Challenges and Limitations of IDS: A Comprehensive Assessment and Future Perspectives

Medha Khenwar, Meenakshi Nawal

Department of CS, Swami Keshvanand Institute of Technology, Management & Gramothan, Ramanagariya, Jaipur, 302017(India)

Email: ***medhakhenwar.mk@gmail.com, meenakshi.nawal.02@gmail.com***

Received 02.04.2024 **received in revised form** 06.06.2024, **accepted** 07.06.2024

DOI: 10.47904/IJSKIT.14.1.2024.35-39

Abstract: **This paper explores the difficulties that Intrusion Detection Systems (IDS) encounter in keeping networks secure. While IDS are vital for identifying and stopping cyber threats, they face several obstacles. These challenges range from inaccuracies in detecting threats to struggles with managing large volumes of data. Additionally, attackers constantly develop new techniques to evade detection, further complicating the task of IDS. The paper discusses these challenges and proposes future directions to enhance IDS effectiveness. By addressing these issues, we can improve the security of computer networks and better protect against cyber threats.**

Keywords**– Intrusion detection system, wireless network, Evasion Techniques, Real-Time Monitoring**

1. INTRODUCTION

In today's interconnected digital world, where information exchange is vital for businesses, organizations, and individuals, securing computer networks is essential, with Intrusion Detection Systems (IDS) playing a critical role as the first line of defense against cyber threats [1]. These systems are designed to monitor network traffic, identify suspicious activities or behaviors, and take appropriate action to mitigate potential risks. The importance of IDS stems from the ever-present and evolving nature of cyber threats [2]. From malicious hackers attempting to breach sensitive data to malware and ransomware targeting vulnerable systems, the range of potential security breaches is vast and continually expanding. In this landscape, IDS serve as vigilant guardians, constantly monitoring network traffic for signs of unauthorized access, malicious activity, or abnormal behaviour [3].

However, despite their significance, IDS face numerous challenges and limitations that can hinder their effectiveness. One of the primary challenges is the sheer volume and complexity of network traffic. In large-scale networks, such as enterprise environments or internet service providers, IDS must analyze vast amounts of data in real-time, requiring significant computational resources and sophisticated algorithms. Furthermore, the dynamic nature of modern networks poses additional challenges for IDS. Traditional network architectures are evolving towards more decentralized and distributed models, such as wireless ad hoc networks and Internet of Things (IoT) deployments. These dynamic environments present unique challenges for intrusion detection, including frequent topology changes, limited resources, and the presence of diverse device types with varying capabilities. Another significant challenge for IDS is the emergence of sophisticated evasion techniques employed by attackers to bypass detection. These techniques include encryption, obfuscation, and polymorphic attacks, designed to conceal malicious activities and evade signature-based detection methods. As attackers continue to innovate, IDS must adapt to these evolving threats to remain effective.

Moreover, IDS commonly grapple with false positives and false negatives, erroneously categorizing legitimate actions as malicious or vice versa. These inaccuracies can lead to alert fatigue, where security personnel are overwhelmed by the sheer volume of alerts, resulting in genuine threats being overlooked or ignored. Despite these challenges, ongoing research and development efforts are focused on enhancing IDS capabilities and addressing their limitations. From leveraging machine learning and artificial intelligence techniques to improve detection accuracy to developing lightweight algorithms optimized for resource-constrained environments, there is a concerted effort to overcome the challenges facing IDS.

In this paper, we conduct a comprehensive exploration of the hurdles and limitations associated with Intrusion Detection Systems. We examine the factors contributing to these challenges, discuss their implications for network security, and explore enhancing IDS effectiveness. By understanding these challenges and actively addressing them, we can strengthen the resilience of computer networks and better protect against cyber threats.

2. LITERATURE OVERVIEW

Securing communication entails employing a myriad of tactics such as access control, optimization-driven secure routing techniques, agent-based methods, temporal analysis, specialized intrusion detection techniques for feature selection and classification, key management protocols, encryption-decryption methodologies, trust management frameworks, firewall implementations, and application-specific considerations. Diverse scholarly works have proposed multifaceted strategies to bolster security in IoT environments through Intrusion Detection Systems (IDS). This section delves into a thorough examination of publications authored by various scholars, scrutinizing their efficacy and constraints in the domain of IoT IDS. Furthermore, a notable recommendation advocates for a genetic algorithm-based IDS tailored for IoT. The proposed algorithm crafts intelligent rules for scrutinizing device behavior, thus enabling the identification and mitigation of malicious content and links within the IoT ecosystem. However, this approach is constrained by significant computational overhead, and it may not accurately detect unknown attacks. Wang et al. proposed employing the hidden Markov model (HMM) for IDS development, optimizing parameters such as speed, efficiency and precision. Despite utilizing a statistical approach to address novel situations, this system lacks uniform detection accuracy, thus compromising security [9]. A survey advocated for a signature-based IDS utilizing data mining techniques, which improved detection accuracy by distinguishing normal from abnormal device behavior. Nonetheless, its computational overhead renders it unsuitable for IoT environments [7]. A research introduced a security system employing swarm intelligence in IDS development, reducing training time and enhancing intrusion detection quality in many scenarios. However, the non-uniform behavior of generated rules and their interdependence pose challenges. [10] conducted an inquiry into IDS, utilizing fuzzy rough sets [11] for outlier detection-based intrusion detection. Gendreu and Moorman [12] conducted a survey of past IDS developments aimed at securing IoT. They outlined the general IDS process and highlighted current research challenges in IoT IDS, along with requirements for developing high-quality IDS in IoT environments. Nevertheless, the exploration of the latest trends and attack patterns is still necessary.

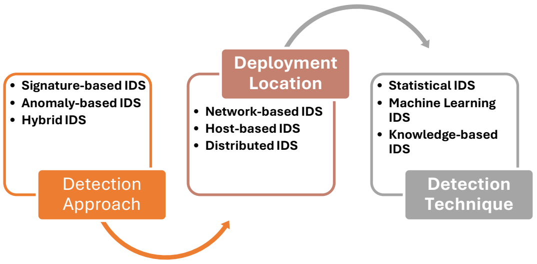

Figure 1 Categorization of IDS

The taxonomy of intrusion detection systems (IDS) is structured based on several key criteria, facilitating a comprehensive understanding of their functionalities. First, IDS can be categorized by detection approach, including signature-based, anomaly-based, and hybrid systems, each offering unique strengths in identifying threats. Deployment location is another crucial factor, with network-based IDS (NIDS), host-based IDS (HIDS), and distributed IDS (DIDS) providing varying levels of coverage across network infrastructures. Detection techniques further refine IDS capabilities, with statistical analysis, machine learning algorithms, and knowledge-based systems enabling effective threat detection. Detection granularity focuses on the level of detail at which IDS operate, ranging from packet-level analysis to application-level scrutiny.[17] potential strategies and future directions for

Finally, IDS response mechanisms dictate their action upon detecting threats, whether passive alerting or active intervention. By considering these categories collectively, organizations can tailor their IDS deployment to effectively safeguard against evolving cybersecurity threats.

A strategy has been devised to protect flying ad hoc networks from disruptive nodes that hinder message transmission among UAVs [18]. These nodes not only tamper with information but also disrupt communication between other nodes, posing risks to network integrity. The proposed solution swiftly identifies and removes these malicious nodes from the network. It employs a cluster-based approach to calculate collaborative trust among nodes, with an observer node guiding a group of nodes. Criteria such as cooperative trust, distance, or range are used to select the observer node, which then serves as the cluster head overseeing its members. Algorithms have been developed to assign the cluster observer and members. [19] Anomaly detection in vehicular networks has been a focus of research for decades, with numerous contributions addressing the vulnerabilities of connected vehicles [20]. It is identified state-of-the-art attack vectors that exploit various devices, highlighting the threat posed by hackers. Consequently, presented several works aimed at detecting intrusions and anomalies in vehicle communications.

3. FOR AD-HOC NETWORKS: INTRUSION DETECTION SYSTEMS

Exploring the Challenges of Intrusion Detection Systems (IDS) in Ad Hoc Networks: IDS tailored for ad hoc networks encounter unique challenges stemming from the decentralized and dynamic nature of these networks. Below, we delve into a comprehensive examination of the primary considerations.

3.1 Dynamic Network Topology

Ad hoc networks lack fixed infrastructure and have constantly changing network topologies due to node mobility. Traditional IDS, which rely on fixed network structures, struggle to adapt to these dynamic environments. Therefore, IDS for ad hoc networks must incorporate dynamic topology awareness and adaptability to effectively monitor and detect intrusions despite frequent changes in network configurations.

3.2 Limited Resources

Nodes in ad hoc networks typically have limited processing power, memory, and energy resources. Traditional IDS algorithms may be too resource-intensive for these constrained devices. As such, IDS solutions for ad hoc networks need to be lightweight and energy-efficient to minimize resource consumption while still providing effective intrusion detection capabilities.

3.3 Wireless Communication

Ad hoc networks rely on wireless communication, which introduces vulnerabilities such as eavesdropping, spoofing, and jamming attacks. IDS for ad hoc networks must be capable of detecting and mitigating these wireless-specific threats to ensure the integrity and confidentiality of communication within the network.

3.4 Highly Dynamic Environment

Ad hoc networks are highly dynamic, with nodes joining, leaving, or moving within the network at any time. This dynamic nature makes it challenging to establish trust relationships between nodes and to distinguish between normal and malicious behavior. IDS for ad hoc networks often leverage anomaly detection techniques, which can adapt to evolving network conditions and identify suspicious activities based on deviations from established behavior patterns.

3.5 Cooperative Monitoring

Traditional centralized IDS architectures may not be suitable for ad hoc networks due to their distributed nature. Instead, IDS for ad hoc networks often employ cooperative monitoring techniques, where nodes collaboratively monitor and analyze network traffic to detect intrusions. Cooperative monitoring allows for decentralized intrusion detection and enables rapid response to security threats without relying on a central authority.

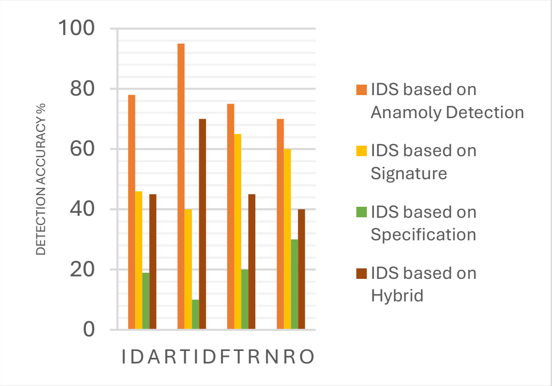

Figure 1: Evaluation Matrix of various IDS system

3.6 Evaluation of Established IDS Methodologies

The analysis of existing IDS approaches involves a comprehensive examination of the different methodologies employed in the field of intrusion detection.

3.6.2 Evaluation based on Signatures based IDS

Signature-based detection, the simplest method, compares network activities against a database of known attack signatures. This approach offers clear understanding and control, as system administrators can easily identify and manage potential threats. However, while effective at detecting known attacks, signature-based models struggle with identifying new or modified threats. To maintain high success rates, continuous updates to the signature database are necessary, requiring the definition of separate signatures for all potential attack types.

3.6.2 Evaluation based on Anomaly IDS

Anomaly-based detection compares network traffic to normal behavior to identify anomalies, making it more versatile than signature-based systems. However, managing alarms from anomaly-based systems is more complex, as they detect deviations without prior knowledge of attack signatures. While anomaly detection can identify unknown attacks, distinguishing true alarms from false positives remains challenging. Therefore, categorizing detected attacks is crucial for effective management of anomaly-based systems.

3.6.3 Evaluation of Host based IDS

Evaluation of host-based Intrusion Detection Systems (IDSs) involves assessing their ability to detect various types of attacks based on the detection techniques employed. Some IDSs combine multiple techniques, while others focus on one or a few. Due to their detailed knowledge of host features, IDS agents can often predict the success of an attack if left unchecked. However, like other IDS technologies, host-based IDSs can generate false positives and negatives, with accuracy being more challenging due to a lack of contextual understanding. For instance, actions like host reboots or new application installations might trigger alerts, but determining their maliciousness without additional context is difficult. Host-based IDSs employing multiple detection techniques typically offer better detection rates by monitoring different aspects of the host, providing a more comprehensive view of events and aiding in assessing their intent.

3.6.4 Evaluation of Wireless IDS

Evaluation of Wireless Intrusion Detection Systems (IDSs) involves assessing their ability to identify WLAN protocol-level attacks, misconfigurations, and policy violations by analyzing IEEE 802.11a, b, g, and i protocol communications. These IDSs are also vulnerable to denial-of-service and physical attacks. While some Wireless IDS products rely solely on signature-based detection, others employ a combination of signature-based detection, anomaly-based detection, and situational protocol analysis techniques. Wireless IDSs generally exhibit higher intrusion detection accuracy compared to other IDS types. However, they have limitations, such as an inability to detect certain types of attacks, including those involving passive monitoring and offline processing of wireless traffic.

3.6.5 Evaluation of Network Based IDS

Network-based analysis (NBA) systems excel at detecting attacks with significant network activity or unusual behavior but struggle with small-scale or slow-developing threats due to their reliance on anomaly detection. Additionally, the delay in detecting attacks, caused by batched data transmission from network devices, poses a challenge. To address these limitations, improved sensitivity to subtle anomalies and real-time monitoring capabilities are needed.

3.6.6 Evaluation of hybrid-based IDS

Hybrid-based Intrusion Detection Systems combine signature-based and anomaly-based methods to detect a wider range of threats. While they offer improved accuracy and coverage, their complexity requires careful configuration and maintenance to ensure effectiveness. Some of the methodologies has been discussed below in Table 1.

Table 1: Evaluation of hybrid-based intrusion detection methods.

Author s	Methodologies	Limitations	Ideal Context
J. Wang et al[13]	Detecting irregular node behavior and associating it with matching signatures using a DoS protection manager.	The pre-established signatures undergo sporadic updates under the supervision of the DoS protection manager.	Dynamic network environm ents
]K Anand et al[14]	Detecting attacks by timestamp to identify inconsistencies in node broadcasts of rank to neighboring nodes.	Excessive utilization of network resources.	Stable network environm ents
Amin et al[15]	Identifying assaults through a broadened framework for IP-USN within the IoT	Computational overhead.	IoT environm ents
Huang, et al[16]	Detection of malicious nodes based on a pattern matching engine.	Real-time implementatio n is unfeasible.	Controlle d lab environm ents

4. CONCLUDING REMARKS AND FUTURE DIRECTIONS

This paper conducts a comprehensive analysis of Intrusion Detection Systems (IDS) tailored for ad-hoc environments, drawing upon the extensive research available in the field. Within this paper, IDS solutions customized for ad-hoc networks are organized into four main categories: anomaly detection-based IDS, signature-based IDS, specifications-based IDS, and hybrid methods. This classification facilitates a methodical and comparative assessment of the diverse intrusion detection approaches within ad-hoc networks. Looking ahead, the envisioned trajectory for the proposed system involves the integration of intelligent IDS mechanisms utilizing deep learning methodologies into ad-hoc networks characterized by dynamic network topology. Utilizing deep learning capabilities empowers the IDS to dynamically adapt and learn from the ever-changing network dynamics, thereby augmenting its capacity to promptly identify and counter emerging threats in real-time. This prospective strategy emphasizes the criticality of harnessing state-of-the-art technologies to fortify the security stance of ad-hoc networks amidst the continuously evolving threat landscape.

REFERENCES

[1] S. O. Amin, Y. jig Yoon, M. S. Siddiqui, and C. S. Hong, "A novel intrusion detection framework for IP-based sensor networks," in Proceedings of the International Conference on Information Networking, 20 09, pp. 1–3, Newyork, NY, USA, April 2009.

[2] Munirul, Haque and Sheikh Iqbal Ahamedm, Security in Pervasive Computing: Current Status and Open Issues, International Journal of Network Security (**2007**), Volume 3, Pages 203–214.

[3] W. Meng, W. Li, and L.-F. Kwok, "Efm: enhancing the performance of signature-based network intrusion detection systems using enhanced flter mechanism," Computers & Security, vol. 43, pp. 189–204, 2014.

[4] S. V. N. Santhosh Kumar, Y. Palanichamy, M. Selvi, S. Ganapathy, and A. Kannan, "Energy efcient secured K means based unequal fuzzy clustering algorithm for efcient reprogramming in wireless sensor networks," Wireless Networks, Springer, Berlin, Germany, pp. 1–22, 2021.

[5] T. Kalidoss, L. Rajasekaran, K. Kanagasabai, G. Sannasi, and A. Kannan, "QoS aware trust based routing algorithm for wireless sensor networks," Wireless Personal Communications, vol. 110, no. 4, pp. 1637–1658, 2020.

[6] M. A. Jan, P. Nanda, X. He, and R. P. Liu, "A Sybil attack detection scheme for a centralized clustering-based hierarchical network," Proceedings of the Trust-com/BigDataSE/ ISPA, vol. 1, pp. 318–325, 2015.

[7] A. Shiravi, H. Shiravi, M. Tavallaee, and A. A. Ghorbani, "Toward developing a systematic approach to generate benchmark datasets for intrusion detection," Computers & Security, vol. 31, no. 3, pp. 357–374, 2012

[8] R. Rajendran, S. V. N. Santhosh Kumar, Y. Palanichamy, and K. Arputharaj, "Detection of DoS attacks in cloud networks using intelligent rule based classifcation system," Cluster Computing, vol. 22, no. 1, pp. 423–434, 2019

[9] . Qiu, Y. Ma, X. Chen, H. Yu, and L. Chen, "Hybrid intrusion detection system based on Dempster-Shafer evidence theory," Computers & Security, vol. 117, Article ID 102709, 2022.

[10] Y. Zhang, N. Meratnia, and P. J. Havinga, "Outlier detection techniques for wireless sensor networks: a survey," IEEE Communications Surveys & Tutorials, vol. 12, no. 2, pp. 159–170, 2010

[11] M. Mahdavisharif, S. Jamali, and R. Fotohi, "Big data-aware intrusion detection system in communication networks: a deep learning approach," Journal of Grid Computing, vol. 19, pp. 46–28, 2021.

[12] K. Sonar and H. Upadhyay, "An approach to secure internet of things against DDoS," in Proceedings of the International Conference on ICTfor Sustainable Development, pp. 367–376, 2016.

[13] J. Wang, Q. Kuang, and S. Duan, "A new online anomaly learning and detection for large-scale service of Internet of Ting," Personal and Ubiquitous Computing, vol. 19, no. 7, pp. 1021–1031, 2015.

[14] K. Anand, S. Ganapathy, K. Kulothungan, P. Yogesh, and A. Kannan, "A rule based approach for attribute selection and intrusion detection in wireless sensor networks," Procedia Engineering, vol. 38, pp. 1658–1664, 2012

[15] P. Nancy, S. Muthurajkumar, S. Ganapathy, S. Santhosh Kumar, M. Selvi, and K. Arputharaj, "Intrusion detection using dynamic feature selection and fuzzy temporal decision tree classifcation for wireless sensor networks," IET Communications, vol. 14, no. 5, pp. 888–895, 2020.

[16] Huang, Y. A., & Lee, W. (2003, October). A cooperative intrusion detection system for ad hoc networks. In Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks (pp. 135-147).

[17] Alsarhan, A., Alauthman, M., Alshdaifat, E. A., Al-Ghuwairi, A. R., & Al-Dubai, A. (2023). Machine Learning-driven optimization for SVM-based intrusion detection system in vehicular ad hoc networks. *Journal of Ambient Intelligence and Humanized Computing*, *14*(5), 6113-6122.

[18] Gupta, S., & Sharma, N. (2024). SCFS-securing flying ad hoc network using cluster-based trusted fuzzy scheme. *Complex & Intelligent Systems*, 1-20.

[19] Thuvva, A., Goyal, R., & Balaji, G. N. (2024, June). Internet of Vehicle Ad Hoc Networks (VANETs): Anomaly Detection. In *Disruptive technologies in Computing and Communication Systems: Proceedings of the 1st International Conference on Disruptive technologies in Computing and Communication Systems* (p. 135). CRC Press.

[20] Alaya, B., Sellami, L., & Lorenz, P. (2024). An ontological approach to the detection of anomalies in vehicular ad hoc networks. *Ad Hoc Networks*, *156*, 103417.