Review: Network Intrusion Detection Systems for Attack Detection and Prevention

Mohammad K. Abdul-Hussein
Al-Ma'moon University College, Department of Communication Engineering, Baghdad, Iraq.
Email: mohammad.k.abdul-hussain@almamonuc.edu.iq

Abstract

The use of the Internet has expanded well beyond its initial intended use and has become an essential component of both our personal and professional lives due to the fast growth of current information technology. However, the growth of computer networks has always gone hand in hand with the security of the network. The technology of Network attack detection has long been a crucial component of computer networks' network security. We need to implement operative solutions to the current issues and provide a harmless network situation for users to increase the security of computer networks. In-depth investigation and categorization for detecting network attacks are the focus of this paper. The topic of several issues caused by intruders and attackers is also covered. The report also provides a network security defense approach that can be useful to future scholars that are interested.

Keywords: Computer Network Attack (CNA), Network Intrusion Detection, Detection of Network Attacks.

1. Introduction

Since the use of the Internet was previously restricted to personal computers and laptops, it has significantly increased in scope thanks to the proliferation of tablets and smartphones. However, this rapid expansion was accompanied by an increase in electronic attacks and piracy, making information security a top priority for both individuals and institutions. Network assaults target systems and resources by taking advantage of security gaps and vulnerabilities in network information systems [1][2].

Network information systems are subject to several risks, many of which will evolve. From a broad perspective, these dangers can be separated into natural and man-made dangers. Natural risks include several types of catastrophes, severe site conditions,

electromagnetic interference, and the aging process of network equipment. Despite having no real aim, these dangers have the potential to harm the network communication system and jeopardize communication security. Man-made threats are also man-made assaults on network information systems that aim to steal, falsify, or otherwise alter data and information by seeking vulnerabilities in the system. In comparison to the other two, well-designed man-made assault threats are more diverse and numerous, making them harder to defend against [3].

IoT system intrusion detection is a difficult undertaking owing to the conditions and procedures of IoT strategies. Therefore, to meet the main security concerns and security risks, the area of systems for intrusion detection in Internet of Things systems is necessary to be studied and to be worked on. Detailed information on IDS topics is offered in this review, along with tips for identifying limits and minimizing them.

2. Related Works

In [4] C. Karuppanchetty et al., employed intentionally created payloads to train and test the system. The efficiency of the IDS in classifying regular traffic is also tested, as is the impact of disregarding the cookie component of the payloads of HTTP/TCP/IP packets. The outcomes demonstrated the viability of an enhanced training approach that ignores cookies and makes use of simulated traffic. The processing expense of the cookie stripping technique and the IDS algorithms themselves both contribute to the quantified worst-case delay.

In [5] A. Fadlallah et al., explored the use of Intrusion detection and prevention systems' attack graphs to more effectively recognize difficult assaults founded on models which are predetermined, setups, and warnings. An application is created as a "proof of concept" that integrates with interference detection system SNORT intrusion detection system and compares the warnings with a graph of an attack produced by the scanner NESSUS (which is kept current using the National Vulnerability Database (NVD)) and group library for the attack graph. Through the

using the tool, attackers' actions can be monitored as they progress through the attack graph's various phases.

In [6] H. Moudnia et al. , employed the ANFIS and PSO algorithms in combination for optimization to identify and stop the assault which is called a black hole. The constraints which are inputted for this method are computed from a mobile ad hoc network database that has been retrieved by building a table that registers all of the neighbor's actions. Experimental findings show that our method has a high rate of detection and a low number of false alarms.

In [7] S. Tahir , et al , adopted a solution to detect intrusion, and this solution is for the IoT's Active Sinkhole Routing Attack (PASR). By segmenting the network into IoT clusters, PASR was able to overcome the problem of the sinkhole attack. Every IoT device is linked to its corresponding gateway. A mechanism for detecting intrusions is installed on the gateway devices. An intrusion analyzer is activated by the intrusion detection system to look for abnormalities in the environment for the protocol of the on-demand ad hoc distance vector. The base position serves as the primary device for collecting data from all other devices. Because of this, it recognizes and stops sinkhole attacks, and the base station maintains track of all active devices and their potential linkages. Implementation of the PASR and comparison with the current.

In [8] B. Sinha, et al , presented a system based on fuzzy logic that is capable of accurately detecting intrusion activities inside of a network. Since the suggested fuzzy logic-based system has a superior set of rules in its rule base, it may be able to identify network intrusion behavior. Their article investigated the use of an appropriate model and fuzzy logic for network intrusion detection. The proposed model has been examined after testing against the campus' actual live networking environment.

In [9] O. J. Mebawondu, et al . proposed an information gain-based, lightweight IDS that uses many layers of perceptrons. Before classifying traffic using a neural network, the gain ratio was utilized to choose pertinent characteristics for attacks and regular traffic. The lightweight IDS is appropriate for real-time intrusion

detection based on empirical findings from the UNSWNB15 intrusion detection dataset on thirty chosen qualities, which is a highly rated choice.

In [10] H. Alamsyah et al . , deployed IDPS network security to directly detect and prevent various attack risks. The Intrusion Detection and Prevention System is a technique that may be applied (NIDPS). NIDPS can trade and repel the assaults. IP Tables worked in conjunction with this security mechanism. To filter incoming data packets and discard those that the assault has identified, IP Tables are employed. With the help of the intrusion detection and prevention system, it is possible to identify assaults and stop them by blocking data packets supplied by attackers via telnets, FTP attacks, and port scanning.

In [11] J. Man and G. Sun suggested a method for detecting network intrusions based on residual learning. The use of residual blocks in deeper convolutional neural networks is developed to acquire extra important characteristics after converting the UNSW-NB15 data set into pictures. The class difference issue in the training set is detected using the modified specific loss function, which is calculated instead of the cross-entropy loss function to detect in the set of testing small assaults. The model is improved by using To avoid overfitting, use batch regularization, and global average pooling. According to experimental findings, the suggested model can increase the accuracy of attack detection when compared to current models.

In [12] M. Ghurab , et al . , estimated and compared several machine learning (ML) techniques to identify distinct sorts of assaults on the NSL-KDD dataset. According to their accuracy for various types of attacks, the experiment's classifiers K Nearest Neighbors (KNN), Random Forest (RF), Extra Trees (ET), and Gradient Boosting (GB) were compared. According to the experiment's findings, the KNN method outperformed other classifiers for U2R in terms of accuracy.

In [13] K. Kotecha et al., worked with the UNSW-NB15 Dataset, one of the greatest representations of contemporary assaults at the moment and one that offers several models. We explore many models before settling on the one that performs the best when various assessment indicators are used. A thorough data analysis of the dataset's characteristics utilizing our knowledge of correlation, variance, and related

aspects is conducted in addition to modeling to improve modeling. Additionally, speculative considerations for possible network intrusion detection systems are explored, along with recommendations for prospective modeling and dataset development.

In [14] A. S. Jaradat et al. suggested a machine learning-based methodology for classifying and detecting intrusions. The model initially obtains the data set and formats it appropriately before doing feature selection to identify a subset of features that merit consideration. The Konstanz information miner then processed the revised data set (KNIME). Three alternative classifiers were used to improve performance and conduct a fair comparison analysis. Using datasets from (CICIDS2017), the predicted classifiers have been run and evaluated using the KNIME analytics platform. The results of the trial showed an accuracy rate that varied between (98.6) as the maximum achieved and (90.59%) as the regular, which was pleasing in comparison to previous techniques. The figures gathered from this study motivate researchers in this sector to employ the learning of machines in the analysis of data and cyber security to generate more accurate detection systems for intrusion.

In **[**15] E. AlshahraniI et al., generated adversarial samples at random using the GAN model for both evasion and poisoning assault scenarios. In evasion attacks, these created samples will go unnoticed by machine learning classifiers, and in poisoning attacks, they will interfere with training. The CICIDS2017 dataset has been used in experimental work. The findings demonstrate that in actual assault situations, the effectiveness of the suggested evasion and poisoning attacks had an impact on the decision tree and logistic regression models' accuracy.

3. Computer Network Attack (CNA)

The world is becoming increasingly linked to Computer N.N occupied with the development of the Internet and newfangled technology of networking. In Worldwide, the present is a lot of private, business, fighting, and governmental data on the infrastructure of networking. Whether they are big, small, or government entities, many companies are impacted by network security. An intrusive party can

cause a variety of harm if network security is compromised. Because of this, users need to be informed about network security and various network threats [16].

An organization's network can be attacked to steal information, acquire illegal access, or carry out other nefarious actions. Network attacks often fall into two categories:

- **Passive Attacks:** Traffic analysis, eavesdropping, and monitoring are some examples of passive assaults.
  - **a. Traffic analysis**: An attacker uses a traffic analysis attack to try to determine the sender and receiver's communication channels. A hacker can determine how much data is sent by looking at the source and receiver's paths. The traffic analysis does not alter the data in any way.
  - **b. Eavesdropping**: The mobile ad hoc network was the target of this passive assault. This attack's primary objective is to extract some sensitive or secret information through communication. The sender's or receiver's private or public key, as well as any other secret data, may be included in this information.
  - **c. Monitoring**: In this assault, the attacker can access private information, but he cannot change it[17] [18][19] .
- **Active Attacks:** Attackers alter data by destroying, encrypting, or doing other harm to it in addition to gaining illegal access to it. Attacks such as spoofing, wormhole, development, denial of service, sinkhole, and Sybil are currently active.
  - **a. Spoofing:** sending changes when a nod of malicious presents his identity incorrectly in the topology.
  - **b. Modification**: The communication is sent through a long route by the sender. when a rogue node modifies the routing path in some way. The sender and recipient experienced a communication delay as a result of this assault.
  - **c. Wormhole:** It is also known as the tunneling assault. In this attack, a packet is intercepted by an attacker at a single point, who then shafts it to a second

hostile network node. Therefore, a novice presumes that has located the network's shortest path.

d. **Fabrication:** Untrue routing messages are produced by malevolent nodes. In other words, it produces inaccurate information regarding the path among devices [18].

e. **Denial of services**: In a denial of service bout, a nod of malicious node transmits the communication to the node which is the target and uses up the bandwidth of the network. The rogue node's primary objective is to occupy the network node. When an unauthenticated node sends a message, the receiver will not receive it because he is otherwise occupied, forcing the beginner to wait to respond to the receiver.

f. **Sinkhole**: As a result of this service attack, the base station is unable to get accurate and comprehensive information. A node engages in this assault by attempting to draw data from all nearby nodes to itself. This attack allows for the selective alteration, forwarding, or discarding of data.

g. **Sybil:** The numerous replicas of malicious nodes that are connected to this assault. A hostile node exchanging its key secretly with other nodes of malicious might result in a Sybil attack. As a result, there are more malicious nodes in the network, increasing the likelihood of an attack. The likelihood of a malicious node choosing a path in the network will rise if we employ multipath routing [19].

- **Advance Attacks**

a. **Black Hole Attack**: this is a more sophisticated attack in which the attacker advertises that it has the finest route to the packets of the node that it intends to capture via the routing protocol. A hacker produces a response message stating that he has the straight way to the recipient after listing the initiator's request for a route using the flooding-based protocol. The initiator will believe that this message from the hacker is the quickest way to the recipient because

it arrived before the response from the real node. to build a harmful phony route.

b. **Rushing Attack**: When a packet is sent from the sender to the receiver during a rushing assault, the attacker modifies the packet before sending it on to the recipient. The attacker duplicates the action and repeatedly transmits the replica to the recipient. The receiver is always active because it believes that packets are coming from the sender.
c. **Replay Attack**: The rogue node might recurrence or postpone data in this attack. The source can accomplish this by intercepting and retransmitting the data. At that point, a hacker might get the password.
d. **Byzantine Attack**: Between the sender and receiver, a group of intermediary nodes performs a variety of operations that interrupt or degrade routing services, such as generating routing loops, sending packets down inefficient paths, or selectively discarding packets.
e. **Location Disclosure Attack**: By calculating and observing the traffic, a malicious node gathers data about the node and the path. Therefore, hostile nodes might carry out more network assaults [20] .

4. Network Attacks and Internet

Since the Internet's inception, networks have been attacked. Using the findings of the target network's scanning, network attackers create malicious network packets that are then sent directly or indirectly by proxy to the target network. Of course, there are instances where the packet is inoffensive, but when the flow of the network package is excessive, it overloads the server or device network, quickly depletes the system's hardware resources and eventually prevents the server or network device from responding to the standard admission. In another situation, the assailant makes use of devices and software that may examine, remove, or delay the data transmission on the target network. The server's hardware is outdated, and its power of processing and performance is in no way dissimilar to those of the network at the initial stages of development. Due to this, network attackers find it challenging to

access the target network using their personal computers. Instead, they use the resources of the target network to devour, spoil, and paralyze security flaws. And as a result, such resources are rendered ineffective against any attack. Through agent channels, network attackers employ software of malicious to take governor of the network's other machines. The software of malicious is created the attack packet of the network and transmits it to the intended network host while these control machines get the instruction to attack from the assailant [21].

When a network is attacked in this manner, it is challenging for us to identify the perpetrator. The intensity of network attacks is also quite high since attackers may manage a lot of hosts with malicious software. Early on in the evolution of computer networks, the dependability of computer-to-computer communication was taken into account by protocol designers, who created the TCP/IP_ Five-layer protocol of network (Application) by the network transmission chain of command. Data is first encapsulated at the application layer, then transferred to the transport layer where it is converted to TCP or UDP packets, then to the layer of the network where it is converted to IP_ datagrams, then to the link_ layer where it is converted to MAC_ frames, and finally to the physical layer where it is sent to the network card to be sent to other computers [22].

5. Network Attacks and Communication

Although this architecture is a useful way to communicate between computers, network attackers discovered various gaps in the computer network protocols after studying the network protocol in detail. Currently, there are several varieties of network assaults, which may be categorized as follows:

1. **Denial of Service Attack_ TCP "SYN":** The founding host sends a message from SYN to the object host, and after receiving the syn message, the target host replies with an ACK message before waiting for the initiator. This is how a TCP network connection is established in typical network communication. Following receipt of the message, the initiator responds to the target host with an ACK

message, and a full connection is made [23] [100], Figure (1) shows a Denial of service attack using the SYN flood

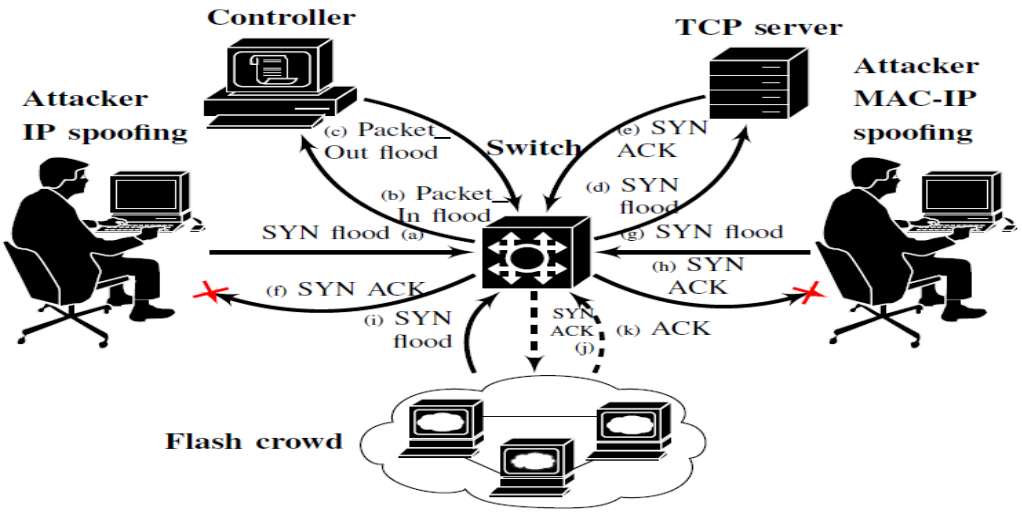

Figure (1): Denial of service attack using the SYN flood [23].

2. **ICMP flood attack:** Network protocol designers utilize tools like the ping and traceroute programs to detect other hosts via the network to see if they are operating properly. The majority of these apps send ICMP messages, to which the computer receiving the message responds with an ICMP-echo message. A large number of controlled machines are used by network attackers to send these signals, which hinder the target network host from processing ordinary network traffic because it is too busy processing ICMP packets [24].
3. **UDP Flood Attack:** Similar to an ICMP flood attack, network attacks work on the same principles. Network attackers bombard the target system with many UDP network packets, preventing it from processing regular network data because it is too busy processing UDP packets [24]. Figure (2) shows the UDP flood attack

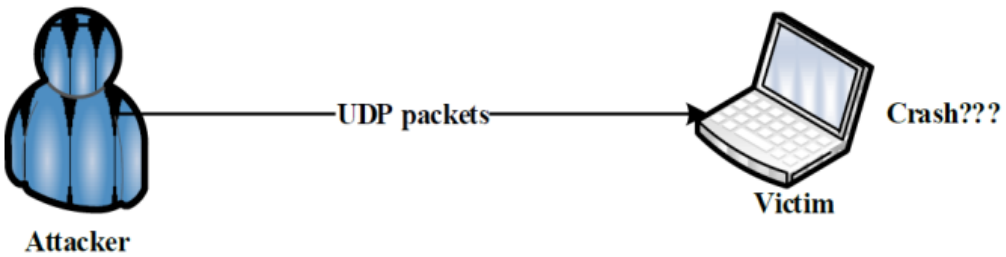

Figure (2): UDP flood attack [24]

4. **Port Scan Attack:** A computer will have two options when it gets a connection request message, or an SYN message, following the network transmission protocol. If a port_in an equivalent to demand is open, then the computer is replied to the data message of SYN and ACK and creates a connection of TCP; if the port_in an equivalent demand is closed, the computer is replied to a data message of RST and informs the initial request that the port is in the computer is closed. The three-way handshake is depicted in the following table [25]

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

Table 1: TCP response to flag packets [25].

5. **IP Fragment Message Attack:** The IP protocol will collect the network's MTU to transport a big IP message over a computer network. The big IP message will be split by computation after the MTU has been obtained. The fragment will also have a simultaneous numbering of the identifier and slice offset [26]

6. Requirements for Optimal Intrusion Detection Systems (IDS)

Several requirements are derived from studying many works of literature, and they are:

- **Response Optimality for Attack:** It is argued that the challenge of selecting the best reaction attack is a choice issue by taking a look at the computing complexity of choosing the best response assault.
- **Monitoring the Network:** It needs to operate continuously without human oversight. The system needs to be dependable enough to function behind the scenes of the system under observation. information that serves as a record of witnessed events. Information may be transferred to other systems, such as

corporate managing systems and centralized logging servers, although it is frequently logged locally.

- **Analysis of Stateful Protocols**, It searches for discrepancies between established profiles of commonly recognized descriptions of appropriate protocol behavior for every level of the protocol. In contrast to anomaly-based detection, which needs host- or network-specific profiles, analysis of stateful protocol relies on vendor-developed universal profiles that specify how particular protocols should and should not be used. It can identify many attacks that other techniques cannot because it can comprehend and track the protocols stat that requires a sense of state. Stateful protocol analysis has several drawbacks, including the need for a lot of resources, the inability to identify assaults that do not go against the rules of commonly satisfactory protocol performance, and the difficulty or impossibility of developing correct models of protocols.
- **Upholding Intrusion Regulations:** Users should be able to enforce intrusion rules using the IDPS tool. These rules specify which sort of activity constitutes an incursion and which does not base on constantly updated threat data. The rules may be pre-configured and handled by the provider depending on the tool you use, which is a low-effort but rigid method. Configurable rule sets provide users with more control but take more work to implement.
- **Activity Records Analysis:** The technique of comparing definitions of what behavior is typical with observable occurrences to spot noticeable departures from the norm is known as anomaly-based detection. The usual behavior of entities like users, hosts, network connections, or applications is represented by profiles in an IDPS that uses anomaly-based detection.
- **Tracking Suspicious Behavior:** It is becoming more crucial to update the database with new signatures or to characterize typical patterns and behaviors. Attacks are happening more often, which is driving this trend, and the system that has to be secured is becoming more dynamic. When it comes to web

servers, a change in the hosted material may also necessitate the need to retrain the system with fresh data. To do this, the training may be guided by a website's ontological model that is built on both independent algorithms and input from content creators. When training is conducted using both fictional and actual traffic, this strategy can be extremely helpful.

- **The systems' features that are specialized to certain applications:** IDS deployment should be optimized, and their detection levels should be tuned to maximize security while reducing losses.
- **Blocking Malicious Activity:** A blacklist is a collection of distinct objects, such as hosts, UDP or TCP port_ numbers, ICMP_ types, software programs, usernames, URLs, names of the file, or extensions of the file, these collections that earlier shown to be connected to harmful behavior. Blacklists often referred to as hot lists, are frequently used by IDPs to identify and prevent behavior that is very likely malicious. They may also be used to give alarms that counterpart blacklists items to get greater priority. Some IDPs produce blacklists dynamically that are used to momentarily threats of blocky that have just remained discovered (such as the IP address activity of an assailant). A whitelist is a collection of distinct things that are thought to be good. Whitelists are often used to limit or disregard false positives for recognized benign conditions behavior from hosts trusted on a grainy level. The most popular applications of whitelists and blacklists are stateful protocol analysis and signature-based detection.

7. Conclusion

There are numerous different safeguards to lessen the danger of business users exposing sensitive information because The conventional network gateway firewall hasn't been able to successfully thwart every attack type. These techniques include intrusion detection systems and anti-virus walls, but each has its protection limitations. The idea of this paper is to review in_ depth the functional protection

for the network, which is described by using protection and filtering layer-by-layer to develop the level of security. Several requirements derived from studying are recommended to be followed, and they are: Response Optimality for Attack, Monitoring the Network, Analysis of Stateful Protocols, Upholding Intrusion Regulations, Activity Records Analysis, Tracking Suspicious Behavior, The systems' features that are specialized to certain applications, and Blocking Malicious Activity. These requirements are recommended to be followed to achieve three fundamental information security requirements: Confidentiality, Integrity, and Availability. Each piece of protective gear carries out its functions to block and filter, which can successfully stop attacks from happening.

References

[1] N. Hoque et al . , "Network attacks: Taxonomy, tools and systems," Journal of Network and Computer Applications, Vol. 40, pp. 307-324, 2014.

[2] R. Ismael Farhan, A. Tariq Maolood, and N.Flaih Hassan, “Performance analysis of flow-based attacks detection on CSE-CIC-IDS2018 dataset using deep learning”, Indonesian Journal of Electrical Engineering and Computer Science Vol. 20, No. 3, pp. 1413~1418, 2020.

[3] R. Khan and M. Hasan, "Network Threats, Attacks And Security Measures: A Review," International Journal of Advanced Research in Computer Science, vol. 8, 2017.

[4] C. Karuppanchetty et al , “Artificially Augmented Training for Anomaly based Network Intrusion Detection System”, I. J. Computer Network and Information Security, 2015, 10, 1-14. DOI: 10.5815/ijcnis.2015.10.01.

[5] A. Fadlallah, H. Sbeity, M. Malli , and P. Lteif , “Application of Attack Graphs in Intrusion Detection Systems: An Implementation” International Journal of Computer Networks (IJCN), Vol. 8, Issue 1, 2016

[6] H. Moudnia, M. Er-rouidib, H. Mouncifc , B. El Hadadia “Black Hole attack Detection using Fuzzy based Intrusion Detection Systems in MANET”, International Workshop on Web Search and Data Mining (WSDM), 2019.

[7] S. Tahir , S. Tahir Bakhsh and R. A Alsemmeari, “An intrusion detection system for the prevention of an active sinkhole routing attack in the Internet of things” International Journal of Distributed Sensor Networks 2019, Vol. 15, 2019. DOI: 10.1177/1550147719889901

[8] [18 August 2019.] Bhawna Sinha, S.S. Sahay, and Braj Kishor Prasad " Fuzzy Logic And Network Intrusion Detection System", International Journal of Development Research · August 2019. URL: https://www.researchgate.net/publication/335227752

[9] [24 July 2020] Olamantanmi J. Mebawondu, 2Olufunso D. Alowolodu, 3 Jacob O. Mebawondu and 4Adebayo O. Adetunmbi, "Network Intrusion Detection System using Supervised Learning Paradigm", Scientific African (2020),
DOI: https://doi.org/10.1016/j.sciaf.2020.e00497

[10] H. Alamsyah, Riska, and A. Al Akbar, " Network Intrusion Detection and Prevention System ", Journal of Information Technology and Computer Science, Vol. 5 , No. 1 , pp. 17 - 24 , 2020.

[11] J. Man and G. Sun, " A Residual Learning-Based Network Intrusion Detection System ", Hindawi, Security and Communication Networks, p. 9, 2021. https://doi.org/10.1155/2021/5593435

[12] M. Ghurab , R. Alshamy, and S. Othman, "Performance Evaluation for Attack Detection in Intrusion Detection System", International Journal of Scientific Research and Engineering Development—Vol. 4, Issue 5, 2021.

[13] K. Kotecha, R. Verma, P. V. Rao, P. Prasad, V. Kumar Mishra, T. Badal, D. Jain, D. Garg, and S. Sharma, "Enhanced Network Intrusion Detection System" Sensors 2021. https://doi.org/10.3390/s21237835

[14] A. S. Jaradat, M M. Barhoush, R. Bani Easa, " Network intrusion detection system: machine learning approach", Indonesian Journal of Electrical Engineering and Computer Science Vol. 25, No. 2, pp. 1151~1158. 2022. DOI: 10.11591/ijeecs.v25.i2.pp1151-1158

[15] E. AlshahraniI, D. Alghazzawi , R. Alotaibi , and O. Rabie, **"** Adversarial attacks against supervised machine learning based network intrusion detection systems ", PLOS ONE , 2022.

[16] G. Kumar , A. Kaur , S. Sethi, "Computer Network Attacks - A Study" International Journal of Computer Science and Mobile Applications, Vol.2 , Issue. 11, pp 24-32, 2014

[17] K. Gupta and P . Kumar Mittal, "An Overview of Security in MANET" , International Journals of Advanced Research in Computer Science and Software Engineering, Vol. 7 , Issue-6, 2017 . DOI: 10.23956/ijarcsse/V7I6/0254

[18] A. Joshi and W. Li. "Security Issues in Mobile Ad Hoc Networks- A Survey", 2008.

[19] A. Ghaffari, "Vulnerability and Security of Mobile Ad hoc Networks", Proceedings of the 6th WSEAS International Conference on Simulation, Modelling and Optimization, 2006

[20] M. V. Pawar , J. Anuradha, “ Network Security and Types of Attacks in Network” , International Conference on Intelligent Computing, Communication & Convergence (ICCC-2014) .

[21] 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.

[22] 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.

[23] 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.

[24] D. Almeida Neto, J. Ribeiro, L. Santos Souza, and A. Ribamar Lima "Comparative Analysis between the k-means and Fuzzy c-means Algorithms to Detect UDP Flood DDoS Attack on a SDN/NFV, pp. 105-112, 2020

[25] 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.

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