Computer Network Intrusion Detection: Principles and Techniques

Preprint · December 2024

DOI: 10.13140/RG.2.2.25112.71683

Davoud Yousefi Shishehgaran
Ardabil University of Medical Sciences

Computer Network Intrusion Detection: Principles and Techniques

Amirhossein Rakhshani, Davoud Yousefi

Department of Computer Engineering, Ardabil Branch, Islamic Azad University, Ardabil, Iran

Abstract

With the rapid growth of information technology and the widespread use of computer networks, network security has emerged as one of the most important and challenging topics in this field of management. Intrusion detection systems have been developed to mitigate software security vulnerabilities, ensure information security, and enhance efficiency in computer networks. In the realm of network security, access control and timely attack detection are significant research topics. The aim of this paper is to review and provide an overview of intrusion detection systems, starting with an introduction to related concepts and the background of research conducted on intrusion detection systems; it includes a review of network-based intrusion detection systems, social networks, signatures, and anomaly detection.

Keywords: intrusion detection, network attacks, computer network, social network

Introduction

With the increasing use of the internet, a large volume of information is exchanged between various communication devices. Data must be securely transmitted between these devices, and therefore, network security has become one of the predominant research areas for the current network scenario. Consequently, intrusion detection systems (IDS)[1] are widely used alongside other security mechanisms such as firewalls and access control. On the other hand, the evolution of attack scenarios has made it a significant challenge to find efficient and optimized intrusion detection systems that can keep up with frequent updates. Despite the use of intrusion detection systems (IDS) to identify various attacks, the number and complexity of unknown cyberattacks have increased. This has led to the distribution and heterogeneity of applications complicating

[1] . Intrusion Detection System

and challenging network services. Intrusion detection systems (IDS) are a crucial defensive mechanism for the vulnerable points of computer networks [2, 4].

Since it is practically impossible to create computer systems without vulnerabilities and security failures from a technical perspective, intrusion detection is pursued with particular importance in computer system research. Intrusion detection systems, which are used to monitor abnormal activities in networks, have attracted significant attention from researchers in recent years, and various models have been designed and proposed to identify and prevent attacks and ensure security. The fundamental goal of information security is to prevent unauthorized access, use, disclosure, disruption, modification, or destruction [6, 8]. To prevent and detect malicious attacks on computer networks, factors such as information tracking, monitoring alerts, installing and deploying intrusion detection tools, and supervising and controlling user behavior by reviewing log files and receiving timely alerts in the event of security breaches should be taken into account. The goal of an intrusion detection system is not to prevent attacks but to discover and potentially identify attacks and detect security flaws in the system or computer networks and inform the system administrator. Generally, intrusion detection systems are used alongside firewalls and serve as complementary security measures for them. Intrusion detection systems are recognized as one of the main components of security infrastructure in many organizations. These systems consist of a set of hardware and software models and patterns that automate the monitoring processes of computer system events [10, 12]. Intrusion detection systems examine and analyze network events to address security issues in computer systems and networks. These systems aim to identify user activities that can be categorized as either normal or anomalous, designed by specialists and experts through the comparison of network transactions based on known patterns. Another capability of intrusion detection systems is the ability to detect unusual traffic from outside to inside the network and to notify the network administrator or to terminate suspicious connections. In general, there are two types of intrusion detection systems: misuse detection systems and anomaly detection systems. In misuse detection systems, the system is aware of the overall structure of attacks and has specific patterns for various types of attacks, which allows it to prevent intrusions into the system or take necessary actions to counteract intrusions. However, in anomaly detection systems, only the correct and normal behavior of the user is known, and its information and characteristics are available to the system. Therefore, the goal in these systems is to identify abnormal behavior that may indicate an attack or intrusion. Overall, there are three major security concerns that exist for network security [14]:

- Data Confidentiality: Information transmitted over the network should only be accessible to authorized individuals. Breaching confidentiality allows unauthorized individuals to access the information [16].

- Data Integrity: Data integrity must be maintained from the time of transmission until the time of receipt. The loss of data accuracy means that the information has been altered during transmission over the network from the source to the destination [18].

- Accessibility: The services provided by the network must always be available. Due to data loss or denial-of-service attacks, the services offered by the network may not be accessible [20].

Research Background

The foundation of network-based intrusion detection systems is the dataset used for training and testing the models. To this end, various datasets have been introduced and utilized over the years.

MIDAS is an expert system implemented using P-Best and LISP in 1988. In the same year, Haystack was also implemented, which aimed to reduce audit overheads using statistics. In 1989, it was implemented as an anomaly detector based on statistics that generated rules through statistical analysis and then used those rules for anomaly detection [1, 3]. In 1990, Heberlein initially proposed the idea of a network intrusion detection system, developing network security monitoring and hybrid intrusion detection systems. An expert system for intrusion detection named SRI was presented, which included two approaches: a rule-based expert system and a statistical anomaly detector that was implemented on the workstations of Sun Microsystems, capable of analyzing data at both the user and network levels. In 1991, a distributed intrusion detection system was developed, which included an expert system created by researchers at the University of California, a statistical anomaly detector named NADIR, and an expert system implemented by Los Alamos. A common point that generally occurs in attacks on these networks is the presence of DoS, DDoS, SQL Injection, MITM (Man-in-the-Middle), Brute-Force attacks, and similar types. Therefore, in the cases examined, we do not continuously refer to attacks, as it is outside the discussion; rather, we mention only the type of method used in the system and, in some cases, provide a critical perspective on the method and, in others, the advantages of the method [5, 7]. A comprehensive explanation of the attack methods in a cloud computing system is something that cannot be covered in a seminar, and should be addressed in its foundational discussions and elaborated upon in a complete thesis. In 1998, the Lawrence Berkeley National Laboratory introduced a scripting language called Bro for analyzing packets from the libpcap dataset [9]. In 2001, tcpdump was utilized in the analysis of audit data and intrusion detection systems to create rule profiles for classifications. Following this, three innovative methods that utilize a specific type of intrusion detection systems in cloud environments will be reviewed. In [11], a novel method for intrusion detection systems in mobile networks, particularly in ad-hoc networks and cloud computing networks, is presented. The methodology of this research employs Bayesian classification with the formulation of game theory. Reducing energy consumption during intrusion detection and improving accuracy in identifying and detecting attacks and various intrusions are among the most significant achievements of this research. In [13, 28], a system for intrusion detection aimed at identifying and detecting distributed denial-of-service attacks is presented. The distributed denial-of-service attack in a cloud environment is uniform, and identifying and detecting it is considered extremely challenging. In [15, 30], a statistical wave classification for detecting attacks using an intrusion detection system in cloud computing has been presented. In article [17, 32], a comprehensive review of the types of introduced datasets and their advantages and disadvantages has been conducted. It discusses the first network-based datasets that have been used for intrusion detection systems. The international knowledge discovery and data mining dataset is KDD CUP99, which was collected and produced from network traffic by the Intrusion Detection Systems Evaluation Program project known as DARPA in 1998. Although this data set has been widely used as a benchmark for evaluating intrusion detection systems, the existence of duplicate records that cause the exploitation of algorithms towards frequent attacks is its biggest flaw. To fix this data set, another data set named NSL-KDD Network Security Laboratory data set has been adapted from it. In the article [19, 34]. A technique has been introduced that can find the effects of attacks on network data more quickly based on the effect of signatures of known attacks. In this method, compared to the a priori signature effect method, progress has been achieved in terms of speed. Considering that in these methods, a lot of time is spent on searching the database, so in this article, a new method is proposed to shorten the time of searching the database. The proposal of using a deep learning approach to implement and develop network-based intrusion detection systems is presented by the article [21, 22]. In this proposal and study, the NSL-KDD network security laboratory dataset is used for evaluation. Following this path, the article [23, 36] presented a new deep learning technique for intrusion detection system. In this research, asymmetric deep auto encryption (ADAE) is used for unsupervised feature learning. With this method, significant progress has been achieved in the evaluation parameters compared to other proposed methods. In the article [24, 39], one of the famous network attacks called SYN-Flood is discussed.

This attack disrupts the normal functions of the network by consuming network resources [20, 25]. In the article [2, 26] entitled "A new method of light-weight intrusion detection for computer networks", applying the attraction operator of the colonial competition algorithm to the genetic algorithm, a new method for selection the optimal features are presented in the intrusion detection system [27]. The proposed method of decision tree classification by Barosh has been tested on the KDD99 dataset, which shows an increase in the detection rate (95.03%), a decrease in the false alarm rate (1.46%), and also an increase in the convergence speed. (3.28 seconds). Therefore, in this research, we will review the types of intrusion detection systems that are most used in computer networks by paying attention to the theoretical foundations [29, 31].

Theoretical foundations

1. Types of network attacks

In the past years, many attempts have been made to classify attacks. One of the classifications accepted by the majority classifies attacks into the following four groups [21]:

• Port scanning attacks: attacks that are based on obtaining information about the system to advance penetration [33].

• Denial of service attacks: Dos attacks that try to disrupt the use of a system or services for legitimate users by causing a small or complete interruption [35].

• User attacks to the root (: (U2R) attacks whose goal is to gain the access level of the main administrator of the system by using the existing vulnerabilities in the operating system or applications [37].

• Remote attacks (R2L) are attacks based on gaining local access outside the internal network [3].

2. Intrusion detection systems

In general, IDS can be divided into two general categories:

- Network intrusion detection systems: in many cases, they are practically "sniffers" that look for attempts to attack by examining packets and protocols, and monitor traffic in real time on communication lines. In other words, the standard of NIDS is only the packets that are exchanged on the networks. However, these systems lose their efficiency when faced with encrypted packets or networks with high speed and traffic like Snort software in Linux operating system [38].

- Snort software: It is an open-source software for intrusion detection and prevention; which is written in C programming language. It was created in 1998 by Martin Roach and is currently being developed by the developers of Sourcefire, a subsidiary of Cisco. This software was recognized as the best open-source software in 2009. It is a free product with a functional database that can be installed and used on operating systems such as Windows, Linux, Unix and Mac. Rules updates are available for free [39].

Snort software examines the traffic on the network and system immediately. This software can be used in 3 modes:

1.2. Sniffer mode: In this mode, Snort eavesdrops on network traffic.

2.2. Packet recording mode: In this mode, a report of detected traffic is prepared in listening mode.

3.2. Intrusion detection mode: In this mode, network intrusion and attack are detected and the incoming traffic is checked based on the rules created by the user [44,51].

Intrusion is also the set of illegal actions that compromise the integrity, confidentiality or access to a resource. Intrusions are divided into the following categories:

1. Illegal entry: Illegal entry occurs when an outsider gains access to a valid user ID and password. 2. Impersonation attacks: Impersonation attacks occur when an intruder convinces the system that he is an authorized user with high privileges. 3. Security control: The intruder tries to modify the security aspects of the system such as passwords. 4. Leakage: Information is transferred outside the system. 5. Denial of service: Resources become unavailable to other users. 6. Malicious use: This category of intrusions includes different attacks such as deleting files, misusing resources, etc. Malware software evaluation poses a critical challenge for the design of intrusion detection systems. Malware attacks have become more complex and have created many challenges to detect unknown and obscure malware, so malware designers use various evasive methods to obtain information in order to avoid detection by an IDS [40]. In addition, an increase in threats there is security like zero-day attack designed for target internet users; Therefore, computer security has become necessary to use information technology, which has become a part of our daily life [41].

1.2. Host-based intrusion detection systems (HIDS)

These systems are responsible for identifying and detecting unauthorized activities on the host computer. Host-based intrusion detection systems can detect attacks and threats such as file access, Trava horses, etc. on the host computer. Host-based intrusion detection systems run only on the host computer or individual computers and do not know about the entire network. These types of systems only check and monitor incoming and outgoing packets to a computer and alert the network administrator or computer user when detecting intrusion or suspicious activity. The important advantage of these systems is the ability to organize very well decisions for each host specifically and uniquely [42].

2.2. Network-based intrusion detection systems (NIDS)

Network-based intrusion detection systems monitor and analyze network-wide traffic to identify threats. These systems detect malicious activities such as denial of service (DOS) attacks, port scanning, etc. in the entire network. Network-based intrusion detection systems are in the form of hardware or software that are used to monitor the traffic passing through the entire network and the computers in the network are placed in a specific location or locations of the network, they analyze the network traffic. And when an attack or abnormal behavior is detected, an alert message is sent to the network administrator. Network-based intrusion detection systems do not depend on the operating system because they operate at the network layer level... These intrusion detection systems analyze network traffic for each packet passing through the network in real time and in real time or close to it in order to identify intrusion patterns [43].

3.2. Social Network Based Intrusion Detection Systems (SNIDS)

One of the new methods of sharing knowledge is using the model of social networks. As the name of SNIDS system suggests, it is a system based on social network and its functional nature is a method based on cooperation [45].

The overview of SNIDS is as shown in Figure (1). As shown in this figure, the general format of the social network has been preserved, but in order to provide the possibility of sharing knowledge of intrusion between intrusion detection systems, it has been changed and human nodes have been replaced by intrusion detection systems along with their users. Also, this network, like any other national network, consists of a number of areas [46].

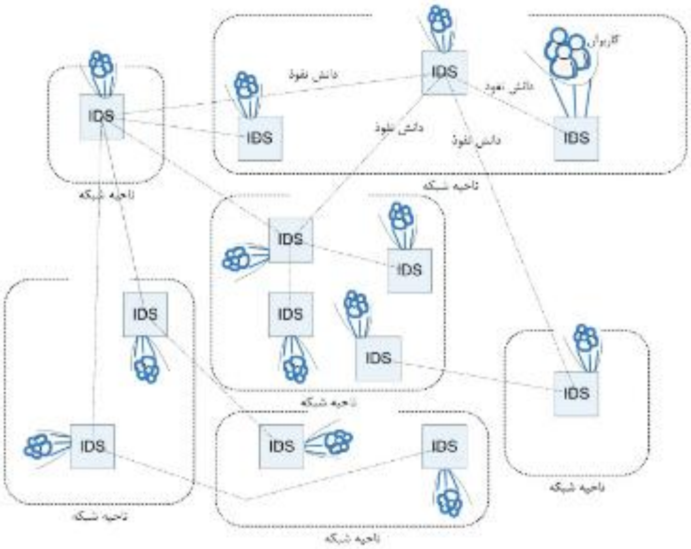

Figure 1. Overview of the SNIDS system (same source).

4.3. Signature-based intrusion detection systems (SIDS)

Signature intrusion detection systems are based on machine learning techniques to find a known attack. These are also known as knowledge-based detection or abuse detection. In SIDS, matching methods are used to find a previous intrusion. In other words, when an intrusion signature matches a previous intrusion signature that exists in the signature database, an alarm signal is released. For SIDS, host-related logs are examined to find sequences of commands or operations previously identified as malware [27]. Figure 2 shows the conceptual working of SIDS methods. The main idea is to create a database of intrusion signatures and compare the current set of operations against existing signatures and raise an alert if one is matched. For example, a rule of the form if: precedence-then: tali may result in an A if (source IP address = destination IP address) then tag being considered an attack.

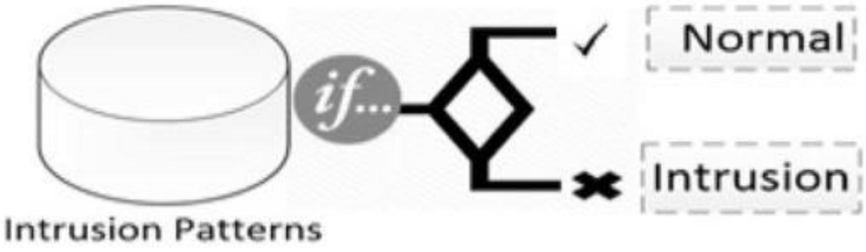

Figure 2: Conceptual work of SIDS methods [23]

5.2. Intrusion detection systems based on anomaly detection

The methods of detecting intrusion into computer networks based on anomaly detection consist of comparing the normal conditions of the system with the observed conditions, in order to detect serious differences that usually occur in the event of attacks. The systems that operate based on these methods have a documented history that shows the state of the various components of the system in a normal state. The status of communications, the number of subscribers, the behavioral status and usual requests of subscribers, as well as the ongoing software and hardware relations are among these. These records are obtained by checking and recording user performance and system status in a certain period of time [50]. Intrusion detection methods based on anomaly detection based on static methods measure the characteristics of the current situation. The measured properties are compared with the threshold limits recorded in the system history. If the measured values are more than the threshold limits, it can be said that the network is threatened. For example, the web traffic, the amount of network processing, the amount of received and sent emails, the number of attempts to log in to the system, or the percentage of CPU usage may exceed the threshold in a period of time, it can be said that an error may have occurred in the system. is another example of the use of these methods, we can refer to the detection of TPC attacks [8].

6.2. Detection of network-based intrusion by neural network anomaly method

The penetration detection system in this method has a three-layer structure. The layers guide the flow of packets and finally provide a stimulus vector for the neural network. These layers include traffic preprocessor probe, neural network. The function of each of these layers is briefly as follows:

Probe: collects network traffic of a host or network traffic at the network level. If we want to detect abnormal behavior and abuses at the network level and not at the server level, the best source available to us is network traffic, that is, packets sent between the source and destination hosts. The network probe is responsible for collecting network traffic [41].

Traffic pre-processor: This section receives the traffic from the probe and extracts the available connections and connection characteristics from the information about the packets and performs statistical-time pre-processing on the network traffic using the connection characteristics. and finally, by using the pre-processing done for each of the connections, the stimulus vector is created and delivered to the neural network unit [42].

Most attacks are a sequence of events and it is not possible to diagnose such attacks by examining network packets separately. In order to generalize part of Dan to detect different attacks in the network, the existing connections in the network are extracted from the network traffic. Views extracted from network connections specify a more accurate representation of network traffic, and since the features extracted from each packet are insufficient to create normal traffic views, connections between source and destination hosts are tracked instead of packets. to be in this project, due to the accuracy of the statistics and also the type of attacks tested, network connections are used instead of network packets. Every connection request is sent from the source host to the destination host. The destination host responds to this request as soon as it receives it [47]. Therefore, the packets related to each connection are analyzed and the information contained in them is collected and put together and is considered as the information of a connection. Based on this information, abnormal behaviors and investigated the abuses at the network level. The data preprocessing process is done in two stages. In the first step, a series of characteristics such as time stamp, source address, destination address, source port, etc. are extracted from the data related to each packet. In the second step, information about packages is processed to generate connection records [48, 51].

Neural networks: The stimulus vector received from the preprocessor examines the traffic and determines whether the network traffic is normal or not. After the traffic preprocessor layer, there is a neural network layer which is used as a classifier in the intrusion detection system. The vector neural network examines the traffic received from the preprocessor and determines whether the network traffic is normal or not. The neural network used is the PBH neural network [49, 52].

conclusion

With the growth of information technology, network security is considered as one of the challenging topics. Intrusion detection systems are known as one of the main elements of security infrastructure in many organizations. These systems are a set of hardware and software models and patterns that automate the processes of monitoring the events of computer systems. In this article, while explaining the concepts related to the intrusion detection system, we have reviewed the history and researches done and at the end we have explained some types of intrusion detection systems for more information.

References

[1] Gavel, S., Raghuvanshi, A. S., & Tiwari, S. (2021). Distributed intrusion detection scheme using dual-axis dimensionality reduction for Internet of things (IoT). The Journalof Supercomputing, 77(9), 10488-10511.

[2] Nemati, Z., Mohammadi, A., Bayat, A., & Mirzaei, A. (2024). Metaheuristic and Data Mining Algorithms-based Feature Selection Approach for Anomaly Detection. IETE Journal of Research, 1-15

[3] Najafi, Mehdi and Rafei, Reza (2014). A new method of light-weight intrusion detection for computer networks. Scientific Research Journal of Modern Defense Sciences and Technologies, 8th year, number 3, pp. 191-200

[4] Nemati, Z., Mohammadi, A., Bayat, A., & Mirzaei, A. (2023). Financial Ratios and Efficient Classification Algorithms for Fraud Risk Detection in Financial Statements. International Journal of Industrial Mathematics

[5] Marousi, Ali, Zabakh, Iman and Atai Khabaz, Hossein (2018). Detection of intrusion in the network using the combination of artificial neural networks in a hierarchical manner. Scientific Journal of Electronic and Cyber Defense, Year 8, Number One, Springer 2019 pp. 89-99

[6] Nemati, Z., Mohammadi, A., Bayat, A., & Mirzaei, A. (2024). Fraud Risk Prediction in Financial Statements through Comparative Analysis of Genetic Algorithm, Grey Wolf Optimization, and Particle Swarm Optimization. Iranian Journal of Finance, 8(1), 98-130.

[7] Mahmoudi, Kyomarth, Kitabdar, Mohammad Javad and Saibani, Mosbah (2012). Identification of intrusion into computer networks of military systems by anomaly intrusion detection method. Maritime Science and Technology Quarterly, No. 69, pp. 17-27

[8] Nemati, Z., Mohammadi, A., Bayat, A., & Mirzaei, A. (2024). The impact of financial ratio reduction on supervised methods' ability to detect financial statement fraud. Karafan Quarterly Scientific Journal

[9] Najjar, Marzieh and Moatar, Mohammad Hossein (2017). Detection of network penetration using the combined approach of hidden Markov model and hyper machine learning. Electrical Engineering Journal of Tabriz University, Volume 48, Number 4, Winter 2017, pp. 1817-1807

[10] Nematia, Z., Mohammadia, A., Bayata, A., & Mirzaeib, A. (2024). Predicting fraud in financial statements using supervised methods: An analytical comparison. International Journal of Nonlinear Analysis and Applications, 15(8), 259-272.

[11] Hosseinnejad, Rouzbeh and Ghafari, Ali (2014). Detection of penetration in cloud computing by the technique of heterogeneity detection. Quarterly journal of intelligent multimedia processing and communication systems, Scientific Association of Electronic Commerce of Iran, third year, Springer 2011, pp. 37-46

[12] Nemati, Z., Mohammadi, A., Bayat, A., & Mirzaei, A. (2025). Fraud Prediction in Financial Statements through Comparative Analysis of Data Mining Methods. International Journal of Finance & Managerial Accounting, 10(38), 151-166.

[13] Latif, Masoumeh and Batani, Zohra (2015). Investigation and comparison of intrusion detection methods in computer networks. The first national conference of technology in applied engineering young and elite researchers club of Islamic Azad University, February 2015, pp. 1-24

[14] Duan, H., & Mirzaei, A. (2023). Adaptive Rate Maximization and Hierarchical Resource Management for Underlay Spectrum Sharing NOMA HetNets with Hybrid Power Supplies. Mobile Networks and Applications, 1-17.

[15] Beheshti, Zahra, and S. M. H. Shamsudding. (2013). A review of population-based metaheuristic algorithms" Int. J. Adv. Soft Comput. Appl., Vol. 5, No. 1, pp.1-35.

[16] Mirzaei, A., & Najafi Souha, A. (2021). Towards optimal configuration in MEC Neural networks: deep learning-based optimal resource allocation. Wireless Personal Communications, 121(1), 221-243

[17] Blondin, James, and Ashraf, Saad. (2010). Metaheuristic techniques for support vectormachine model selection. 2010 10th International Conference on IEEE Hybrid Intelligent Systems (HIS).

[18] Javid, S., & Mirzaei, A. (2021). Presenting a Reliable Routing Approach in IoT Healthcare Using the Multiobjective-Based Multiagent Approach. Wireless Communications and Mobile Computing, 2021

[19] Antoon, Rufi. (2014). Network Security 1 and 2 Companion Guide, Pearson Education India, and Chapter 1: Vulnerabilities, Threats, and Attacks.

[20] Li, X., Lan, X., Mirzaei, A., & Bonab, M. J. A. (2022). Reliability and robust resource allocation for Cache-enabled HetNets: QoS-aware mobile edge computing. Reliability Engineering & System Safety, 220, 108272.

[21] Larson, Robert, and Cockcroft, Lance (2003). CCSP: Cisco Certified Security Professional Certification. Part I Introduction to Network Security, Chapter 1 Understanding Network Security Threats.

[22] Somarin, A. M., Barari, M., & Zarrabi, H. (2018). Big data based self-optimization networking in next generation mobile networks. Wireless Personal Communications, 101(3), 1499-1518.

[23] Uma, M., and Padmavathi, G. (2013). A Survey on Various Cyber Attacks and their Classification", IJ Network Security, Vol. 15, No. 5, pp. 390-396.

[24] Zhang, S., Madadkhani, M., Shafieezadeh, M., & Mirzaei, A. (2019). A novel approach to optimize power consumption in orchard WSN: Efficient opportunistic routing. Wireless Personal Communications, 108(3), 1611-1634.

[25] Subba, Basant, Biswas, Santosh, and Karmakar, Sushanta. (2016). Intrusion detection in Mobile Adhoc Networks: Bayesian game formulation. Engineering Science and Technology, an International Journal, Vol. 19, Issue 2, pp. 782-799.

[26] Hosseinalipour, A., KeyKhosravi, D., & Somarin, A. M. (2010, April). New hierarchical routing protocol for WSNs. In 2010 Second International Conference on Computer and Network Technology (pp. 269-272). IEEE.

[27] Carlin, Andrew, Hammoudeh, Mohammad, and Aldabbas, Omar. (2015). Defense for Distributed Denial of Service Attacks in Cloud Computing. Procedia Computer Science, Vol. 73, pp. 490-497.

[28] Narimani, Y., Zeinali, E., & Mirzaei, A. (2022). QoS-aware resource allocation and fault tolerant operation in hybrid SDN using stochastic network calculus. Physical Communication, 53, 101709.

[29] Liu, Yiming, Tseng, Kuo-Kun, and Pan, Jeng- Shyang. (2012). Statistical Based Waveform Classification for Cloud Intrusion Detection. IEEE 2012 International Conference on Computing, Measurement, Control and Sensor Network (CMCSN), Taiyuan, China.

[30] Mirzaei, A. (2022). A novel approach to QoS-aware resource allocation in NOMA cellular HetNets using multi-layer optimization. Concurrency and Computation: Practice and Experience, 34(21), e7068.

[31] Yousefi, D., Yari, H., Osouli, F., Ebrahimi, M., Esmalifalak, S., Johari, M., ... & Mirzapour, R. Energy Efficient Computation Offloading and Virtual Connection Control in. *learning (DL)*, *44*, 43.

[32] M. Ring, S. Wunderlich, D. Scheuring, D. Landes, A. Hotho, “A survey of network-based intrusion detection data sets”, Computers and Security, vol. 86, pp. 147-167, Sept. 2019 (doi: 10.1016/j.cose.2019.0- 6.005).

[33] Jahandideh, Y., & Mirzaei, A. (2021). Allocating Duplicate Copies for IoT Data in Cloud Computing based on Harmony 33 Algorithm. IETE Journal of Research, 1-14.

[34] H. Zhengbing, L. Zhitang, W. Junqi, "A novel network intrusion detection system (NIDS) based on signatures search of data mining", Proceeding of the IEEE/WKDD, pp. 10-16, Adelaide, SA, Australia, Jan.2008 (doi: 10.1109/WKDD.2008.48).

[35] Mirzaei, A., Barari, M., & Zarrabi, H. (2019). Efficient resource management for non-orthogonal multiple access: A novel approach towards green hetnets. Intelligent Data Analysis, 23(2), 425-447.

[36] N. Shone, T.N. Ngoc, V.D. Phai, Q. Shi, "A deep learning approach to network intrusion detection", IEEE Trans. on Emerging Topics in Computational Intelligence, vol. 2, no. 1, pp. 41-50, Feb. 2018

[37] Mirzaei, A., & Rahimi, A. (2019). A Novel Approach for Cluster Self-Optimization Using Big Data Analytics. Information Systems & Telecommunication, 50.

[38] M. Momeni, S. Gharavi, F. Hourali, “Reducing the impact of SYN flood attacks by increasing the accuracy of PSO algorithm using adaptive effective filters,” Journal of Intelligent Procedures in Electrical Technology, vol. 10, np. 37, pp. 51-57, Spring 2019.

[39] Rad, K. J., & Mirzaei, A. (2022). Hierarchical capacity management and load balancing for HetNets using multi-layer optimisation methods. International Journal of Ad Hoc and Ubiquitous Computing, 41(1), 44-57.

[40] Hozouri, A., EffatParvar, M., Yousefi, D., & Mirzaei, A. Scheduling algorithm for bidirectional LPT.

[41] Safari, Mohammad and Parvin Nia, Elham and Keshavarz Haddad, Alireza (1401). Combined intrusion detection system to deal with cyber-attack in industrial control systems with dedicated network. Journal of Smart Methods in Electric Industry, Year 13, No. 51, Fall 1401, pp. 31-50

[42] Mirzaei, A. (2021). QoS-aware Resource Allocation for Live Streaming in Edge-Clouds Aided HetNets Using Stochastic Network Calculus

[43] Catania, C. A.; Garino, C. G. "Automatic Network Intrusion Detection: Current Techniques and Open Issues"; Computers & Electrical Eng. 2012, 38, 1062-1072.

[44] - Mirzaei, A., & Zandiyan, S. (2023). A Novel Approach for Establishing Connectivity in Partitioned Mobile Sensor Networks using Beamforming Techniques. arXiv preprint arXiv:2308.04797

[45] Rahimi, Shahzad, Niazi Tarshiz, Masoud and Hosseini, Seyedabed (1401). An overview of intrusion detection systems from the point of view of structure and methods of improving their performance. Journal of information technology in engineering design. 14th period, number 2, fall and winter 1400, pp. 72-93

[46] Gajjar, H., & Malek, Z. (2020, July). A survey of intrusion detection system (IDS) using OpenStack private cloud. In 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4) (pp. 162-168). IEEE.

[47] Ziaeddini, A., Mohajer, A., Yousefi, D., Mirzaei, A., & Gonglee, S. (2022). An optimized multi-layer resource management in mobile edge computing networks: a joint computation offloading and caching solution. *arXiv preprint arXiv:2211.15487*.

[48] Singh, U. K., Joshi, C., & Singh, S. K. (2017). Zero-day attacks defense technique for protecting system against unknown vulnerabilities. International Journal of Scientific Research in Computer Science and Engineering, 5(1), 13-18.

[49] V. Jaiganesh, S. Mangayarkarasi, P. Sumathi. " Intrusion Detection Systems: A Survey and Analysis of Classification Techniques." International Journal of Advanced Research in Computer and Communication Engineering ,2 (2013).

[50] Alizadeh Thani, Mehdi and Ghaemi Bafghi, Abbas (1388). Intrusion detection system based on social network. The sixth conference of the National Cryptographic Association of Iran, October 1388, pp. 223-230

[51] Javaid, A., Niyaz, Q., Sun, W., & Alam, M. (2016). A deep learning approach for network intrusion detection system. Eai Endorsed Transactions on Security and Safety, 3(9), e2.

[52] Alishzadeh, Rababe, Sadeghian, Babak and Safabakhsh, Reza (1382). Annual National Conference of the Iranian Computer Association Year: 1382 | Holding period: 9