International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online) Volume 13, Issue 02, February 2024)

Review of Machine Learning based Intrusion Detection Techniques in Wireless Sensor Network

[1]Mousham Kumari Sharma, [2]Dr Anshuj Jain

[1]Research Scholar, Dept. of Electronics and Communication Engineering, SCOPE College of Engineering, Bhopal, India,
[2]Associate Professor & HOD, Dept. of Electronics and Communication Engineering, SCOPE College of Engineering, Bhopal, India

***Abstract*— Wireless Sensor Networks (WSNs) play a pivotal role in numerous applications, ranging from environmental monitoring to healthcare systems. However, their deployment in various domains introduces security challenges, making intrusion detection a critical component for safeguarding the integrity and reliability of these networks. Machine learning techniques have garnered considerable attention in recent years for enhancing intrusion detection capabilities in WSNs due to their ability to adapt to evolving threats and complex network environments. This review paper presents a comprehensive examination of machine learning-based intrusion detection techniques specifically tailored for WSNs. We provide an overview of the existing methodologies, including supervised, unsupervised, and semi-supervised learning approaches, along with their advantages, limitations, and performance evaluation metrics. Furthermore, we discuss the challenges and future research directions in the domain to provide insights for researchers and practitioners aiming to enhance the security posture of WSNs.**

***Keywords*— *Intrusion, Detection, Wireless Sensor Network*.**

I. INTRODUCTION

Wireless Sensor Networks (WSNs) have emerged as a fundamental technology enabling various applications such as environmental monitoring, industrial automation, healthcare systems, and military surveillance. These networks consist of a large number of small, inexpensive sensor nodes with limited computational and communication capabilities, which collaborate to collect, process, and transmit data from the deployed environment to the base station or sink node. However, the distributed and resource-constrained nature of WSNs exposes them to various security threats and vulnerabilities, including node capture, tampering, data interception, and malicious attacks, which can compromise the integrity, confidentiality, and availability of the network.

Intrusion detection systems (IDSs) serve as a crucial line of defense against these security threats by continuously monitoring network traffic and node behavior to detect and respond to malicious activities in real-time. Traditional rule-based and signature-based IDSs, although effective to some extent, often struggle to cope with the dynamic and unpredictable nature of attacks in WSNs, thus necessitating the exploration of more adaptive and intelligent approaches. Machine learning (ML) techniques have emerged as promising solutions for intrusion detection in WSNs due to their ability to learn from historical data, detect anomalies, and adapt to evolving threats without the need for explicit rule definition.

This paper aims to provide a comprehensive review of machine learning-based intrusion detection techniques specifically tailored for WSNs. The review encompasses various ML paradigms, including supervised, unsupervised, and semi-supervised learning, and discusses their applicability, advantages, limitations, and performance evaluation metrics in the context of WSN security.

In the supervised learning paradigm, algorithms such as Support Vector Machines (SVM), Decision Trees, Random Forests, and Neural Networks are trained on labeled datasets comprising both normal and malicious network traffic to learn the characteristics of different types of attacks. Unsupervised learning techniques, including K-means clustering, DBSCAN, and Isolation Forest, aim to identify patterns and anomalies in the absence of labeled data, making them suitable for detecting novel and unknown attacks in WSNs. Semi-supervised learning methods combine the strengths of both supervised and unsupervised approaches by leveraging a small amount of labeled data along with a larger pool of unlabeled data to enhance detection accuracy and scalability.

Additionally, we discuss the challenges associated with ML-based intrusion detection in WSNs, such as energy efficiency, resource constraints, scalability, and the curse of dimensionality, and propose potential solutions and future

research directions to address these challenges effectively. By providing a comprehensive overview of the state-of-the-art ML-based intrusion detection techniques in WSNs, this review paper aims to facilitate further advancements in securing these critical network infrastructures against evolving cyber 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. The obtained 99.65% and 99.17% accuracy rates are quite high when compared to leading methods in the literature. In addition, common tools were used to obtain a mix of normal activities and current attack behaviors in order to test on novel attacks within the scope of the study. The different types of attacks were captured with the Wireshark tool. Some of the captured attacks were used only in the testing phase. In this test case, the attacks were detected with an accuracy rate of 99.69%.

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

Challenges in Machine Learning-based Intrusion Detection in Wireless Sensor Networks (WSNs):

1. **Resource Constraints**: Sensor nodes in WSNs typically have limited computational power, memory, and energy resources. Implementing machine learning algorithms on such constrained devices poses significant challenges in terms of model complexity, memory usage, and energy consumption.
2. **Scalability**: As the size of WSNs grows, the scalability of intrusion detection systems becomes a major concern. Traditional machine learning algorithms may struggle to scale efficiently to large-scale networks due to the computational and memory requirements associated with training and inference.
3. **Dynamic Network Environment**: WSNs operate in dynamic and unpredictable environments where network topology, traffic patterns, and environmental conditions can change rapidly. Adapting machine learning models to these dynamic conditions and maintaining their effectiveness in real-time poses a significant challenge.
4. **Limited Labelled Data**: Annotated data for training machine learning models in WSNs is often scarce and expensive to acquire. This scarcity of labeled data hampers the effectiveness of supervised learning approaches and necessitates the exploration of unsupervised and semi-supervised techniques, which can leverage both labeled and unlabeled data.
5. **Security and Privacy Concerns**: The deployment of machine learning-based intrusion detection systems in WSNs raises security and privacy concerns, particularly regarding the confidentiality of sensitive data collected by sensors and the potential for adversarial attacks targeting the learning algorithms themselves.
6. **Adversarial Attacks**: Adversaries can launch sophisticated attacks against machine learning-based intrusion detection systems in WSNs by crafting

malicious data or exploiting vulnerabilities in the learning algorithms. Defending against such adversarial attacks requires robust techniques for model validation, data sanitization, and anomaly detection.

7. **Energy Efficiency**: Energy efficiency is paramount in WSNs, where sensor nodes are often powered by batteries or energy harvesting mechanisms with limited capacity. Machine learning algorithms must be optimized for energy efficiency to prolong the operational lifetime of sensor networks without sacrificing detection accuracy.

IV. CONCLUSION

This paper present the literature survey and study of security algorithms for high speed and internet of things application and also introduced briefly the main ideas of IoT and called attention to the significance of having a protected structure for this new encouraging innovation. We went over the present difficulties related with giving protection which is the best basic segment, on the grounds that without enough security. Secondly different security techniques discussed and compare their performance. Also discuss existing AES algorithm studied and analyzed well to promote the performance of the encryption methods also to ensure the security proceedings. Therefore AES has many advantages but if it will use IOT application then give more delay and consume large area and more power. In future it can be modified and design MAES sothat requirement of security in IOT application can be fulfill.

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.