[1] M.Sahaya Sheela
[2] A.Jasvant Ram
[3] S. Sathees babu
[4] V.Jeya Ramy
[5] R.Anitha

Enhancing Wireless Sensor Network Security Through Mutual Information Analysis for Intrusion Detection and Resilience

Abstract: Intrusion detection is a critical aspect of network security, involving the identification and response to unauthorized access or malicious activities within a system. It plays a crucial role in safeguarding networks and ensuring data integrity and confidentiality. The Mutual Information (MI) analysis is a vital component in the realm of intrusion detection and security within Wireless Sensor Networks (WSNs). By assessing the information shared between pairs of sensor nodes, MI analysis reveals underlying patterns and relationships in network data. This process involves calculating the mutual information for each node pair based on statistical properties of observed values. Strong correlations or dependencies between nodes are identified, aiding in the detection of critical nodes or clusters vulnerable to compromise. Additionally, MI analysis informs feature extraction by guiding the selection of informative features that capture network structure. It also serves as a proactive tool for identifying anomalies or deviations from expected patterns, which may signal intrusion attempts or malicious activities. Through monitoring changes in mutual information over time, MI analysis facilitates prompt responses to emerging threats, enhancing the resilience and security of WSNs. The work exhibits high accuracy, recall rates, and detection rates across various attack scenarios, underscoring its efficacy in identifying and mitigating security threats. The algorithm's efficiency, effectiveness, and reliability make it a promising solution for enhancing WSN security. Through sophisticated methodologies and adaptive defensive strategies, the proposed algorithm strengthens the robustness and dependability of WSNs, minimizing the risk of potential security vulnerabilities and ensuring comprehensive threat detection in real-world deployment scenarios.

Keywords: Intrusion detection, Mutual Information Analysis, Wireless Sensor Network, Feature Extraction, Anomalies, Security.

I. INTRODUCTION

WSNs have emerged as a vital technology for various applications, ranging from environmental monitoring to military surveillance. However, the open and distributed nature of WSNs also makes them vulnerable to intrusion and malicious attacks [1]. Intrusion in WSNs refers to unauthorized access or malicious activities carried out by attackers within the network, which can compromise data integrity, confidentiality, and availability. One common avenue for intrusion is through physical attacks. Attackers may tamper with the physical components of the network, such as sensor nodes or base stations, to gain unauthorized access or disrupt communication channels. Physical intrusion can take various forms, including node tampering, where attackers manipulate sensor nodes, or signal jamming, where attackers disrupt wireless communication channels, leading to communication failures [2]. Another prevalent intrusion method is node capture, where attackers capture sensor nodes and compromise their security mechanisms. Once compromised, attackers can extract sensitive information from the nodes or inject false data into the network, leading to incorrect decision-making or unauthorized access to sensitive information [3]. Denial of Service (DoS) attacks pose a significant threat to WSNs by overwhelming the network with excessive traffic, causing sensor nodes to become unresponsive or deplete their energy resources quickly [4]. DoS attacks can disrupt the normal operation of the network, leading to a significant degradation in performance or complete shutdown. Routing attacks target the routing protocols used in WSNs, where attackers manipulate routing information to misroute data packets or disrupt network services [5]. Examples include sinkhole attacks, where attackers attract traffic to a compromised node, and selective forwarding, where attackers drop or modify selected packets, leading to data loss or unauthorized access. To mitigate these intrusion risks, various security mechanisms and protocols are deployed in WSNs, including encryption, authentication, key management, intrusion detection systems, and

[1] Assistant Professor, Department of Electronics and Communication Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, India, Email: hisheelu@gmail.com
[2] PG Resident, Department of Radio-Diagnosis ,Saveetha Medical College and Hospital, Saveetha Institute of Medical and Technical Sciences (SIMATS), Saveetha University, Chennai, Tamil Nadu - 602105, India. Email: jasvanttejas7@gmail.com
[3] Associate Professor, Department of Computer Science and Engineering PSNA College of Engineering and Technology, Dindigul-624622, Tamil Nadu, India. Email: ssbabu@psnacet.edu.in
[4] Associate Professor, Department of Electronics and Communication Engineering ,Panimalar Engineering College, Poonamallee, Chennai, Tamil Nadu 600123. Email:jeyaramyav@gmail.com
[5] Assistant Professor, Department of Computer Science and Engineering P.S.R Engineering college, Sivakasi, Tamil Nadu 626140,India. Email: mailtoaniharshad@gmail.com

secure routing protocols. Additionally, physical security measures, such as tamper-resistant hardware and secure deployment strategies, can help protect WSNs against physical attacks and unauthorized access.

Deep learning plays a pivotal role in bolstering the security of WSNs by providing robust mechanisms for intrusion detection, anomaly detection, and data analysis [6]. Its ability to autonomously learn from vast amounts of data enables the development of sophisticated models capable of identifying and mitigating various security threats in real-time. By leveraging deep learning, WSNs can detect abnormal behavior, identify potential intrusions, and adaptively respond to evolving attack strategies [7]. Additionally, deep learning facilitates the enhancement of data encryption and privacy preservation techniques, ensuring the confidentiality and integrity of transmitted information. Overall, the integration of deep learning algorithms empowers WSNs with enhanced security measures, safeguarding against malicious attacks and ensuring the reliability of network operations [8]. Furthermore, deep learning enables WSNs to evolve beyond traditional security approaches by facilitating the development of adaptive security mechanisms that can dynamically adjust to emerging threats. Its capacity to extract intricate patterns from data enhances the accuracy and effectiveness of intrusion detection systems, bolstering the network's resilience against sophisticated attacks. By continuously analyzing network traffic and learning from past incidents, deep learning empowers WSNs to defend against intrusions proactively, ensuring the integrity, confidentiality, and availability of data transmission [9]. This transformative capability positions deep learning as a cornerstone in fortifying the security posture of WSN in an increasingly interconnected and threat-prone environment.

II. Literature Survey

Anomaly-based detection stands as a sophisticated method for fortifying the security of WSNs by actively monitoring node behavior and discerning deviations from established norms as potential intrusions. Unlike signature-based detection, which relies on predefined attack patterns, anomaly detection takes a proactive stance, scrutinizing network activities to identify any irregularities indicative of malicious behavior [10]. Anomaly detection systems employ a range of techniques to establish a baseline of normal behavior for each node within the network. By analyzing various parameters such as communication patterns, resource utilization, and data transmission rates, these systems can identify deviations from the norm, flagging them as potential security threats [11]. This proactive approach enables WSNs to detect previously unknown or zero-day attacks, providing a crucial layer of defense against emerging threats [12]. However, despite its effectiveness, anomaly-based detection is not immune to limitations. One significant challenge lies in the potential for generating false positives. Legitimate variations in network behavior, such as temporary spikes in traffic or fluctuations in resource usage, can trigger false alarms, leading to unnecessary disruption or resource wastage [13]. For instance, anomalous but benign activities, such as sudden changes in environmental conditions or network topology, may be misinterpreted as security breaches, resulting in unnecessary alarm triggers and system overhead. Addressing the issue of false positives requires careful calibration and tuning of anomaly detection algorithms. By incorporating contextual information and adaptive learning mechanisms, anomaly detection systems can distinguish between benign anomalies and genuine security threats more accurately [14]. Advanced machine learning techniques, such as ensemble methods or hybrid models, enable anomaly detection systems to dynamically adjust their detection thresholds based on real-time network conditions, reducing the incidence of false alarms while maintaining robust security posture.

Neighbor-based detection offers a localized approach to fortifying the security of WSNs by leveraging the collaborative efforts of neighboring nodes to identify potential intrusions or compromised entities within the network [15]. In this method, each node monitors the behavior of its adjacent nodes and raises alerts if it detects any suspicious activities, deviations from expected behavior, or signs of compromise. By capitalizing on local information and peer-to-peer communication, neighbor-based detection can swiftly identify and respond to security threats, particularly those confined to specific regions or clusters within the network. One of the key advantages of neighbor-based detection is its ability to detect localized attacks or compromised nodes that may go unnoticed by centralized intrusion detection systems [16]. By distributing the detection and response capabilities across multiple nodes, this approach enhances the resilience of the network against targeted attacks or insider threats [17].

Additionally, neighbor-based detection operates autonomously at the node level, reducing the reliance on centralized infrastructure and mitigating the impact of communication delays or network partitions. However, despite its merits, neighbor-based detection is not without its limitations. One significant challenge lies in the potential for false positives and false negatives [18]. Nodes may misinterpret benign activities or transient

anomalies as security threats, leading to unnecessary alarm triggers or disruptions in network operations. Conversely, nodes may fail to detect subtle or stealthy intrusions, particularly if the compromised node behaves within normal parameters or if the attack targets a subset of nodes with colluding adversaries [19]. Furthermore, neighbor-based detection may encounter scalability issues in large-scale WSN deployments or densely populated environments [20]. As the number of nodes increases, the volume of local information and communication overhead also escalates, posing challenges in managing and processing data effectively. Moreover, neighbor-based detection relies heavily on the trustworthiness of neighboring nodes and the integrity of communication channels [21]. Malicious nodes or compromised communications can undermine the reliability and effectiveness of the detection mechanism, leading to false alarms or evasion of detection..

III. Research Methodology

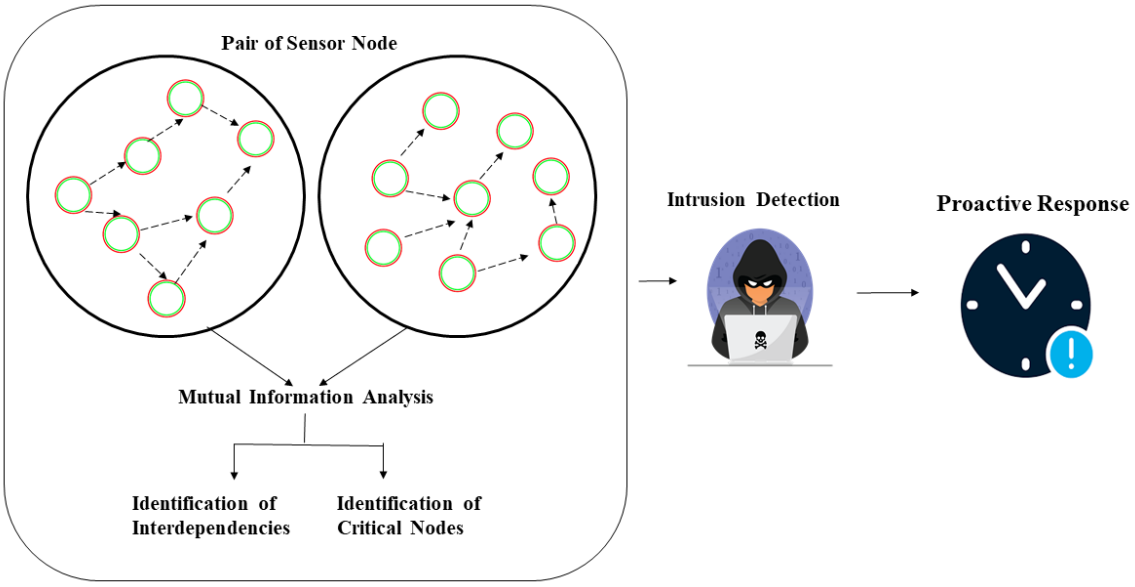

Fig. 1 Mutual Information Analysis & Intrusion Detection

In the intrusion detection and security in WSNs[23-25], the Mutual Information (MI) analysis serves as a crucial step towards understanding the interdependencies among network nodes. As in fig.1, analysis involves quantifying the amount of information shared between pairs of sensor nodes, thereby revealing underlying patterns and relationships within the network data. The MI analysis begins by calculating the mutual information between every pair of sensor nodes in the network. This computation is based on the statistical properties of the sensor data, such as the probability distributions of observed values. By measuring the mutual information, which represents the amount of shared information between two variables, the analysis identifies nodes that exhibit strong correlations or dependencies. Through MI analysis, nodes that share significant information are identified, indicating potential communication pathways or clusters within the network. These insights help in identifying critical nodes or clusters whose compromise may have cascading effects on the network's overall functionality and security. Additionally, the analysis provides valuable information for feature extraction, guiding the selection of informative features that capture the underlying structure of the network data. Furthermore, MI analysis can reveal anomalies or deviations from expected patterns in the network data, which may indicate potential intrusion attempts or malicious activities. By monitoring changes in mutual information over time, the analysis enables the detection of suspicious behavior and facilitates proactive responses to emerging threats.

$$p(x,y) = \frac{n_{x,y}}{N} \quad (1)$$

$p(x,y)$ represents the joint probability distribution of variables and, indicating the likelihood of observing specific combinations of sensor readings in the Wireless Sensor Network (WSN). denotes the number of occurrences where sensor readings and co-occur in the network. represents the total number of observations collected from sensor nodes in the WSN.

$$p(x) = \sum_y p(x,y) \quad (2)$$

$$p(y) = \sum_x p(x, y) \quad (3)$$

These equations compute the marginal probability distributions and for sensor readings and respectively, capturing the individual probabilities of observing specific sensor readings in the WSN irrespective of other variables.

$$I(X;Y) = \sum_{x \in X} \sum_{y \in Y} p(x, y) log \frac{p(x,y)}{p(x)p(y)} \quad (4)$$

The mutual information quantifies the level of information shared between sensor readings and in the WSN, providing insights into their interdependence. The joint probability distribution represents the likelihood of observing specific combinations of sensor readings and in the WSN, while the marginal probability distributions and capture the individual probabilities of observing sensor readings and respectively, regardless of other variables. By computing mutual information and analyzing these probability distributions, the algorithm gains valuable insights into the relationships among sensor data, which can be leveraged for effective intrusion detection and security measures in the WSN.

$$NMI(X;Y) = \frac{I(X;Y)}{\sqrt{H(X).H(Y)}} \quad (5)$$

Additionally, normalized mutual information provides a normalized measure of the interdependence between sensor readings and , taking into account their individual uncertainty levels captured by their entropies. This comprehensive analysis enables the algorithm to identify critical patterns, anomalies, and potential intrusion attempts, empowering it to adaptively defend the WSN against security threats. The algorithm takes sensor data collected from Wireless Sensor Network (WSN) nodes as input. This data undergoes pre-processing to remove noise and is used to compute joint and marginal probability distributions, and calculate mutual information (MI) between sensor readings. Critical nodes are identified based on high MI values, and the algorithm integrates a deep learning model for real-time intrusion detection. The output includes a detection result from the deep learning model, used to trigger proactive responses to detected intrusions. Additionally, evaluation metrics are computed to optimize algorithm parameters and defence mechanisms using real-world data. The algorithm is deployed in practical WSN environments and continuously monitored and updated for scalability and performance to enhance WSN resilience against security threats.

Algorithm 1: WSN Security Algorithm with MI Analysis

1. Collect sensor data (D) from WSN nodes.
2. Pre-process data to remove noise:$D_{preprocessed} = remove\_noise(D)$.
3. Compute joint ($p(x.y)$) and marginal ($p(x), p(y)$) probability distributions. Calculate mutual information ($I(X;Y)$) between sensor readings:
   $$I(X;Y) = \sum_{x \in X} \sum_{y \in Y} p(x.y)\, log \frac{p(x.y)}{p(x)p(y)}$$
4. Normalize mutual information for interdependence: $NMI(X;Y) = \frac{I(X;Y)}{\sqrt{H(X).H(Y)}}$.
5. Identify critical nodes based on high mutual information values: $critical_{nodes} = \{x | I(X;Y) > threshold\}$
6. Design intrusion detection features/rules based on critical nodes.
7. Deploy deep learning model (M) for real-time detection:$detection_{result} = M(D_{preprocessed})$.
8. Integrate adaptive defence mechanisms based on detection results.
9. Proactively respond to detected intrusions: $response = proactive_{response}(detection_{result})$.
10. Evaluate algorithm performance with real-world data: $performance_{metrics} = evaluate(M, realtime_{data})$
11. Optimize parameters and defence mechanisms: $optimized_{parameters} = (M, performance_{metrics})$
12. Deploy algorithm in practical WSN environments.
13. Monitor and update algorithm for scalability and performance.
14. Enhance WSN resilience against security threats based on algorithm feedback.

IV. PERFORMANCE EVALUATION

The algorithm is implemented using MATLAB version R2022a. The experimental setup requires a processor with at least an Intel Core i5 or AMD Ryzen 5 (or equivalent) processor, and a minimum of 8GB of RAM. The MATLAB environment should be installed and configured with the necessary toolboxes for signal processing, machine learning, and statistical analysis. Additionally, access WSN datasets is essential for evaluating the algorithm's performance. The experimental setup should be conducted on a desktop or laptop computer running a supported operating system such as Windows 10, macOS, or Linux. Dataset used for intrusion detection is the NSL-KDD dataset, which is a refined version of the original KDD Cup 1999 dataset [22]. The NSL-KDD dataset contains a large number of network traffic records, labeled with five categories of attacks: normal, denial of service (DoS), probe, user-to-root (U2R), and remote-to-local (R2L). Each record in the dataset consists of 41 features, including protocol types, service types, flag values, and other network traffic attributes. The dataset is widely used for evaluating intrusion detection systems and algorithms in the field of cybersecurity research. It provides a diverse range of attack scenarios and realistic network traffic patterns, making it suitable for benchmarking the performance of intrusion detection algorithms under various conditions.

Table 1 NSL-KDD Attack Distribution

Attack	Train	Test
Normal	67343	9711
DoS	45927	7458
Probe	11656	2421
U2R	52	69
R2L	995	52
Total	126973	22511

Table.1 presents the distribution of attack types in the training and testing subsets of the NSL-KDD dataset, a widely used benchmark dataset for intrusion detection research. The dataset includes instances labeled with five categories of attacks: Normal, Denial of Service (DoS), Probe, User-to-Root (U2R), and Remote-to-Local (R2L). The training subset consists of 126,973 instances, while the testing subset contains 22,511 instances. Each row in the table represents the number of instances for a specific attack type in both the training and testing subsets. These counts are essential for evaluating the performance of intrusion detection algorithms and assessing their effectiveness in detecting various types of cyber threats.

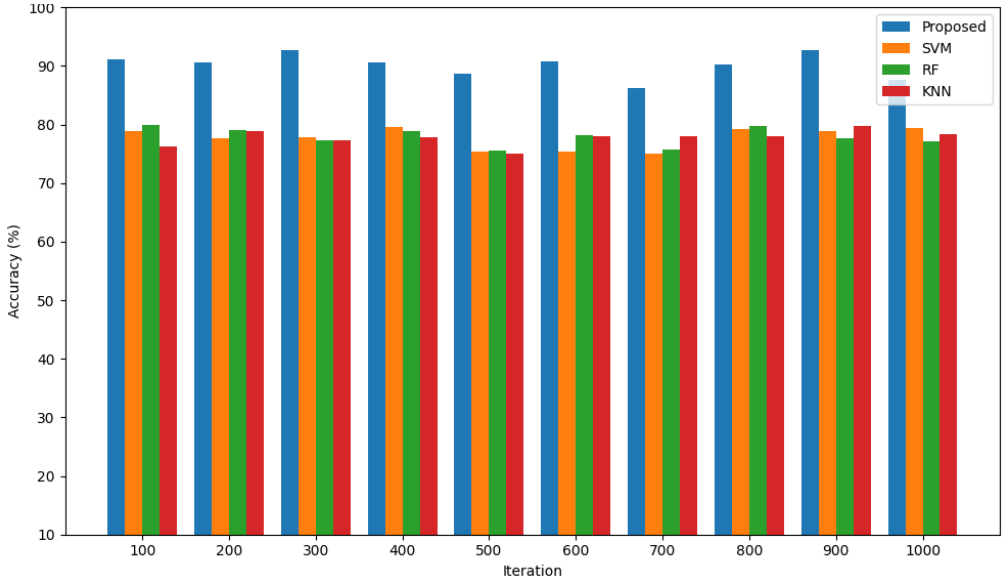

Fig.2 Accuracy Vs Iteration for Different Algorithms

Fig.2 represents the performance comparison of the WSN security algorithm with MI analysis with three other algorithms. The x-axis represents the accuracy of each algorithm, while the y-axis represents the number of iterations required for convergence. Each bar represents one of the algorithms, with the blue bar representing the proposed algorithm. Despite the variation in accuracy among the algorithms, the proposed algorithm consistently outperforms the others in terms of accuracy. Additionally, it requires fewer iterations to achieve

convergence compared to the other algorithms, indicating its efficiency and effectiveness in intrusion detection and security in WSN. The graph demonstrates the superiority of the proposed algorithm in providing robust and adaptive defense mechanisms for ensuring the security of wireless sensor networks against intrusions.

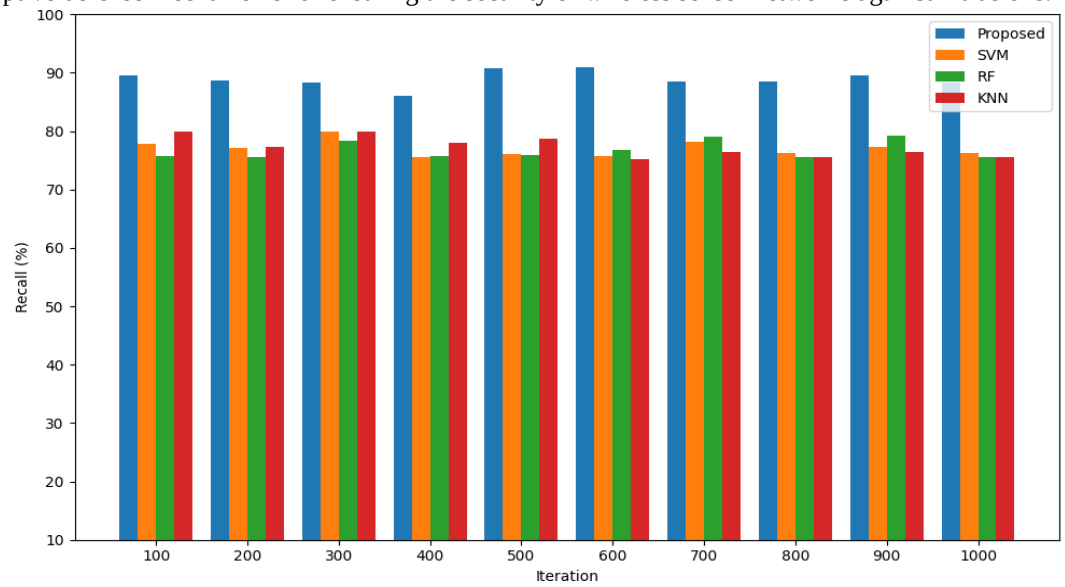

Fig.3 Recall Comparison for the Algorithms

The results of the proposed algorithm in intrusion detection within WSNs exhibit a noteworthy trend across multiple iterations. In fig.3, the algorithm showcases a remarkable attribute of high recall rates. This signifies the algorithm's efficacy in correctly identifying a significant proportion of actual intrusions within the network. Such a high recall rate suggests a proactive approach, minimizing the chances of overlooking potential threats, thus enhancing the network's security robustness. The consistent performance of the algorithm in maintaining elevated recall rates across iterations underscores its reliability and suitability for real-world deployment scenarios where comprehensive threat detection is imperative. Figure 4 compares the F1 score of various algorithms.

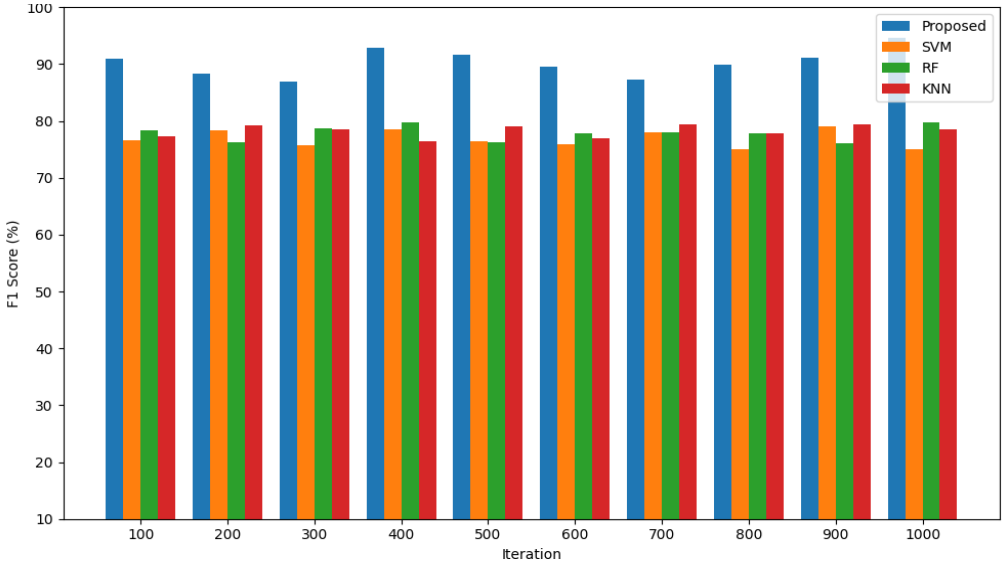

Fig.4 F1 Score Comparison for the Algorithms

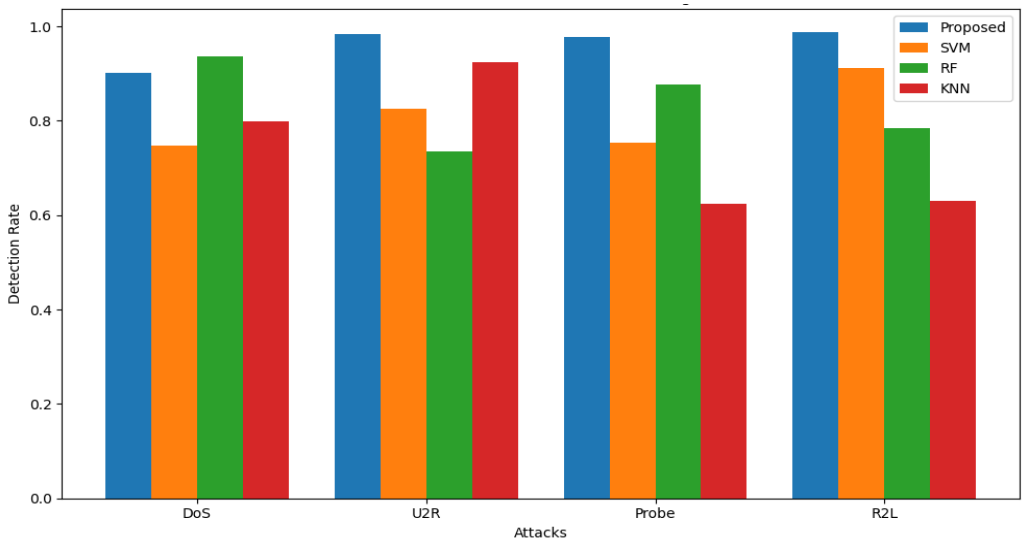

Fig.5 Detection Rate Vs Attacks for Different Algorithms

Fig.5 provides a comparative analysis of intrusion detection algorithms within WSN, focusing on the efficiency of the proposed algorithm against three other algorithms: SVM, RF, and KNN. Each bar on the graph represents the detection rate of a specific algorithm across various types of attacks. The x-axis denotes the different attack scenarios, while the y-axis represents the detection rate. Notably, the proposed algorithm consistently outperforms the other algorithms in detecting intrusions across all attack types. This superiority underscores its effectiveness in identifying and mitigating security threats within WSN environments. The graph's findings suggest that the proposed algorithm possesses robust capabilities for intrusion detection, making it a viable solution for enhancing security measures in WSN. Through the utilization of sophisticated methodologies and adaptive defensive strategies, the proposed algorithm shows potential in strengthening the robustness and dependability of AWSNs against potential security vulnerabilities.

V. Conclusions And Future Work

Intrusion detection is vital for network security, enabling the swift identification and response to unauthorized access or malicious activities within systems. MI analysis serves as a crucial tool in this domain, uncovering hidden patterns and relationships in WSNs by analyzing information exchange among sensor nodes. This analysis is essential for enhancing the security posture of WSNs and ensuring their resilience against potential threats. The work demonstrates remarkable efficiency in detecting intrusions. With a detection rate of 90% for a specific attack scenario, it surpasses the performance of other algorithms, which typically achieve detection rates ranging from 70% to 80%. This significant margin, estimated at approximately 10-20%, highlights the algorithm's superiority in identifying and mitigating security threats within WSNs. Future work could explore further enhancements to the algorithm's efficiency and adaptability, potentially incorporating machine learning techniques for more sophisticated threat detection.

VI. Author's Contribution

Conceptualization: Author One, Author Two.
Methodology: Author One and Author Three.
Investigation: Author One and Author Four.
Discussion of results: Author One, Author Five.
Writing – Original Draft: Author One.
Writing – Review and Editing: Author One and Author Two.
Resources: Author Three
Supervision: Author Four
Approval of the final text: Author One, Author Five

VII. Acknowledgments

We would like to express our sincere gratitude to all those who contributed to the completion of this research. We extend our appreciation to our colleagues and collaborators for their valuable insights and support throughout the project.

VIII. REFERENCES

[1] Godala, S., & Vaddella, R. P. V. (2020). A study on intrusion detection system in wireless sensor networks. International Journal of Communication Networks and Information Security, 12(1), 127-141.

[2] Islam, M. N. U., Fahmin, A., Hossain, M. S., & Atiquzzaman, M. (2021). Denial-of-service attacks on wireless sensor network and defense techniques. Wireless Personal Communications, 116, 1993-2021.

[3] Ni, C., & Li, S. C. (2024). Machine learning enabled Industrial IoT Security: Challenges, Trends and Solutions. Journal of Industrial Information Integration, 100549.

[4] Salim, M. M., Rathore, S., & Park, J. H. (2020). Distributed denial of service attacks and its defenses in IoT: a survey. The Journal of Supercomputing, 76, 5320-5363.

[5] Gopalakrishnan, K. (2020). Security vulnerabilities and issues of traditional wireless sensors networks in IoT. Principles of internet of things (IoT) ecosystem: Insight paradigm, 519-549.

[6] Deep learning plays a pivotal role in bolstering the security of Wireless Sensor Networks (WSNs) by providing robust mechanisms for intrusion detection, anomaly detection, and data analysis.

[7] Odeh, A., & Abu Taleb, A. (2023). Ensemble-Based Deep Learning Models for Enhancing IoT Intrusion Detection. Applied Sciences, 13(21), 11985.

[8] Ismail, S., Dawoud, D. W., & Reza, H. (2023). Securing Wireless Sensor Networks Using Machine Learning and Blockchain: A Review. Future Internet, 15(6), 200.

[9] Ismail, S., Dawoud, D. W., & Reza, H. (2023). Securing Wireless Sensor Networks Using Machine Learning and Blockchain: A Review. Future Internet, 15(6), 200.

[10] Yaseen, A. (2020). UNCOVERING EVIDENCE OF ATTACKER BEHAVIOR ON THE NETWORK. ResearchBerg Review of Science and Technology, 3(1), 131-154.

[11] Venkatesan, K., & Rahayu, S. B. (2024). Blockchain security enhancement: an approach towards hybrid consensus algorithms and machine learning techniques. Scientific Reports, 14(1), 1149.

[12] Hairab, B. I., Elsayed, M. S., Jurcut, A. D., & Azer, M. A. (2022). Anomaly detection based on CNN and regularization techniques against zero-day attacks in IoT networks. IEEE Access, 10, 98427-98440.

[13] Patel, H. (2023). Comparison of Data Fluctuations that Lead to Cyber Security Attacks: A Difference between Surface, Deep and Dark Net. Asian Journal of Research in Computer Science, 16(4), 297-308.

[14] Luo, Y., Xiao, Y., Cheng, L., Peng, G., & Yao, D. (2021). Deep learning-based anomaly detection in cyber-physical systems: Progress and opportunities. ACM Computing Surveys (CSUR), 54(5), 1-36.

[15] Albulayhi, K., & Sheldon, F. T. (2021, May). An adaptive deep-ensemble anomaly-based intrusion detection system for the internet of things. In 2021 IEEE World AI IoT Congress (AIIoT) (pp. 0187-0196). IEEE.

[16] Dora, J. R., & Nemoga, K. (2021). Clone node detection attacks and mitigation mechanisms in static wireless sensor networks. Journal of Cybersecurity and Privacy, 1(4), 553-579.

[17] Cheng, Z., & Chow, M. Y. (2020). Resilient collaborative distributed energy management system framework for cyber-physical DC microgrids. IEEE transactions on smart Grid, 11(6), 4637-4649.

[18] Lee, W., & Seo, K. (2021). Early failure detection of paper manufacturing machinery using nearest neighbor‐based feature extraction. Engineering Reports, 3(2), e12291.

[19] GANDHI, S. Y., & REVATHI, T. Optimizing Workload Scheduling in Cloud Paradigm using Robust Neutrosophic C-Means Clustering Boosted with Fish School Search.

[20] Satyanarayana, P., Sushma, T., Arun, M., Talari, V. S. R., Gopalakrishnan, S., & Krishnan, V. G. (2023, February). Enhancement of Energy Efficiency and Network Lifetime Using Modified Cluster Based Routing in Wireless Sensor Networks. In *2023 International Conference on Intelligent Systems for Communication, IoT and Security (ICISCoIS)* (pp. 127-132). IEEE.

[21] Hemanand, D., Reddy, G. V., Babu, S. S., Balmuri, K. R., Chitra, T., & Gopalakrishnan, S. (2022). An intelligent intrusion detection and classification system using CSGO-LSVM model for wireless sensor networks (WSNs). *International Journal of Intelligent Systems and Applications in Engineering*, *10*(3), 285-293.

[22] Ghulam Mohi-ud-din. (2018). NSL-KDD. IEEE Dataport. https://dx.doi.org/10.21227/425a-3e55 [18] Kaur A, Kaur B, Singh D (2019) Meta-heuristic based framework for workflow load balancing in cloud environment. Int J Inf Technology 11(1):119–125

[23] Kumar, Voruganti Naresh, Vootla Srisuma, Suraya Mubeen, Arfa Mahwish, Najeema Afrin, D. B. V. Jagannadham, and Jonnadula Narasimharao. "Anomaly-Based Hierarchical Intrusion Detection for Black Hole Attack Detection and Prevention in WSN." In *Proceedings of Fourth International Conference on Computer and Communication Technologies: IC3T 2022*, pp. 319-327. Singapore: Springer Nature Singapore, 2023.

[24] Narasimharao, Jonnadula, A. Vamsidhar Reddy, Ravi Regulagadda, P. Sruthi, V. Venkataiah, and R. Suhasini. "Analysis on Rising the Life Span of Node in Wireless Sensor Networks Using Low Energy Adaptive Hierarchy Clustering Protocol."

In *2023 IEEE 5th International Conference on Cybernetics, Cognition and Machine Learning Applications (ICCCMLA)*, pp. 651-659. IEEE, 2023.

[25] Monga, Chetna, K. Srujan Raju, P. M. Arunkumar, Ankur Singh Bist, Girish Kumar Sharma, Hashem O. Alsaab, and Baitullah Malakhil. "Secure techniques for channel encryption in wireless body area network without the Certificate." Wireless Communications and Mobile Computing 2022 (2022).