal range by broadcasting probe request frames.

IV. CONCLUSION

Undoubtedly, network attacks present a serious problem in the field of information technology and challenge its rate of growth and wide acceptance by the public, government and businesses. This provides an overview of intrusion detection and the way it is expected to operate in a wireless network. The prominent IDS research of the past decade (2008-2023) is analyzed with the intent to find the trend towards network protection and intrusion detection. Heavy reliance on networked computer resources and the increasing connectivity of these networks has greatly increased the potential damage that can be caused by attacks launched against computers from remote sources (wireless networks). It is not easy to prevent these attacks with a firewall, mechanism, or security policy due to their dynamism.

REFERENCES

[1] Alazab, M. H. (2012). Using feature selection for intrusion detection system. international symposium on communications and information technologies.

[2] Alazab A, K. A. (2016). New strategy for mitigating of SQL injection attack. Int J Comput Appl.
[3] Australian. (2017). Australian cyber security center threat report 2017. Retrieved from https://www.acsc.gov.au/publications/ACSC_Threat_Report_2017.pdf
[4] Bhuyan MH, B. D. (2014). Network anomaly detection: methods, systems and tools. IEEE Communications Surveys & Tutorials.
[5] Butun I, M. S. (2014). A survey of intrusion detection systems in wireless sensor networks. IEEE Communications Surveys & Tutorials.
[6] Modi, D. P. (2013). A survey of intrusion detection techniques in cloud. J Netw Comput Appl.
[7] Meiners, J. P. (2010). Fast regular expression matching using small TCAMs for network intrusion detection and prevention systems. Washington, DC.
[8] Creech G, H. J. (2014a). A semantic approach to host-based intrusion detection systems using Contiguousand Discontiguous system call patterns. IEEE Trans Comput.
[9] Denning D.E (1987). An instrusion detection model.
[10] DeMara, R. (2004). Mitigation of network tampering using dynamic dispatch of mobile agents.
[11] Hindy. (2018). taxonomy and survey-based IDS design techniques. Proceedings of 2nd International Conference on Information Technology for Application. Retrieved 2004
[12] Camacho, A. P.-V.-T.-F. (2016). PCA-based multivariate statistical network monitoring for anomaly detection. Computers & Security.
[13] Ilgun, R. A. (1995). State transition analysis: A rule-based intrusion detection approach.
[14] Khraisat A, G. I. (2018). An anomaly intrusion detection system using C5 decision tree classifier. In: Trends and applications in knowledge discovery and data mining. Springer International Publishing, Cham.
[15] Kim, D. M. (2017). DynODet: detecting dynamic obfuscation in malware," in Detection of intrusions and malware, and vulnerability assessment. Bonn, Germany: 14th international conference, DIMVA 2017.
[16] Kolias C, K. G. (2016). Intrusion detection in 802.11 networks: empirical evaluation of threats and a public dataset. IEEE Communications Surveys & Tutorials.
[17] Kreibich C, C. J. (2004). Honeycomb: creating intrusion detection signatures using honeypots. SIGCOMM Comput Commun Rev.
[18] Lin C, L. Y.-D.-C. (2011). A hybrid algorithm of backward hashing and automaton tracking for virus scanning. IEEE Trans Comput.
[19] Cova, C. K. (2010). Detection and analysis of drive-by-download attacks and malicious JavaScript code. North Carolina, USA: Presented at the Proceedings of the 19th international conference on world wide web.
[20] Satyanarayanan, J. J. (1993). Experiences with disconnected operation in a mobile environment.
[21] Metke AR, E. R. (2010). Security Technology for Smart Grid Networks. IEEE Transactions on Smart Grid.
[22] Mukkamala, A. H. (2003). Identifying important features for intrusion detection using support vector machines and neural networks. in Symposium on Applications and the Internet.
[23] Heady, G. L. (1990). The architecture of a network level intrusion detection system.
[24] Spafford, S. K. (1995). A software architecture to support misuse intrusion detection.
[25] Symantec. (2017). Internet security threat report 2017. Retrieved from https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf
[26] Lunt, A. T. (1992). A real-time intrusion detection expert system (IDES).
[27] Vigna G, K. R. (1999). NetSTAT: a network-based intrusion detection system. J Comput Secur.
[28] Lee, S. a. (1999). Mining in a data flow environment: Experience in network intrusion detection.