Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 08, August-2021

A Survey of Network Attack Detection Research

Abas Aboras[1], Mohammed Kamal Hadi[2]
[1]School of Software Engineering, Yangzhou University, Yangzhou, China.
[2]School of Material Science and Engineering, Lanzhou University of Technology, Lanzhou, China.

***Abstract*—With the popularization of the Internet, resources shared on the Internet have become the main targets of hackers'. In view of the rapid increase in network attacks and their adverse effects, information security issues have become the focus of attention. In recent years, the number of security incidents has been increasing year by year. Hackers use hidden loopholes in the system to attack, resulting in threats to the system's confidentiality, consistency, and availability. This makes application Internet organizations face severe challenges. Therefore, the detection of malicious attacks has become the top priority of network security. With the development and update of network attack technology, attacks are becoming more complex and difficult to understand and defend. In this paper, a survey on network attack detection is presented. Moreover, the paper also provides a network security protection strategy to make users use the network more safely and avoid network attacks.**

***Keywords*— Computer network, Network attack, Network security.**

I. INTRODUCTION

The scope of the use of the Internet has expanded tremendously over the past few years thanks to the spread of tablets and smartphones, after their use was limited to personal computers and laptops, but this great spread was accompanied by a rise in the rate of piracy and electronic attacks in a way in which information security became an obsession for individuals and institutions alike. Network attacks are attacks on systems and resources by exploiting vulnerabilities and security flaws in network information systems [1]. The threats faced by network information systems come from many aspects and will change over time. From a macro perspective, these threats can be divided into man-made threats and natural threats. Natural threats come from various natural disasters, harsh site environments, electromagnetic interference, and natural aging of network equipments. These threats are purposeless, but they can cause damage to the network communication system and endanger communication security. And man-made threats are man-made attacks on network information systems, which seek to destroy, deceive, and steal data and information in an unauthorized manner by looking for weaknesses in the system. Compared with the two, well-designed man-made attack threats are difficult to guard against, and there are many types and numbers. From the perspective of the destructiveness of information, the types of attacks can be divided into passive attacks and active attacks. However, the following is the security problem, hackers can use a variety of attack methods to steal personal data or remote control [2]. The traditional network gateway firewall has been unable to effectively block all kinds of attacks, so there are a variety of protection methods in order to reduce the risk of enterprise users leaking confidential data such as intrusion detection system and anti-virus wall, but they all have their own protection limitations. In order to meet the three basic characteristics of information security: confidentiality, integrity and availability, the concept of defense in depth has been applied to network security protection, which is characterized by using layer by layer protection filtering technology to expand the defense line. Each protective equipment performs its own duties to block and filter, which can effectively prevent the occurrence of attacks.

II. RELATED WORK

Network attacks are an important hidden danger that affects network security. In order to ensure the safe operation of the network, it is necessary to detect the attack behavior in the network on time. The concept of intrusion detection was first proposed by Anderson in 1980 [3]. Heberlein, et al [4] proposed a network intrusion detection method based on network traffic data to detect suspicious network behaviors. According to the data source of mining and analysis, network intrusion detection can be divided into host-based, network-based and hybrid detection method. The host-based method monitors the client-level attack behavior, the network-based method monitors the attack risk of the entire network, and the hybrid type can simultaneously monitor the entire network and the network security of specific users. Sharma, et al [5] presented fundamentals like a network attack, how to prevent it, its types, preventive measures, and current procedures that focus on this paradigm. In addition, attempt to help users understand the concept of attacks to avoid them. Farooqi, et al [6] proposed a method of network intrusion detection based on analyzing and mining different patterns in different types of network attacks. Additionally, the network behavior data is judged as an attack when it matches one of the patterns. Godala, et al [7] presented the taxonomy of security attacks, different intrusion detection system mechanisms for detecting attacks, and performance metrics used to assess the IDS algorithm. Azeez, et al. [8] proposed a method of abnormal data detection based on comparing the behavior of network data; if the behavior of the data is abnormal, it is judged to be aggressive behavior. Although the anomaly-based method has a high rate of misjudgment, it can effectively detect unknown attack types. Y. wu, et al [9] performed a literature analysis investigating various attack detection methods involving the strength of deep learning techniques. D. Liu, et al [10] proposed an approach to network attack detection based on reverse detection and protocol analysis. The proposed method analyzes the network attack site quickly and accurately by knowing the specific attack behavior, which effectively ensures the safe operation of the system network.

III. NETWORK ATTACK

Network attack has existed since the development of the Internet. Network attackers construct malicious network packets according to the scanning results of the target network to be attacked, and then send huge network packets to the target network directly or indirectly by proxy. Of course, in

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 08, August-2021

some cases, the packet is harmless, but when the network packet flow is too large, it will cause the normal network server or device to overload, consume the hardware resources of the system very quickly, and eventually cause the server or network device to not respond to other normal access. In other cases, the attacker uses some tools and programs that can analyze, delete or delay the traffic of the target network data. The hardware of the server is not what it used to be, and its processing speed and performance are by no means comparable to the early development of the network. Because of this reason, it is difficult for network attackers to attack the target network through their personal computers, and it works to consume the resources of the target network by exploiting the security holes, spoiling and paralyzing them. And those resources become unable to effectively resist any attack.

Network attackers use malicious software to control other computers on the network through agent channels. When these controlled computers receive the attack command from the attacker, the malicious software will construct the network attack packet and send it to the target network host [11]. It is difficult for us to locate the attacker when the network is attacked in this way. At the same time, because attackers control a large number of hosts through malicious software, the intensity of network attacks is very large.

In the early stage of the development of computer network, the protocol designers considered the reliability of communication between computers, and designed the TCP / IP five layers network protocol “Application” according to the hierarchy of network transmission. The data is encapsulated from the initial application layer, then it is encapsulated into UDP or TCP packets through the transport layer, then it is encapsulated into IP datagrams through the network layer, then it is encapsulated into MAC frames through the link layer, and finally the data is sent to the physical layer and transmitted to other computers through the network card [12]. This design is a good solution to the communication between computers, but with the in-depth study of the network protocol, network attackers found that there are still some loopholes between the network protocols of the computer. At present, there are many kinds of network attacks, which can be summarized as follows:

1) TCP “SYN” denial of service attack: In normal network communication, the establishment of a TCP network connection needs three handshakes, that is, the founder sends a SYN message to the target host, and the target host replies to the founder's SYN and ACK message after receiving the syn message, and then waits for the initiator. After receiving the message, the initiator replies with an ACK message to the target host, and a complete connection is established [13].

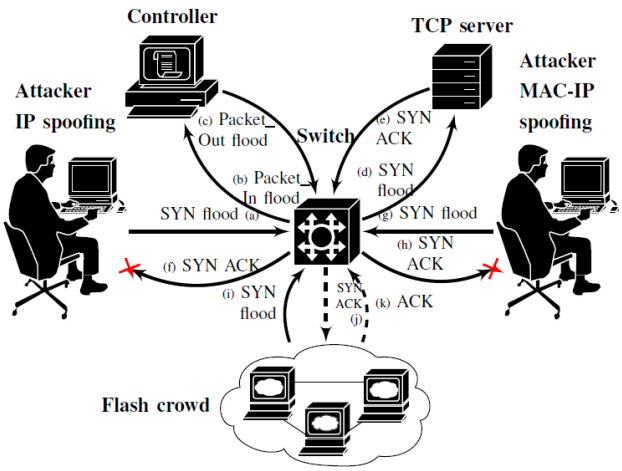

Fig. 1. Shows SYN flood denial of service attack

2) ICMP flood attack: In the design of network protocol, designers hope to diagnose other hosts through the network to judge whether they are working normally, such as ping program, traceroute program and so on. These programs mainly send ICMP message, and the computer that receives ICMP message will reply to the message, that is ICMP-echo message. Network attackers use such messages to send a large number of ICMP messages through a large number of controlled computers, which makes the target network host busy processing these ICMP messages and unable to process normal network data.

3) UDP flood attack: the principle of network attack is similar to ICMP flood attack. Network attackers send a large number of UDP network packets to the target host, which eventually leads the target host to being busy with processing these UDP packets and unable to process normal network data [14].

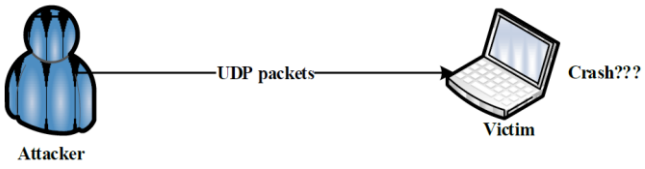

Fig. 2. Shows UDP flood attack

4) Port scan attack: according to the network transmission protocol, when a computer receives a connection request message, that is, a SYN message, the computer will have two choices. If the port in the corresponding request is open, the computer will respond to a SYN and ACK message data, and establish a TCP connection; if the port in the corresponding request is closed, the computer will respond to an RST message data, telling the request initiator that the port is closed in the computer [15]. The following table shows the three-way handshake. We have performed three-port scan attacks.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 08, August-2021

TABLE I: TCP response to flag packets

S. no	TCP Flag value	Receiving host	
		Open /listening port	Close port
1	ACK	Drop packet and send RST message	Drop packet
2	FIN/PSH/URG	Drop packet	Drop packet and send RST message
3	Null	Drop packet	Drop packet and send RST message

5. IP fragment message attack: In the computer network, in order to transmit a large IP message, the IP protocol will obtain the MTU in the network. After obtaining the MTU, the large IP message will be divided by calculation. At the same time, the identification and slice offset in the fragment will be numbered.

IV. CLASSIFICATION OF NETWORK ATTACK DETECTION

The technological revolution, especially the communications revolution, is the most important development that the world is experiencing today, and the communications revolution is the main engine in the current developments, but it is not the only engine in these developments as the great development in computer technology has contributed greatly to the acceleration of the rates of progress in the field of Communication and information [16]. Since entering the information age, with the wide application of computer network, all kinds of security problems in computer network are becoming more and more serious, which has become an important problem in the new era.

A. Network attack detection process

With the widespread use of high-speed networks and malicious software, the targets and methods of network attacks have shown diversity, and cyberspace security is facing unprecedented challenges [17]. The high-speed network intrusion detection system based on data mining faces huge challenges in constructing and executing intrusion detection tasks. The key to network attack detection is to quickly identify unknown attack behaviors in the network through the analysis of network traffic [18]. In the big data environment, it is necessary to study how to ensure that anomaly detection is not affected. The coarse-grained reduces the network traffic data that needs to be processed, filters out the subset that needs fine-grained anomaly detection, provides reliable data support for network attack discovery, and improves the efficiency of anomaly detection processing. In recent years, data reduction has received close attention from many researchers at home and abroad. There are two main ways of data reduction: data sampling and data feature dimensionality reduction. The network attack detection process proposed in this paper is shown in Figure 3.

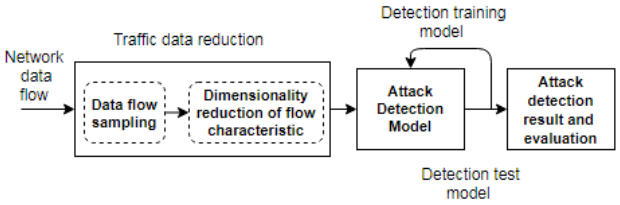

Fig. 3. Network attack detection process

The network attack detection process is roughly divided into five steps: 1) network traffic data acquisition; 2) traffic data sampling; 3) traffic feature dimensionality reduction; 4) attack detection modeling; 5) attack detection results and evaluation. At present, domestic and foreign researchers have done more research on the dimensionality reduction of network traffic data characterization and relatively little research on network traffic data sampling in intrusion detection [19]. The quality of network traffic sampling method directly affects the results of the detected attack [20].

Network attacks are quite extensive in today's Internet, from the network layer in the network protocol stack to the transport layer, and then to the application layer used by the user program. At present, network attack detection is mainly divided into abuse detection and anomaly detection.

1. Abuse Detection

Abuse detection, also known as the detection based on attack features or knowledge base, its working principle is to extract attack features from known network data attack packets, and sort these attack features into rules according to certain standards, and then grab network data packets for analysis. When a certain data packet analyzes some of the features or when it matches a rule in the detected rule base, the network attack detection system thinks that the network packet is an attack packet [21]. As long as the rules obtained from the analysis of network attack packets are added to the rule base of network attack detection system, the occurrence of network attack can be detected or prevented effectively. By analyzing the principle of abuse detection, it can be concluded that abuse detection depends on the rule base constructed by the system to some extent. Moreover, when the number of rule base in the system is large, the matching of rule base will be huge. Therefore, in the network attack detection method based on abuse monitoring, to improve the overall performance of the network attack detection system is mainly seen from two aspects. First, increase the rule base of network attack detection to improve the detection rate of attacks. Second, improve the performance of network attack detection algorithm. The principle of abuse detection is shown in Figure 4.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 08, August-2021

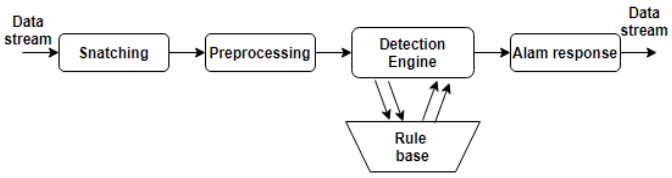

Fig. 4. The principle of abuse detection

2. Anomaly detection

Anomaly detection, also known as behavior-based detection method, whose working principle is to extract features from the captured network packets, and then analyze the features of the normal network data set. It primarily uses the algorithms in data mining to construct the normal behavior contour of network data, such as SVM, clustering algorithm, outliers algorithm and artificial immune algorithm, etc., if the data mining algorithm after processing deviates from the normal network data contour, the system will determine that the current network packet is an attack packet, and then make an alarm response and interception to the attack packet [22]. Theoretically, anomaly detection algorithm is mainly based on normal data. It is a major breakthrough in the field of network attack detection to solve unknown network attacks based on network data, because it does not need to build rule base or knowledge base according to network data packet, and it does not need to predict network attacks in advance.

However, the data mining algorithm used in anomaly detection is mainly for academic research. In engineering applications, it is greatly limited because of its high false negative rate and false positive rate. Most of the results are mainly focused on the detection of DDoS network attacks. The principle of anomaly detection is shown in Figure 5.

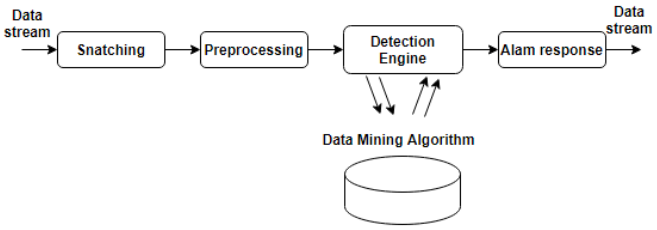

Fig. 5. The principle of anomaly detection

V. NETWORK SECURITY PROTECTION STRATEGY

The security problem in the network is becoming progressively serious [23]. Network attacks are quite extensive in today's Internet, from the network layer in the network protocol stack to the transport layer, and then to the application layer used by the user program [24].

3. Virus problems and countermeasures

In view of the various virus problems in the enterprise network, the enterprise has carried out the following measures.

1) Source of specification software: The enterprise has carried out the software legitimate processing, purchased the legitimate operating system and office software, and deployed anti-virus software. In order to minimize the vulnerability of each software in the system, all operating system software, application software and intermediate software of enterprises need to purchase genuine software. Through the services provided by these software providers, the vulnerability of software in the system can be updated in time to reduce the network security risk caused by software problems.

2) Reduce the influence range of virus: The enterprise network realizes the flat transformation. Each terminal is a VLAN, isolated from each other, to prevent the spread through the network. Through the use of VLAN technology, the IP address of each specialty and department is separated. VLAN technology allows the physical LAN logic of a network to be divided into different broadcast domains. The broadcast and unicast traffic within a VLAN is limited within the VLAN and will not be forwarded to other VLANs, which helps to control traffic, simplify network management and improve network security. VLAN is a protocol to solve the broadcast problem and security of Ethernet. It adds VLAN header on the basis of Ethernet frame, divides users into smaller working groups with VLAN ID, and limits the two-layer mutual access of users between different working groups. The advantage of VLAN is that it can limit the scope of broadcasting. It is a relatively mature networking specification. In enterprises, it can be used to divide the network into small networks. Enterprises can further monitor the network as long as IP conflicts occur, they can easily know which department (if VLAN Division is based on the enterprise department).

4. Network attack problems and Countermeasures

In view of the virus problem in the enterprise network, the enterprise refers to the external network technology to prevent network attacks to protect the enterprise network.

1) Install server firewall: Firewall is the simplest and most efficient way to prevent network attacks. Through the configuration of firewall, we can achieve fine-grained control of network access can be achieved to ensure that the network access is carried out as intended. Each server in the enterprise network is required to update the firewall immediately according to the corresponding firewall, so as to effectively prevent or resist network attacks [25].

a) Important data communication is confidential. All the data in the enterprise network must have encrypted transmission. IT personnel of the enterprise network are required to design the corresponding digital certificate and install the certificate when using the enterprise network, so as to ensure the security of the data. This encryption method can prevent hackers from attacking the enterprise network.

b) Use antivirus software. Enterprise network IT staff need to install anti-virus software in the host, and update the software constantly, so that the staff can find worms and trojan viruses latent in the enterprise network in time, so as to effectively resist and prevent network attacks [26]. IT staff need to update the virus database regularly and

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 08, August-2021

scan all computers in the enterprise network regularly. In order to avoid downloading known malicious programs and browsing malicious websites, security protection software (such as anti-virus software) can be installed. The enterprise can use the user terminal management system to manage the user terminals in the enterprise. The main purpose of user terminal management system management is to limit the user terminal, remote change and clear device content. For example, enterprises can manage sending short messages through the user terminal management system, and also require the user terminal to set a password, limit the length of the password, encrypt the files in the user terminal, and use software permissions.

c) Scan the whole network regularly. Because the operating system used by the server and host may have vulnerabilities, it is easy to be exploited and attacked by attacked. Therefore, it is necessary to find the existing vulnerabilities through network scanning software in time, and download patches to solve the problem. In particular, windows servers need to update and download patches in time.

2) Installation of intrustion detection system:

At present, the traditional Internet Gateway security solution is usually in the regional network access to the Internet gateway firewall, intrusion prevention system architecture. The malicious program attacks mainly rely on the host side to install anti-virus software to block, but today's malicious program attack methods are changing with each passing day, often using some clever methods or system vulnerabilities to shut down the host type anti-virus software from the core layer of the operating system, which brings serious losses to the enterprise, so there is the protection measures of the elucidating type anti-virus wall.

Intrusion Detection System (IDS), as an important defense against network attacks, undertakes the task of protecting computer security and ensuring the smooth operation of industrial enterprise networks and is an important research topic in information security [27]. Among them, anomaly detection is an important means of network intrusion detection by modeling network traffic characteristics to identify normal traffic and abnormal traffic in the network. By blocking the identified abnormal traffic in the intrusion detection system, passive defense against network attacks can be realized. At the same time, classifying abnormal traffic, analyzing different attack behaviors, and continuously improving the attack feature database by modeling attack methods can further improve the system's defense level [28].

Therefore, the research on network anomaly detection can be divided into the following two parts: (1) the identification of abnormal traffic; (2) the classification of traffic types, including normal traffic and attack types. At present, there are several methods of network attack in the network. For example, some weaknesses of the operating system have been discovered but have not been solved. Hackers will use the weaknesses of the operating system to attack the hosts in the network, that is, zero-time difference attack. Firewall can filter packets according to IP address or network communication port, but it doesn't have the ability to block illegal behavior using legitimate connections, because the firewall will not inspect the content in the packet. Thus, the defense mechanism plays an important role in preventing the formation of any threat to the network, such as the intrusion detection system, but this system rarely has the ability to prevent any attack on the network immediately. Therefore, intrusion detection system combined with firewall system to form a new system namely intrusion prevention system. This system works to prevent intrusion, filtering and blocking packets that belong to illegal activities. In addition, it can deeply check the network packets and find the attack characteristic code it knows, filter and discard the harmful network packets. The design of the intrusion detection system is divided as follows:

A. Design of a Network Intrusion Detection System.

A network intrusion detection system is installed in the protected computer network, and the original network message is used as the data source for analyzing the intrusion object. In the design of a network intrusion detection system, a network adapter is usually used for real-time monitoring and analysis of all data transmitted over the network; to design the data acquisition unit. The main function of the data acquisition unit is to get all the data about the intrusion event from the network. According to the network protocol, will transfer it to the analysis engine unit in the intrusion detection system after it is acquired and perform a detailed and comprehensive analysis to determine whether it is aggressive. In addition, the main function of the intrusion analysis engine module is to integrate with the computer network security database to perform security analysis on the information transmitted from the data acquisition module and transfer the results of the analysis to the configuration and management module. The main function achieved by the configuration and management module is to effectively manage the configuration work of other functional modules and inform the network administrator of the security analysis results transmitted from the intrusion analysis engine module efficiently so that the network administrator can do so in a timely manner. To provide a foundation, support, and countermeasures against intrusion. When the network intrusion system detects an attack, the corresponding functional unit will immediately respond to the intruder by alarm, broadcast, and disconnect, and send reminders to the user.

B. Design of Host Intrusion Detection System

The data sources of host intrusion detection systems usually include application logs, system logs, etc. The realization of its intrusion detection function is mainly through matching the content recorded in these audit record files with the attack content. If it does not match, it means that the intrusion object is not offensive. If it matches, the intrusion detection system will alert the network administrator in time and make corresponding protection actions simultaneously. Audit data records system user behavior information, and it must be ensured that it will not be modified or leaked during system operation. However, when the system is under attack, these data are likely to be modified or leaked. Therefore, the design of the host intrusion detection system must have a function; that is, the detection system completes the analysis

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 08, August-2021

of the audit data before being completely controlled by the attacker and sends it out in time. The alarm adopts certain protective measures. The host intrusion detection system has the advantages of accurately judging and accurately judging events at the computer network application layer according to the characteristics of different operating systems.

In brief, the research and design of intrusion detection systems is a critical link in dealing with computer network security issues. A good performance intrusion detection system can effectively make up for the deficiencies of firewalls and provide a reliable guarantee for the safety of computer networks. It is a relatively effective protection technology in modern network security measures. Although intrusion detection technology is still in the development stage, as society pays more and more attention to the design of computer network intrusion detection systems, the application scope and detection performance of intrusion detection systems will surely rise to a better level.

VI. CONCLUSION

With the rapid development of modern information technology, the application of Internet has gone far beyond the original design purpose, and has become a very important part of our life and work. However, network security has always been accompanied by the development of computer network. In the field of network security, network attack detection technology has always been a very important technology in computer network. To improve the security of computer network, we must take effective measures to solve the existing problems and create a secure network environment for users. This paper discusses an in-depth analysis and classification of network attack detection. The paper also offers network security protection strategy that may help interested future researchers.

REFERENCES

[1] N. Hoque, M. H. Bhuyan, R. C. Baishya, D. K. Bhattacharyya, and J. K. Kalita, "Network attacks: Taxonomy, tools and systems," *Journal of Network and Computer Applications*, vol. 40, pp. 307-324, 2014.

[2] R. Khan and M. Hasan, "NETWORK THREATS, ATTACKS AND SECURITY MEASURES: A REVIEW," *International Journal of Advanced Research in Computer Science*, vol. 8, 2017.

[3] Anderson and P.James, " Computer security threat monitoring and surveillance," *Technical Report, James P. Anderson Company*,1980.

[4] Heberlein, L. Todd, Gihan V. Dias, Karl N. Levitt, Biswanath Mukherjee, Jeff Wood, and David Wolber. A network security monitor. No. UCRL-CR-105095. Lawrence Livermore National Lab., CA (USA); California Univ., Davis, CA (USA). Dept. of Electrical Engineering and Computer Science, 1989.

[5] Sharma et al., "Network Attacks and Intrusion Detection System: A Brief," 2019 2nd International Conference on Intelligent Communication and Computational Techniques (ICCT), pp. 280-283, 2019.

[6] Farooqi, K. Ashfaq Hussain, and Farrukh Aslam, "Intrusion detection systems for wireless sensor networks: A survey," *International Conference on Future Generation Communication and Networking*, pp. 234-241, 2009.

[7] Godala, V. Sravanthi, and P. Rama," A study on intrusion detection system in wireless sensor networks," *International Journal of Communication Networks and Information Security*, vol. 12, pp. 127-141, 2020.

[8] Azeez et al., " Intrusion detection and prevention systems: an updated review," *Data management, analytics and innovation*, pp. 685-696, 2020.

[9] Y. Wu, D. Wei, and J. Feng, "Network attacks detection methods based on deep learning techniques: a survey," *Security and Communication Networks*, 2020.

[10] D. Liu, X. Liu, H. Zhang, W. Wang, X. Zhao, Y. Zhao, *et al.*, "Research on Network Attack Detection Technbology based on Reverse Detection and Protocol Analysis," in *2019 6th International Conference on Information Science and Control Engineering (ICISCE)*, 2019, pp. 490-494.

[11] L. Cao, Jiang, Z. Xiaoning, W. Yumei, Y. Shouguang, X. Dan, and Xianli, "A survey of network attacks on cyber-physical systems," *IEEE Access*, vol. 8, pp. 44219-44227, 2020.

[12] I. Ruban, N. Lukova-Chuiko, V. Mukhin, Y. Kornaga, I. Grishko, and A. Smirnov, "The method of hidden terminal transmission of network attack signatures," *International Journal of Computer Network and Information Security*, vol. 10, p. 1, 2018.

[13] N. Ravi, S.M. Shalinie, C. Lal, and M. Conti, " AEGIS: Detection and mitigation of TCP SYN flood on SDN controller," *IEEE Transactions on Network and Service Management*, vol. 18, pp. 745-759, 2020.

[14] de Almeida Neto, João Ribeiro, Layse Santos Souza, and Admilson de Ribamar Lima Ribeiro"Comparative Analysis between the k-means and Fuzzy c-means Algorithms to Detect UDP Flood DDoS Attack on a SDN/NFV," WEBIST, pp. 105-112, 2020

[15] A. Gupta and L.S. Sharma, " Detecting attacks in high-speed networks: Issues and solutions," *Information Security Journal: A Global Perspective*, vol.29, pp. 51-61, 2020.

[16] A. Thakkar and R. Lohiya, "Attack classification using feature selection techniques: a comparative study," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1-18, 2020.

[17] M. Ussath, D. Jaeger, F. Cheng, and C. Meinel, "Advanced persistent threats: Behind the scenes," *2016 Annual Conference on Information Science and Systems (CISS)*, pp. 181-186, 2016.

[18] Q. Zhu , " Research on road traffic situation awareness system based on image big data," IEEE Intelligent Systems, vol. 35, pp. 18-26, 2019.

[19] F. Salo, M. Injadat, A.B. Nassif, A. Shami, and A. Essex, , "Data mining techniques in intrusion detection systems: A systematic literature review, " *IEEE Access*, vol. 6, pp. 56046-56058, 2018.

[20] R. Atefinia and M. Ahmadi , "Network intrusion detection using multi-architectural modular deep neural network,"*The Journal of Supercomputing*, vol. 77, pp. 3571-3593, 2021.

[21] D. Yao, X. Shu, L. Cheng, and S J. Stolfo, "Anomaly detection as a service: challenges, advances, and opportunities, "*Synthesis Lectures on Information Security, Privacy, and Trust*, vol. 9, pp. 1-173, 2017.

[22] G. Fernandes, J. Rodrigues, L. Carvalho, J. Al-Muhtadi, and M. Proença, " A comprehensive survey on network anomaly detection, " *Telecommunication Systems*, vol. 70, pp. 447-489, 2019.

[23] Y. Ye, L. Yan, S. Ren, and Q. Zhang, "Research on network security protection strategy," in *2019 International Conference on Robots & Intelligent System (ICRIS)*, 2019, pp. 152-154.

[24] J. Raiyn, "A survey of cyber attack detection strategies," *International Journal of Security and Its Applications*, vol. 8, pp. 247-256, 2014.

[25] D. Shijie, Z. Zhiwei, and X. Jun, Xie, "Network security defense model based on firewall and IPS, "*Journal of Intelligent & Fuzzy Systems*, pp. 1-9, 2020.

[26] M.Z. Hasan, M.Z. Hussain, and Z. Ullah, "Computer Viruses, Attacks, and Security Methods, "LGURJCSIT, vol. 3, pp. 20-25, 2019.

[27] H. Liao, C. Lin, Y.Lin, and K. Tung, "Intrusion detection system: A comprehensive review,*" Journal of Network and Computer Applications*, vol. 36, pp. 16-24, 2013.

[28] M. Ahmed, A. Mahmood and J. Hu, "A survey of network anomaly detection techniques," *Journal of Network and Computer Applications*, vol. 60, pp. 19-31, 2016.