International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 12, Issue 10, October 2023)

Review of Intrusion Detection in Wireless Sensor Network

Ankita Verma[1], Prof. Suresh S. Gawande[2]

[1]*Research Scholar,* [2]*Head of Department, Dept. of Electronics & Communication Eng., Bhabha Engineering Reasearch Institute, Bhopal, India*

***Abstract*— Wireless Sensor Networks (WSNs) have emerged as a vital technology for various applications, ranging from environmental monitoring to surveillance and healthcare. However, their inherent characteristics, such as resource constraints, dynamic network topology, and vulnerability to attacks, expose them to potential security threats. Intrusion Detection Systems (IDSs) play a crucial role in safeguarding WSNs against malicious activities and ensuring the integrity and reliability of data. This paper presents a comprehensive review of Intrusion Detection in Wireless Sensor Networks. The main objective is to assess the state-of-the-art techniques and methodologies employed in IDSs for WSNs, examining their strengths, weaknesses, and applicability in different scenarios. The review encompasses both centralized and distributed IDS approaches, as well as anomaly-based and signature-based detection techniques.**

***Keywords*— WSN, NIDS, Machine, Deep, Python, Accuracy.**

I. INTRODUCTION

A Wireless Sensor Networks (WSNs) have emerged as a transformative technology with a wide range of applications, including environmental monitoring, industrial automation, healthcare, and smart city infrastructure. These networks consist of numerous tiny, resource-constrained sensor nodes that collaborate to collect and disseminate valuable data. Despite their invaluable contributions to various domains, WSNs face significant security challenges due to their unique characteristics, such as limited computational power, limited memory, and susceptibility to communication and physical attacks.

Ensuring the security and integrity of data transmitted and processed within WSNs is of paramount importance to prevent unauthorized access, data tampering, and other malicious activities. Intrusion Detection Systems (IDSs) have been recognized as an essential component in safeguarding WSNs against potential security threats. IDSs are designed to detect and respond to suspicious or malicious behavior, providing an added layer of defense beyond traditional encryption and authentication mechanisms.

Over the years, extensive research efforts have been directed toward developing efficient and effective intrusion detection techniques tailored to the specific constraints of WSNs. However, due to the dynamic nature of these networks and the continually evolving threat landscape, achieving robust and reliable intrusion detection remains a challenging task.

The review aims to consolidate the vast body of research in this domain, offering insights into the various intrusion detection approaches, algorithms, and protocols proposed by the research community. By evaluating the strengths and limitations of existing techniques, this review seeks to shed light on the advancements made in securing WSNs and identify potential areas for improvement.

The subsequent sections of this paper will delve into the fundamental principles of intrusion detection in WSNs, providing an overview of the different types of attacks that threaten the network's security. We will also discuss the challenges faced by IDSs in the context of WSNs and examine the requirements that these systems must meet to be effective in real-world scenarios.

The review will then analyze and categorize various intrusion detection algorithms and methodologies employed in WSNs, including anomaly-based and signature-based techniques. Furthermore, we will explore machine learning-based approaches that leverage the power of data-driven models to detect emerging and previously unseen threats.

In addition to discussing individual detection algorithms, this review will also examine the significance of collaborative approaches, data fusion, and information sharing among sensor nodes to enhance the overall intrusion detection capabilities of WSNs. Furthermore, we will explore strategies like data aggregation and hierarchical architectures that optimize network resources and energy consumption.

By providing an extensive review of the current state of intrusion detection in WSNs, this paper aims to contribute to the advancement of this critical research area.

By identifying the strengths and limitations of existing techniques, we hope to inspire future research endeavors that can push the boundaries of intrusion detection capabilities and fortify the security of wireless sensor networks in the face of evolving security threats.

II. Literature Survey

S. Subbiah et al.,[1] Attacks in wireless sensor networks (WSNs) aim to prevent or eradicate the network's ability to perform its anticipated functions. Intrusion detection is a defense used in wireless sensor networks that can detect unknown attacks. Due to the incredible development in computer-related applications and massive Internet usage, it is indispensable to provide host and network security. The development of hacking technology tries to compromise computer security through intrusion. IDS was employed with the help of ML Algorithms to detect intrusions in the network.

H. W. Oleiwi et al.,[2] the proposed hybrid method using correlation with the random forest algorithm of ensemble learning. It reduces dimensionality and retrieves the best subset feature of all the three datasets separately. The third stage is using hybrid EL algorithms to detect intrusions. It involves modifying two classifiers (i.e., random forest RF, and support vector machine SVM) to apply them as adaboosting and bagging EL Algorithms; using the voting average technique as the aggregation process.

I. Mbona et al.,[3] The solution proposed in this study demonstrates that the law of anomalous numbers, famously known as Benford's law, is a viable technique that can effectively identify significant network features that are indicative of anomalous behaviour and can be used for detecting zero-day attacks. Finally, our study illustrates that semi-supervised ML approaches are effective for detecting zero-day attacks if significant features are optimally chosen. The experimental results demonstrate that one-class support vector machines achieved the best results (Matthews correlation coefficient of 74% and F_1 score of 85%) for detecting zero-day network attacks.

S. Otoum et al.,[4] In this work, a Split Learning-based IDS (SplitLearn) for Intelligent Transportation System (ITS) infrastructures has been proposed to address the potential security concerns. The proposed model has been evaluated and compared against other models (i.e., Federated Learning (FedLearn) and Transfer Learning (TransLearn)-based solutions). With the highest accuracy and detection rates, the proposed model (SplitLearn) outperforms FedLearn and TransLearn by 2 to 5 % respectively. We also see a decrease in power consumption when utilizing SplitLearn versus FedLearn.

H. Siddharthan et al.,[5] Recently, the number of Internet of Things (IoT) networks has been grown exponentially, which results in more data sharing between devices without appropriate security mechanisms. Since huge data management is involved, maintaining the time constraints between the devices in IoT networks is another significant issue. To address these issues, an intelligent intrusion detection system has been adapted to recognize or predict a cyber-attack using Elite Machine Learning algorithms (EML), and a lightweight protocol is used to manage the time-constrained issue.

M. S. A. Muthanna et al.,[6] The IoT has established itself as a multibillion-dollar business in recent years. Despite its obvious advantages, the widespread nature of IoT renders it insecure and a potential target for cyber-attacks. Furthermore, these devices broad connectivity and dynamic heterogeneous nature can open up a new surface of attack for refined malware attacks. There is a critical need to protect the IoT environment from such attacks and malware. Therefore this research aims to propose an intelligent, SDN-enabled hybrid framework leveraging Cuda Long Short Term Memory Gated Recurrent Unit for efficient threat detection in IoT environments.

P. Freitas et al.,[7] compare two machine learning algorithms' ability to detect fuzzing and spoofing attacks, and evaluate which of them is most accurate with the fewest number of data bytes. The fewer data bytes required, the sooner detection can start and the sooner attacking frames can be detected. Experiment results show that our proposed detection mechanism achieves accuracy higher than 99%, F1-scores higher than 97%, and detection times shorter than 80 μs for the types of attacks considered. Moreover, when compared to four state-of-the-art intrusion detection systems, it is the only solution that is capable of discarding attacking frames before damage occurs while being deployed on inexpensive Raspberry Pi. Such an inexpensive deployment is particularly desirable, as cost is one of the automotive industry's primary concerns.

M. Ozkan-Okay et al.,[8] proposed methodology basically has two contributions. The first contribution is the Feature Selection Approach (FSAP) to increase the speed of attack detection by reducing the number of used features. The second contribution is the hybrid attack detection technique, SABADT (Signature and Anomaly Based Attack Detection Technique), which detects attacks fast with high accuracy. The proposed methodology is implemented on the KDD'99 and UNSW-NB15 datasets.

Y. K. Saheed et al.,[9] These developments enable the healthcare business to maintain a higher level of touch and care for its patients. Security is seen as a significant challenge in whatsoever technology's reliance based on the IoT.

Security difficulties occur owing to the various potential attacks posed by attackers. There are numerous security concerns, such as remote hijacking, impersonation, denial of service attacks, password guessing, and man-in-the-middle. In the event of such attacks, critical data associated with IoT connectivity may be revealed, altered, or even rendered inaccessible to authorized users.

A. R. Gad et al.,[10] the vast majority of existing research is based on NSL-KDD or KDD-CUP99 datasets. Recent attacks are not present in these datasets. As a result, we employed a realistic dataset called ToN-IoT that derived from a large-scale, heterogeneous IoT network. This work tested various ML methods in both binary and multi-class classification problems. We used the Chi-square (Chi^2) technique was used for feature selection and the Synthetic minority oversampling technique (SMOTE) for class balancing. According to the results, the XGBoost method outperformed other ML methods.

N. Venkata et al.,[11] causes serious disruption of delay-sensitive applications that can lead to life endangering situations and therefore such an attack needs to be addressed. In this letter, we propose a mechanism that uses a support vector machine to detect the presence of a jammer in the network. We obtain jointly sufficient statistics of packet drop probabilities and use them to generate the training data. The results demonstrate the effectiveness of the proposed detection system.

T. Moulahi et al.,[12] presents some nodes malfunctioning or total system failure, which can affect the safety of the driver as well as the vehicle. Detecting intrusions is a challenging problem in the context of using CAN bus for in-vehicle communication. Most existing work focuses on the physical aspects without taking into consideration the data itself. Machine Learning (ML) tools, especially classification techniques, have been widely used to address similar problems. In this work, we use and compare several ML techniques to deal with the problem of detecting intrusions in in-vehicle communication.

III. Challenges

Intrusion Detection in Wireless Sensor Networks (WSNs) faces several unique challenges due to the specific characteristics and constraints of these networks. These challenges hinder the development and deployment of robust and efficient Intrusion Detection Systems (IDSs). Some of the key challenges include:

1. *Resource Constraints:* WSN nodes are typically resource-constrained in terms of processing power, memory, and energy supply. Traditional IDSs designed for resource-rich environments may not be directly applicable to WSNs. Developing lightweight and energy-efficient intrusion detection algorithms that do not overly burden the sensor nodes is a significant challenge.
2. *Communication Overhead:* The process of transmitting and analyzing data for intrusion detection can introduce considerable communication overhead in WSNs. This overhead can lead to increased energy consumption and latency, impacting the overall performance of the network. IDSs should be designed to minimize communication requirements while ensuring timely and accurate detection.
3. *Dynamic Network Topology:* WSNs often operate in dynamic and harsh environments, leading to frequent changes in network topology due to node mobility, failures, or environmental conditions. Traditional centralized IDS architectures may struggle to adapt to such dynamic topologies. Developing distributed and decentralized intrusion detection mechanisms that can handle topology changes effectively is crucial.
4. *Scalability:* WSNs can encompass a vast number of sensor nodes, making scalability a significant concern. As the network size increases, the intrusion detection system should be able to handle the growing volume of data and maintain accurate detection rates without overwhelming the resources of the sensor nodes and the base station.
5. *Security and Privacy:* While IDSs aim to enhance security, they themselves can become potential targets for attackers. Adversaries may attempt to evade or tamper with the IDS, leading to false negatives or false positives. Moreover, the collected data may contain sensitive information, raising concerns about privacy and secure data transmission.
6. *Real-Time Requirements:* Some WSN applications require real-time or near-real-time intrusion detection to respond promptly to security threats. Meeting these real-time requirements while preserving the accuracy and reliability of the detection is a challenge, especially in resource-constrained environments.
7. *Lack of Global Knowledge:* Sensor nodes in WSNs typically have limited knowledge of the overall network state, as they only communicate with their immediate neighbors. This lack of global knowledge can make it challenging to detect coordinated attacks or to identify emerging threats that may span multiple nodes.
8. *Adapting to Evolving Attacks:* The threat landscape is continually evolving, with new attack techniques and patterns emerging over time. IDSs need to be adaptive and capable of detecting unknown or zero-day attacks effectively.

9. *Energy-Efficient Deployment:* Deploying and maintaining IDS components on sensor nodes can significantly impact the network's energy consumption. Balancing the energy expenditure for intrusion detection with the overall network performance and the desired level of security is a complex challenge.
10. *False Alarm Minimization:* Minimizing false alarms is crucial to avoid unnecessary responses and conserve network resources. However, achieving a low false alarm rate while maintaining high detection rates is a delicate trade-off.

These challenges require interdisciplinary research efforts that consider the unique characteristics of WSNs, such as energy efficiency, mobility, and adaptability. Developing innovative intrusion detection techniques that strike a balance between accuracy, efficiency, and scalability will be critical to enhancing the security posture of wireless sensor networks in the face of ever-evolving threats.

IV. Conclusion

Intrusion Detection in Wireless Sensor Networks (WSNs) plays a crucial role in safeguarding these networks against potential security threats. This comprehensive review has highlighted the significant progress made in the field and shed light on the challenges that researchers and practitioners face in developing robust and efficient IDSs for WSNs. The review revealed that resource constraints, communication overhead, dynamic network topology, and scalability are among the primary challenges that hinder the deployment of intrusion detection solutions in WSNs. These resource limitations demand the development of lightweight and energy-efficient algorithms, while the dynamic nature of WSNs necessitates adaptive and distributed intrusion detection approaches.

REFERENCES

[1] S. Subbiah, K. S. M. Anbananthen, S. Thangaraj, S. Kannan and D. Chelliah, "Intrusion detection technique in wireless sensor network using grid search random forest with Boruta feature selection algorithm," in Journal of Communications and Networks, vol. 24, no. 2, pp. 264-273, April 2022, doi: 10.23919/JCN.2022.000002.

[2] H. W. Oleiwi, D. N. Mhawi and H. Al-Raweshidy, "MLTs-ADCNs: Machine Learning Techniques for Anomaly Detection in Communication Networks," in IEEE Access, 2022, doi: 10.1109/ACCESS.2022.3201869.

[3] I. Mbona and J. H. P. Eloff, "Detecting Zero-Day Intrusion Attacks Using Semi-Supervised Machine Learning Approaches," in IEEE Access, vol. 10, pp. 69822-69838, 2022, doi: 10.1109/ACCESS.2022.3187116.

[4] S. Otoum, N. Guizani and H. Mouftah, "On the Feasibility of Split Learning, Transfer Learning and Federated Learning for Preserving Security in ITS Systems," in IEEE Transactions on Intelligent Transportation Systems, doi: 10.1109/TITS.2022.3159092.

[5] H. Siddharthan, T. Deepa and P. Chandhar, "SENMQTT-SET: An Intelligent Intrusion Detection in IoT-MQTT Networks Using Ensemble Multi Cascade Features," in IEEE Access, vol. 10, pp. 33095-33110, 2022, doi: 10.1109/ACCESS.2022.3161566.

[6] M. S. A. Muthanna, R. Alkanhel, A. Muthanna, A. Rafiq and W. A. M. Abdullah, "Towards SDN-Enabled, Intelligent Intrusion Detection System for Internet of Things (IoT)," in IEEE Access, vol. 10, pp. 22756-22768, 2022, doi: 10.1109/ACCESS.2022.3153716.

[7] P. Freitas De Araujo-Filho, A. J. Pinheiro, G. Kaddoum, D. R. Campelo and F. L. Soares, "An Efficient Intrusion Prevention System for CAN: Hindering Cyber-Attacks With a Low-Cost Platform," in IEEE Access, vol. 9, pp. 166855-166869, 2021, doi: 10.1109/ACCESS.2021.3136147.

[8] M. Ozkan-Okay, Ö. Aslan, R. Eryigit and R. Samet, "SABADT: Hybrid Intrusion Detection Approach for Cyber Attacks Identification in WLAN," in IEEE Access, vol. 9, pp. 157639-157653, 2021, doi: 10.1109/ACCESS.2021.3129600.

[9] Y. K. Saheed and M. O. Arowolo, "Efficient Cyber Attack Detection on the Internet of Medical Things-Smart Environment Based on Deep Recurrent Neural Network and Machine Learning Algorithms," in IEEE Access, vol. 9, pp. 161546-161554, 2021, doi: 10.1109/ACCESS.2021.3128837.

[10] A. R. Gad, A. A. Nashat and T. M. Barkat, "Intrusion Detection System Using Machine Learning for Vehicular Ad Hoc Networks Based on ToN-IoT Dataset," in IEEE Access, vol. 9, pp. 142206-142217, 2021, doi: 10.1109/ACCESS.2021.3120626.

[11] N. Venkata Abhishek and M. Gurusamy, "JaDe: Low Power Jamming Detection Using Machine Learning in Vehicular Networks," in IEEE Wireless Communications Letters, vol. 10, no. 10, pp. 2210-2214, Oct. 2021, doi: 10.1109/LWC.2021.3097162.

[12] T. Moulahi, S. Zidi, A. Alabdulatif and M. Atiquzzaman, "Comparative Performance Evaluation of Intrusion Detection Based on Machine Learning in In-Vehicle Controller Area Network Bus," in IEEE Access, vol. 9, pp. 99595-99605, 2021, doi: 10.1109/ACCESS.2021.3095962.