Mesopotamian journal of Cybersecurity
Vol. **2021**, **pp**. 1–4
DOI: https://doi.org/10.58496/MJCS/2021/001; ISSN: 2958-6542
https://mesopotamian.press/journals/index.php/CyberSecurity

Review Article

Intrusion Detection: A Review

Mohammad Aljanabi[1,*], Mohd Arfian Ismail [1], Raed Abdulkareem Hasan [2], Junaida Sulaiman[1]

[1] *Faculty of Computing, University Malaysia Pahang, Gambang, Malaysia*

[2] *Northern Technical University, Iraq*

ARTICLE INFO

Article History

Received 1 January 2021
Accepted 10 January 2021

Keywords
Cyber Security
Intrusion Detection
Machine Learning

ABSTRACT

Due to the processes involved in the electronic transformation of data, the use of computer systems and the Internet in recent years has led to significant security, privacy, and confidentiality issues. Intrusion detection systems (IDSs) are one of the most promising data and network protection tools; there are many approaches and techniques used for detection the of intrusions based on the intrusion type, in this paper different types of intrusions are reviewed, and the different types of systems for detecting intrusions, challenges and future directions for researchers determined at the end of this paper

1. INTRODUCTION

A Series of security, confidentiality, and privacy issues have been associated with the use of computer systems and the Internet in recent times due to the need to transfer data electronically. Hence, studies have been focusing on the improvement of privacy and secure computer systems, but despite the effort, these problems still linger in computer systems, to the extent that there is currently no completely secure system on the planet. Attacks are launched in different forms [1]; these attacks emerge in response to the existence of new signatures with abnormal behavior in the signature database. Therefore, several tools have been used to counter different forms of attacks on network systems and one such tool is IDSs. This tool was developed for real-time monitoring of network systems for any form of intrusion. They aim to detect attacks that are aimed at compromising the security features of a system. This paper reviewed the existing work, methods, and techniques in IDS

2. Intrusion Detection

An IDS detects network intrusion via monitoring of network activities [2]. Two main types of IDS currently exist; are host-based IDS and network-based IDS [3-7]Network-based IDSs (NIDS) is intended to detect intrusions by monitoring different network activities; on the other hand, host-based IDS (HIDSs) are designed to detect network intrusions in single hosts. The output of packet sniffers is monitored by NIDS and being that NIDS can monitor more network targets, it can detect more attacks that may not be detected by HIDSs since HIDSs cannot see the packet headers. For instance, NIDS can detect numerous IP-based DoS attacks because they can monitor the packet headers as they pass through the network. Furthermore, NIDS depends less on the operating system of the host as a detection source, rather, it is built with specific operating systems to work effectively. HIDS and NIDS have been combined in some hybrid IDSs and used to detect intrusions [8]. Based on the detection mechanism, IDSs are classified into misuse detection (MD) & anomaly detection (AD) systems [9]. Three types of detection mechanisms are used in IDS; these are ML, statistical, and data mining techniques. Figure 2.1 summarized the IDS.

*Corresponding author. Email: mohammad.cs88@gmail.com

3. Misuse detection (MD)

The IDS in this category searches for known attack patterns to detect intrusion as applied in the current commercial needs. However, the issue with MD is the inability to detect new attacks. Some of the existing MD techniques rely on the use of expert systems (ES), state-transition analysis (STA), signature analysis (SA), and data mining (DM). Regarding expert systems, they rely on a set of rules for the description of intrusions [10]. Expert systems translate audit events into facts that convey their semantic relevance. Then, conclusions are drawn using an inference engine based on these rules and facts. In STA, attacks are analyzed with a set of transitions and goals using a state transition diagram [11]; events are considered an intrusion if they trigger an intrusion state.

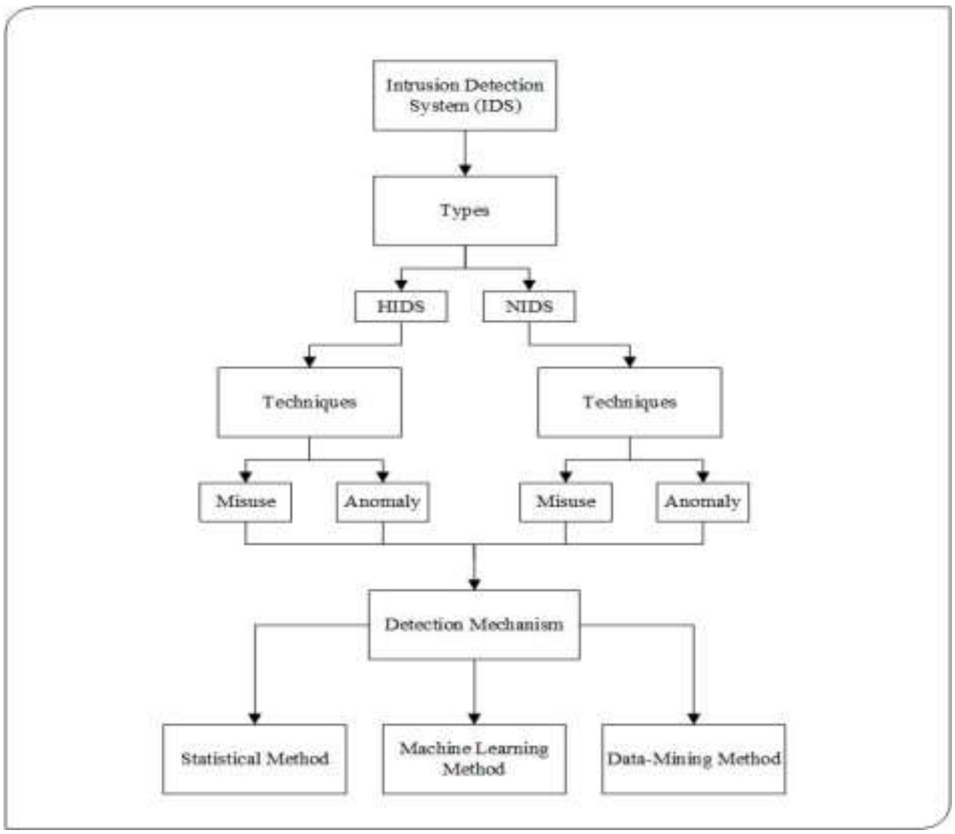

Figure 1 IDS overview

The signatures found in the audit trail are used in signature analysis to describe the attack [12]. Events are considered an attack if they match the attack signatures hosted in the database. Data mining-based IDSs have been developed recently[13]; these systems are based on the fact that useful and previously unnoticed patterns can be extracted from large data sources via data mining processes. The extracted patterns can be presented as rules, decision trees, neural nets, or instance-based examples. Several studies have utilized data mining algorithms in MD; for instance, the association rules algorithm was used by [14], ADAM was used by (Barbara et al., 2001), and IDDM was used by Decision tree and fuzzy association rules have been employed in intrusion detection by while neural network algorithm has been used to enhance IDS performance.

4. Anomaly detection

Being that unknown attacks cannot be detected using misuse detection techniques, such issues are addressed using anomaly detection. Several anomaly detection approaches (such as clustering, classification, etc.) have been proposed and implemented [7]. In supervised anomaly detection, the profile of normal network activities is first built using attack-free training data; then, patterns that deviate from the established normal traffic profile are considered intrusions. ADAM [15] uses an attack-free dataset to build the profile of normal traffic and represent it as association rules. During network activities, suspicious connections are detected based on the established profile. Other supervised techniques are also used in anomaly detection; these include genetic algorithms, fuzzy data mining, neural networks, and SVM , Expert systems and statistical methods have also found application in supervised anomaly detection [16] Statistical methods rely on several samples to build the profiles of the normal user and system behaviours; patterns that deviate from the established profiles are considered abnormal. Regarding expert systems, they rely on a set of rules to describe normal user and system behaviours; then, these rules are applied to detect abnormal behaviours.

5. Challenges of Intrusion Detection Systems

Ongoing research is being conducted on new systems for the automatic detection of abnormal system usages. In addition, Denning reported the creation of an intrusion-detection model that was proposed as a framework for general-purpose IDS. Since then, specialists have developed and implemented several network ID automation algorithms. In addition, they have consistently sought out more precise, faster, and scalable methods for this purpose. With the advent of the Internet of Things and big data, it is anticipated that the number of connected devices will surpass 26 billion by 2020. With this trend, it is anticipated that both the type and quantity of cybersecurity issues will increase. Figure 2 provides a summary of the obstacles in IDS.

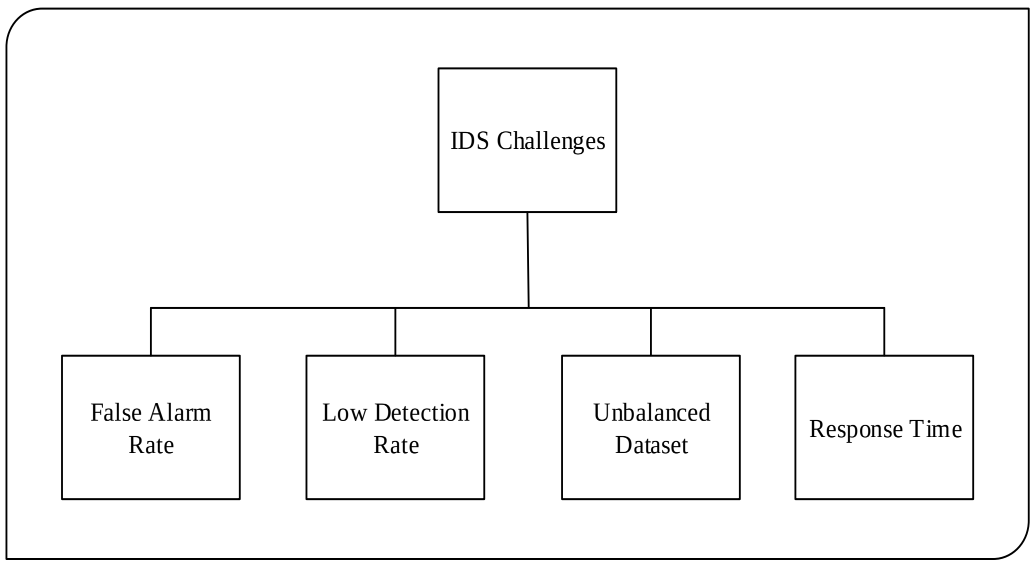

Figure 2 IDS Challenges

Recently, some researchers have advocated for additional IDS categories. Liao et al. [16] argued, for instance, that IDS should be subdivided into five subcategories that may fall under any of the aforementioned classes. Rule-based, pattern-based, state-based, statistics-based, and heuristic-based intrusion detection systems are the suggested subclasses. Due to the number of similarities between the strengths of the individual techniques and the absence of clear criteria that distinguishes one technique from another, such a classification could lead to confusion. The signature or rule-based IDS typically has a low FPR but is incapable of detecting new types of attacks. [17] A system designed to detect anomalies must have a low FPR detection rate. The detection performance of ID systems based on stateful protocol analysis varies based on the level of their profile definition [9]. Keeping attack profiles up-to-date as new protocols emerge over time is a significant challenge for this method.

As stated previously, the purpose of this research is to develop an anomaly-based IDS with high accuracy and low false positive detection. Numerous studies have been conducted on IDS false alarm reduction. Approximately 99% of ID alerts do not involve cyber-security issues, according to Pietraszek's estimations [18]. This is due to the small differences between normal and malicious activities. Other obstacles identified by Pietraszek include the development of accurate signatures that can capture attack behavior but are not triggered during legal operations, given that some activities may be permissible under certain conditions but suspicious under others. The "Adaptive Learner for Alert Classification" (ALAC) approach proposed by Pietraszek [19] combines machine learning techniques with human-based observatory training to adaptively learn implicit classification rules. Due to the involvement of the human factor in training, the ALAC system can be upgraded incrementally as conditions change. As mentioned in the preceding chapter, the primary challenge of the current anomaly IDS are the increased difficulty of developing a system with these features compared to MD. [20] Additionally, a high number of false alarms are generated alongside a low detection rate. In addition, the imbalanced dataset affects the evaluation of the models[21].

Conflicts Of Interest

The authors declare no conflicts of interest.

Acknowledgment

The authors would like to thank the Universiti Malaysia Pahang for their support.

References

[1] H. Debar, M. Dacier, and A. Wespi, "A revised taxonomy for intrusion-detection systems," in *Annales des télécommunications*, 2000, vol. 55, no. 7-8, pp. 361-378: Springer.

[2] E. Schultz, J. Mellander, and C. F. Endorf, "Intrusion Detection And Prevention McGraw-Hill Osborne Media," *December*, vol. 18, pp. 221-254, 2003.

[3] S. N. Abd and H. R. Ibraheem, "Rao-SVM Machine Learning Algorithm for Intrusion Detection System," *Iraqi Journal For Computer Science and Mathematics*, vol. 1, no. 1, pp. 23-27, 2020.

[6] H. Alaidaros, M. Mahmuddin, and A. Al-Mazari, "An overview of flow-based and packet-based intrusion detection performance in high speed networks," 2011.

[7] W. Alhakami, A. ALharbi, S. Bourouis, R. Alroobaea, and N. Bouguila, "Network Anomaly Intrusion Detection Using a Nonparametric Bayesian Approach and Feature Selection," *IEEE Access*, vol. 7, pp. 52181-52190, 2019.

[8] M. Al-Qatf, Y. Lasheng, M. Al-Habib, and K. Al-Sabahi, "Deep Learning Approach Combining Sparse Autoencoder With SVM for Network Intrusion Detection," *IEEE Access*, vol. 6, pp. 52843-52856, 2018.

[10] S. M. H. Bamakan, H. Wang, T. Yingjie, and Y. Shi, "An effective intrusion detection framework based on MCLP/SVM optimized by time-varying chaos particle swarm optimization," *Neurocomputing*, vol. 199, pp. 90-102, 2016.

[11] Y. Zhang, X. Chen, L. Jin, X. Wang, and D. Guo, "Network Intrusion Detection: Based on Deep Hierarchical Network and Original Flow Data," *IEEE Access*, vol. 7, pp. 37004-37016, 2019.

[12] H. Altwaijry, "Bayesian based intrusion detection system," in *IAENG Transactions on Engineering Technologies*: Springer, 2013, pp. 29-44.

[13] R. Abdulhammed, H. Musafer, A. Alessa, M. Faezipour, and A. Abuzneid, "Features Dimensionality Reduction Approaches for Machine Learning Based Network Intrusion Detection," *Electronics*, vol. 8, no. 3, p. 322, 2019.

[14] I. Aljarah and S. A. Ludwig, "Mapreduce intrusion detection system based on a particle swarm optimization clustering algorithm," in *Evolutionary Computation (CEC), 2013 IEEE Congress on*, 2013, pp. 955-962: IEEE.

[15] A. A. Aburomman and M. B. I. Reaz, "A survey of intrusion detection systems based on ensemble and hybrid classifiers," *Computers & Security*, vol. 65, pp. 135-152, 2017.

[16] M. K. Khaleel, M. A. Ismail, U. Yunan, and S. Kasim, "Review on intrusion detection system based on the goal of the detection system," *International Journal of Integrated Engineering*, vol. 10, no. 6, 2018.