INTRUSION-TOLERANT SINK CONFIGURATION: A KEY TO PROLONGED LIFETIME IN WIRELESS SENSOR NETWORKS

By

VAIBHAV KAPIL

* Assis

doi

Date Received: 05/06/2024 Date Revised: 15/07/2024 Date Accepted: 12/08/2024

ABSTRACT

This study investigates the pivotal role of sink configuration in enhancing the lifetime of Wireless Sensor Networks (WSNs). A comparative analysis between configurations employing 2 sinks and 3 sinks reveals that the latter significantly outperforms in terms of network longevity. The study delves into the integration of an intrusion-aware protocol, providing resilience during security breaches. This protocol stabilizes network lifetime amidst intrusion attacks, crucial for maintaining system efficiency. This work introduces a novel machine learning model tailored for WSNs, exhibiting superior accuracy on a WSN-specific dataset. Through these combined efforts, comprehensive approach to improving WSN lifetime, encompassing sink configuration optimization, intrusion tolerance, and innovative machine learning techniques.

Keywords: Multi-Sink Wireless Sensor Network, Precision Agriculture, Intrusion-tolerance, Sink Configuration, Network Longevity

INTRODUCTION

Wireless Sensor Networks (WSNs) have witnessed a significant rise in applications across various domains, with Precision Agriculture (PA) emerging as a prominent field. The integration of WSNs into agricultural practices has introduced a positive impact on reducing network installation costs, where the adoption of wireless technology has successfully eliminated up to 80 percent of the expenses associated with traditional wiring methods (Wang et al., 2006). In precision agriculture, sensor nodes played a pivotal role in reporting acquired measurements to a central collector or sink. While some scenarios involved direct transmission to the sink, others employed data aggregation at sensor nodes before transmitting the condensed data (Corke et al., 2010). It becomes evident that the presence of multiple sinks is necessary to address the challenges posed by network lifetime and the need for efficient data collection.

WSNs in precision agriculture face numerous challenges with the conventional single sink architecture. The limited network lifetime and the inherent constraints related to the number of hops adversely affect the scalability and efficiency of the system.

This research focuses on evaluating the impact of sink configuration on the network's overall lifespan. The performance of WSNs employing 1 sink, 2 sinks, and 3 sinks is compared. Multiple, redundant sinks in a Wireless Sensor Network (WSN) yields several advantages as:

- Distributing the burden of data collection among multiple sinks.
- Mitigating the sink hole problem.
- Decreasing the total number of hops experienced by a packet.
- Offering infrastructure support across multiple

i-manager Publications
Member of:

This paper has objectives related to SDG

interfaces, if necessary.

- Enhancing the overall longevity of the network.
- Eliminating the risk of a single point failure.

The susceptibility of WSNs to intrusion attacks poses a critical threat to the stability and reliability of these networks. Intrusion incidents can disrupt normal operation, leading to potential data compromise and degradation of the network's performance. This study investigates the vulnerabilities introduced by intrusion attacks and their implications for the entire WSN.

An intrusion-tolerant sink configuration strategy is proposed to tackle these challenges, with the goal of prolonging network lifetime. This approach involves the deployment of three sinks, a configuration that comparative analysis indicates significantly outperforms alternatives. Additionally, an intrusion-aware protocol is introduced to stabilize network lifetime during intrusion events.

A specialized machine learning model is developed, comparing the Receiver Operating Characteristic (ROC) of a decision tree with the final ensemble voting method on a WSN dataset to enhance security measures. Findings underscore the effectiveness of the proposed solution in not only extending network lifetime but also ensuring stability during intrusion attacks, thus contributing to the overall resilience and efficiency of WSNs in precision agriculture.

1. Related Works

Several research efforts have explored strategies to enhance the lifetime and security of Wireless Sensor Networks (WSNs) in various application domains, including precision agriculture. This review highlights key contributions relevant to the work, focusing on grid deployment configurations, intrusion-aware routing protocols, and machine learning for intrusion detection in WSNs

1.1 Grid Deployment with Varying Sinks

Grid deployment significantly influences the lifetime of Wireless Sensor Networks (WSN), especially in precision agriculture. Galmes (2006) emphasizes its positive impact, recommending grid patterns for various applications. Diaz et al. (2011) and Ferentinos et al. (2005) aligned on the importance of grid deployment in precision agriculture, suggesting sizes of 30m x 30m and 20m x 20m, respectively. This consensus underscored the critical role of grid deployment in ensuring the longevity and efficiency of WSNs in precision agriculture.

Heinzelman et al. (2000) and Yick et al. (2008) investigated multi-sink configurations, observing significant lifetime improvements compared to single-sink scenarios.

These studies primarily focused on general network topologies and did not delve into optimizing sink placement algorithms within specific deployment patterns like grids. This work shares the focus on multisink configurations, it specifically analyzes a 5x5 grid deployment in the context of precision agriculture, a context often neglected in previous research. While existing studies analyze network performance based on hop count, this study additionally incorporates energy consumption metrics for a more comprehensive evaluation.

1.2 Intrusion-Aware Routing

Securing WSNs against intrusion attacks is crucial for maintaining network stability and reliability. Deng et al. (2006) and Pan et al. (2021) proposed Intrusion Detection Systems (IDS) for WSNs, highlighting the importance of identifying and mitigating malicious activities. These approaches primarily focused on signature-based or anomaly-based detection techniques, which may not be adaptable to diverse attack scenarios.

The proposed intrusion-aware routing protocol differentiates itself by utilizing a 'second-best route' selection strategy, actively avoiding compromised nodes during data transmission. A quantitative evaluation will assess the effectiveness of this method in mitigating the impact of attacks on network lifetime compared to existing IDS-based solutions.

1.3 Machine Learning for Intrusion Detection

Leveraging machine learning techniques for intrusion detection in WSNs has gained significant traction. Cheng and Zhu (2015) and Zhang et al. (2008) demonstrated the

potential of utilizing machine learning models trained on WSN-specific datasets to identify anomalous sensor readings indicative of attacks. Concerns remained regarding the computational efficiency of such models on resource-constrained sensor nodes.

Building upon the work of Ananthakumar et al. (2015) explored an ensemble voting approach based on KNN for intrusion detection in WSNs. The model leveraged multiple KNN classifiers trained on diverse feature subsets, aiming to achieve improved detection performance and robustness against various attack scenarios.

This work develops a resource-efficient machine learning model specifically designed for WSN intrusion detection, utilizing a WSN-specific dataset. The performance metrics of the model (accuracy, false positives) will be compared with existing approaches, emphasizing its computational efficiency and suitability for deployment on sensor nodes

1.4 Addressing Gaps and Contribution

Although existing research provides valuable insights, gaps remain in understanding the most effective ways to:

- The benefits of varying sink configurations are combined with intrusion tolerance mechanisms to optimize network lifetime in specific deployment patterns (e.g., grid).
- Machine learning models tailored for WSNs that balance accuracy with computational efficiency are designed.
- Evaluating the impact of varying sink configurations (1, 2, 3) on network lifetime within a grid deployment in the context of precision agriculture.
- Introducing an intrusion-aware routing protocol that avoids compromised nodes and selects "second-best" routes, mitigating the impact of attacks on network lifetime.

By bridging these gaps, this research provides valuable insights and novel solutions for enhancing the lifetime and security of WSNs in precision agriculture.

2. Methodology and Approach

This study employs a grid-based deployment pattern, with the size of the grid varying between 10m x 10m and 40m x 40m, adapting to the desired node density, following the insights provided by Ghosh et al. (2018). The nodes within this grid are tasked with measuring soil moisture levels and are programmed to report data only when the measured values fall below a pre-defined threshold. The deployment pattern exclusively follows a grid structure, providing a systematic and controlled environment for assessing the impact of sink configurations on Wireless Sensor Network (WSN) performance in precision agriculture.

Figure 1 shows a 10x10 grid of blue dots representing sensor nodes. Within the grid, three red squares denote the sink nodes strategically positioned to optimize data collection and network efficiency. This configuration highlights the spatial distribution and the critical role of sinks in the network.

The effectiveness of sink configurations is evaluated by considering three distinct scenarios: 1-sink, 2-sink, and 3-sink configurations. The sinks are strategically positioned, maintaining a fixed placement in each case. This configuration choice is motivated by its potential advantages, including distributed data collection, mitigation of the sinkhole problem, reduced packet hop count, infrastructure support across multiple interfaces, and overall enhancement of network longevity.

2.1 Intrusion-Aware Routing Protocol

The proposed intrusion-aware routing protocol serves as a

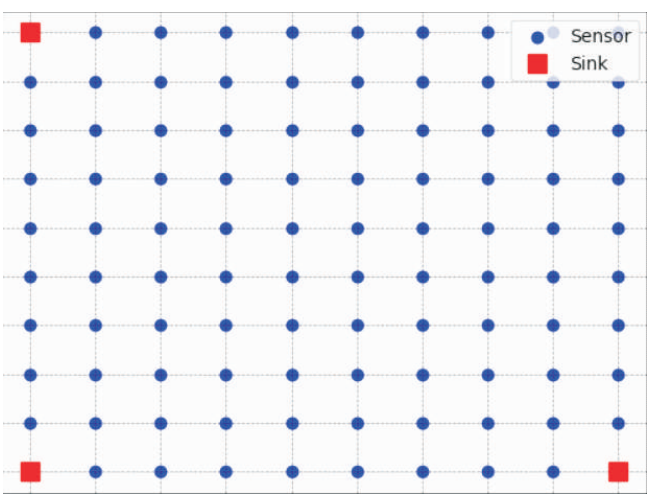

Figure 1. Grid Deployment in WSN with 3 Sinks

robust defense mechanism to strengthen the Wireless Sensor Network (WSN) against potential intrusions in precision agriculture settings. The protocol's methodology is designed to detect and mitigate the impact of compromised nodes, ensuring the security and reliability of data transmission within the network.

The protocol employs a sophisticated anomaly-based Intrusion Detection System (IDS) to identify affected nodes. This IDS combines statistical metrics and machine learning techniques, establishing a baseline for normal node behaviour. Irregularities, indicative of potential compromises, are detected by monitoring parameters such as communication patterns, energy consumption, and abnormal routing behaviour.

Figure 2 shows a visualization of the 10x10 grid Wireless Sensor Network (WSN). In this figure, sensors are represented by circles, sinks are indicated by squares, and a designated corrupted region is marked with an 'X'. Upon detecting a corrupted node, the protocol initiates a dynamic route reconfiguration process, activating the Backup Routing Strategy. Instead of relying on the compromised route, the protocol strategically selects an alternative path for data transmission. The criteria for determining this alternative path encompass factors such as hop count, link quality, energy efficiency, and dynamic adaptability to real-time network conditions.

2.2 Methodology for Backup Routing Strategy

- *Continuous Monitoring:* The protocol continuously monitors network conditions, updating its knowledge with real-time data regarding node behaviour and link quality.
- *Anomaly Detection:* Upon identifying an anomaly in a sensor node, the protocol marks the node as corrupted region, triggering the Backup Routing Strategy.
- *Route Evaluation:* Potential alternative routes are evaluated based on predefined criteria, emphasizing minimal hop count, reliable links, and energy efficiency.
- *Route Reconfiguration:* Upon identifying an alternative route, the protocol reconfigures the routing tables of adjacent nodes, shifting traffic away from the compromised node.
- *Adaptive Learning:* The protocol incorporates adaptive learning mechanisms to continuously refine its Backup Routing Strategy, ensuring adaptability to evolving network dynamics and intrusion patterns.

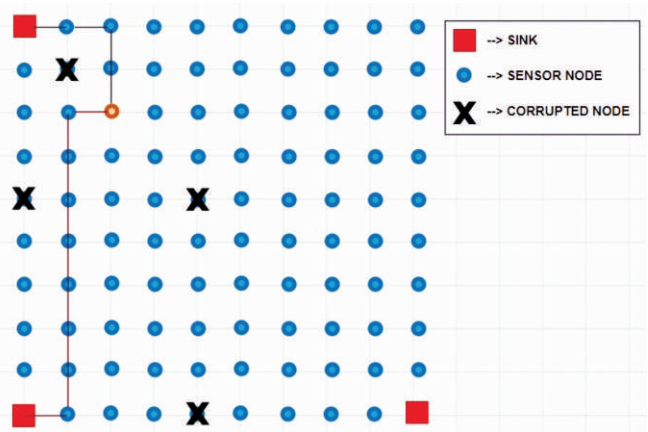

Figure 2. Corrupted Region in WSN

2.3 Dataset

The research leverages the Wireless Sensor Network Dataset (WSNDS), a publicly available dataset curated for the purpose of developing and evaluating intrusion detection systems within Wireless Sensor Networks (WSNs). This dataset serves as a crucial component in understanding and mitigating security threats within the context of WSNs.

A comprehensive Table 1 is shown below, outlining essential attributes of the Wireless Sensor Network Dataset (WSNDS). This dataset, specifically curated for the development and evaluation of intrusion detection systems in Wireless Sensor Networks (WSNs), boasts a significant size, encompassing a total of 374,662 rows. The extensive dataset ensures a diverse array of data

Features	Description
Time	Timestamp of data entries
Is_CH	Indicator of whether a node is a Cluster Head
Dist_To_CH	Distance of a node to its Cluster Head
DATA_S	Data sent from a sensor node
DATA_R	Data received at a sensor node
Attack type	Classification of the type of attack

Table 1. Wireless Sensor Network Dataset (WSNDS) Characteristics

points, crucial for in-depth analysis and understanding, addressing security threats within the realm of WSNs.

The dataset encompasses various attack scenarios encountered in WSNs, providing a realistic representation of security challenges. The attack types include but are not limited to normal behaviour, flooding attacks, grey hole attacks, and TDMA-based attacks. The dataset includes various attack scenarios observed in WSNs, providing a realistic representation of security challenges. The attack types comprise normal behavior, flooding attacks, grey hole attacks, and TDMA-based attacks, among others. The dataset undergoes preprocessing, including handling missing data, feature selection, and label encoding of categorical variables, before model development to ensure it is ready for machine learning applications.

2.4 Machine Learning Model

This model adopts a detailed approach to intrusion detection in Wireless Sensor Networks (WSNs) by employing a sophisticated neural network architecture implemented using TensorFlow and Keras. The design of the network involves a dense (hidden) layer with a Rectified Linear Unit (ReLU) activation function, striking a balance between complexity and expressiveness with 64 strategically chosen units. The input shape is designed to match the feature count present in the dataset. The output layer, utilizing a Soft max activation function, consists of 5 units representing distinct attack types found in the dataset. The model configuration incorporates binary cross entropy loss and the Adam optimizer, optimizing its learning capabilities for effective intrusion detection.

Key strategies are implemented to enhance efficiency and generalization during the training phase. A dynamic learning rate adjustment, facilitated by a callback mechanism, accelerates convergence and mitigates the risk of local minima. The model undergoes training for 20 epochs with a carefully selected batch size of 64, finding a delicate balance between computational efficiency and learning accuracy. A dedicated validation set is employed to monitor the model's performance on unseen data, preventing overfitting and ensuring robust generalization.

For the evaluation of the model's effectiveness, a suite of standard metrics is applied. Accuracy gives a complete view of overall classification accuracy, while the confusion matrix provides detailed insights into true positives, false positives, true negatives, and false negatives for each attack type. The ROC-AUC score quantifies the model's ability to distinguish between normal and attack instances, enriching the evaluation framework.

The research utilizes ensemble learning to improve accuracy and strengthen robustness. Individual classifiers, including decision trees, random forests, and KNNs, are trained independently. Predictions from these diverse classifiers are then aggregated through ensemble voting, harnessing the strengths of each learning algorithm.

3. Results and Discussions

The outcomes of the intrusion detection methodology in Wireless Sensor Networks (WSNs) are analyzed, followed by a comprehensive discussion of the implications and significance of the findings. The exploration includes key metrics, comparative analyses, and a thorough examination of the proposed approach's contribution to the overarching goal of enhancing WSN longevity.

3.1 Sink Configuration Optimization for WSN Longevity

The impact of sink configuration on the network lifetime in a 5x5 Wireless Sensor Network (WSN). The initial setup involves a single sink, and data transmission from each source node to this sink resulted in a total of 71 hops. Configurations with 2 and 3 sinks were then explored, strategically placed at opposite corners.

The graphical representation of the sink configuration shown in Figure 3 further underscores the network optimization achieved through multi-sink configurations. The consistent reduction in hops across varying sink numbers visually emphasizes the enhanced efficiency derived from employing multiple sinks. This efficiency results in the substantial minimization of communication distances between nodes and sinks.

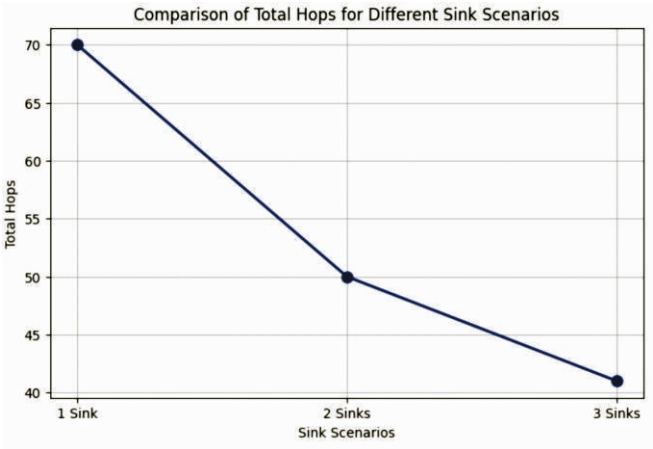

Figure 3. Comparative analysis of Total Hops for Different Sink Scenarios

Various parameters in the deployment mode of a grid with three sinks further assess the impact of sink configuration on network lifetime. Table 2 below shows the network parameters for grid deployment.

The investigation demonstrates a clear correlation between sink configuration and network lifetime in a 5x5 Wireless Sensor Network. The estimated lifetime in rounds increases progressively: with three sinks, it is 114,529.70 rounds; with two sinks, 93,914.35 rounds; and with one sink, 67,081.68 rounds. The graphical representation is shown below in Figure 4.

Referencing the work "Double Sink Energy Hole Avoidance Strategy for Wireless Sensor Network" by Chen et al. (2020), the study proposes an alternative approach to the conventional double sink strategy. Findings indicate that deploying three sinks suggests better performance, addressing energy hole challenges and contributing to an extended operational lifespan of the network. This perspective offers a fresh insight into optimizing the performance of wireless sensor networks.

3.2 Impact of Intrusion Aware Routing Protocol

The results are discussed along with the implications of the

Parameters	Values
Deployment mode	Grid
No. of sinks	1,2,3
Path loss exponent	3
Packet size	4000 bits
Initial energy of nodes	1 joule
Node density	0.0001

Table 2. Network Parameters for Grid Deployment

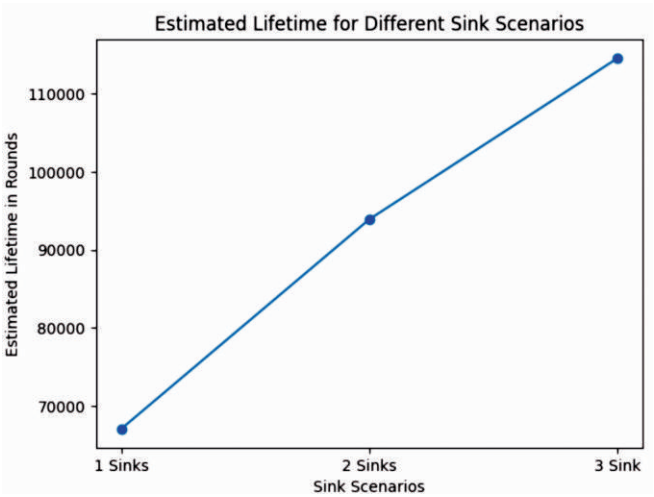

Figure 4. Comparative Analysis of Network Lifetime for Different Sink Scenarios

intrusion-aware routing methodology in a 10x10 Wireless Sensor Network (WSN) with three sinks. The focus is on three scenarios: without intrusion, with intrusion, and utilizing the backup routing strategy.

The recorded energy consumption stands at 399.06 in the absence of intrusion, when an intrusion is introduced, the recorded energy consumption rises to 423.84, exceeding the baseline scenario. The implementation of the intrusion-aware routing methodology, specifically incorporating a backup routing strategy, results in a more controlled energy consumption of 401.82. This approach effectively addresses the intrusion, mitigating its impact and optimizing energy usage, thereby showcasing its potential to improve the network's resilience and longevity.

Figure 5 shows the comparative energy consumption across different scenarios, reinforcing the importance of intrusion-aware routing methodologies in sustaining network performance.

Rathod and Mehta (2011) highlighted the critical impact of intrusion and security attacks on the energy sustainability of Wireless Sensor Networks (WSNs). Stressing the imperative of energy conservation, their survey underscored the necessity of intrusion-aware routing strategies. These approaches, by addressing intrusion vulnerabilities, played a crucial role in preserving energy resources. The essence lay in fortifying WSNs against security threats to ensure both data integrity and

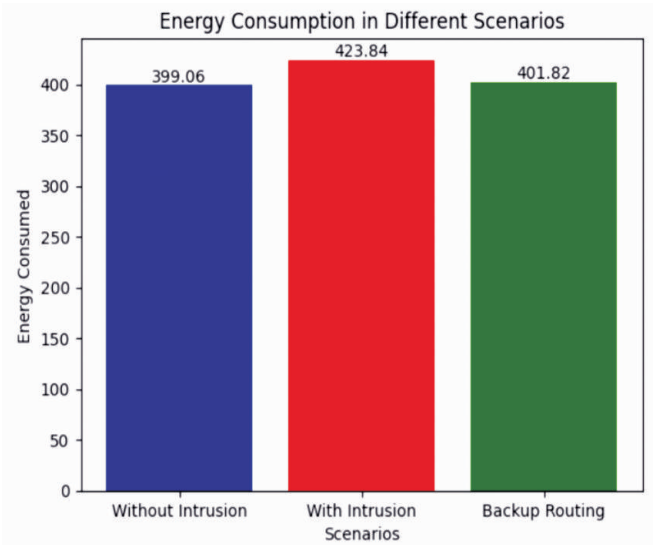

Figure 5. Comparison of Energy Consumption in Different Scenarios

prolonged network life through effective energy management strategies.

3.3 Machine Learning Model Evaluation and Discussion

The intrusion detection model's training progress using a neural network is examined. The following table provides a snapshot of the model's performance across 20 epochs, highlighting the loss and accuracy metrics at each stage of the training process. This chronological overview serves as a foundation for understanding the model's learning dynamics and progression over time.

The Table 3 shows a comprehensive overview of the model's training dynamics over 20 epochs. A discernible pattern emerges as the model refines its understanding of the dataset.

Epoch	Loss	Accuracy	Val_Loss	Val_Accuracy
1	142.7704	0.869	66.8121	0.9077
2	71.5865	0.8938	70.1611	0.9156
3	58.8003	0.9044	17.6915	0.9326
4	50.6646	0.9117	31.1581	0.9319
5	41.8638	0.9169	17.9424	0.9374
6	36.2407	0.9228	47.3756	0.922
7	31.3776	0.9235	46.5024	0.9243
8	25.6763	0.9255	8.7991	0.9435
9	20.669	0.9268	15.6048	0.9301
10	16.6886	0.9295	21.0485	0.8835
11	13.5471	0.9315	16.0031	0.9362
12	11.1875	0.9343	12.033	0.9285
13	8.0697	0.9373	13.9446	0.9187
14	5.6849	0.94	2.3599	0.9462
15	3.6845	0.9389	4.1932	0.9238
16	2.0271	0.9357	1.02	0.9211
17	0.1799	0.9116	0.0934	0.9174
18	0.0996	0.9095	0.1014	0.907
19	0.1154	0.9078	0.1147	0.907
20	0.1056	0.9078	0.0956	0.907

Table 3. Epoch Progression: Loss and Accuracy Metrics

A substantial decrease is observed in both training and validation losses, accompanied by a steady increase in accuracy metrics. This signifies the successful learning and adaptation of the neural network to the intricacies of the Wireless Sensor Networks (WSNs) dataset

Around the middle of the training process (epochs 10-15), there is a detailed interplay between accuracy and loss. While the training accuracy continues to climb, the validation accuracy experiences a slight dip, indicating the need for careful model tuning to prevent overfitting. The model exhibits robustness, as seen in the consistent validation accuracy in the latter epochs, ultimately reaching an impressive 93.62%. Below is a visual representation of the training and validation trends over the 20 epochs. The graph provides a concise visualization of the model's learning trajectory, offering insights into the convergence and generalization capabilities.

In Figure 6 the graphical representation shows a complementary insight into the observed trends, enhancing understanding of the model's performance throughout the training phase. The convergence of loss and the ascent of accuracy depicted in the graph corroborate the quantitative metrics presented in the table, further solidifying the efficacy of the intrusion detection model.

The detailed analysis of the neural network training progression across epochs revealed detailed trends in accuracy and loss metrics. Fortifying the intrusion detection system involved complementing the neural network with diverse classifiers, each contributing unique strengths to the ensemble. This led to the employment of individual classifiers, mentioned in the table. These classifiers, each with its distinctive approach to learning and decision-making, form the foundation of the ensemble learning strategy. The following table presents the individual accuracies achieved by each classifier on the dataset.

Table 4 shows the effectiveness of each standalone

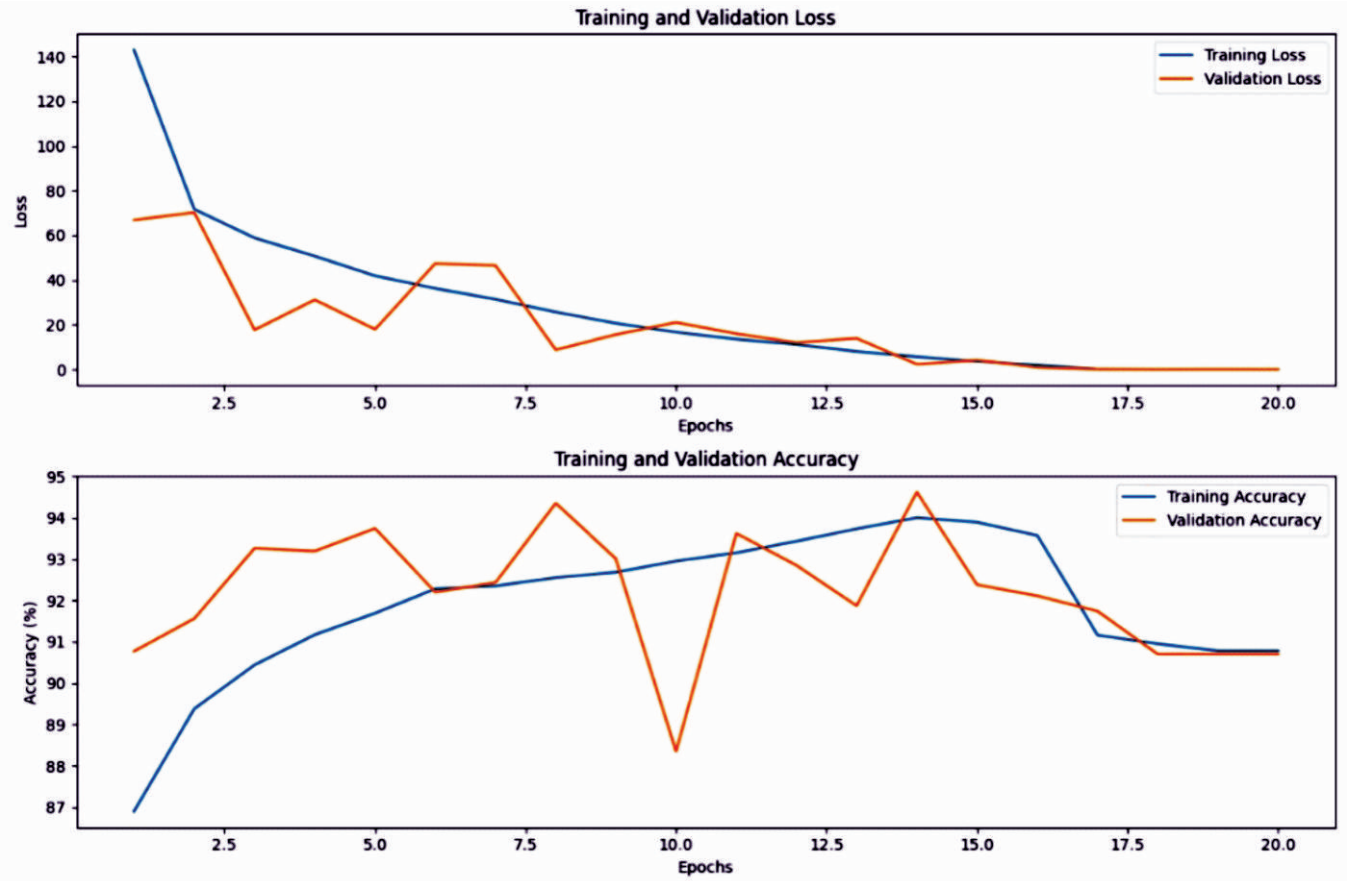

Figure 6. Training and Validation Loss, Training and Validation Accuracy Graph

classifier in discerning patterns and making accurate predictions. The KNN classifier outperformed the others, achieving a remarkable accuracy of 98.11%. This aligns with its inherent ability to capture complex relationships within the data, making it particularly well-suited for intrusion detection tasks.

The strengths of each classifier in Figure 7 were recognized and integrated into an ensemble learning framework, utilizing the power of ensemble voting. The ensemble achieved an exceptional accuracy of 98.70%, surpassing the individual classifiers and further enhancing the overall robustness of the intrusion detection system.

The intrusion detection methodology, combining neural network training and ensemble learning, shows notable effectiveness in Wireless Sensor Networks.

The integration of diverse classifiers, with KNN standing out with an accuracy of 98.11%, enhances the overall system robustness. The ensemble approach, particularly leveraging KNN, offers potential for advancing the accuracy and reliability of intrusion detection systems in Wireless Sensor Networks.

Conclusion

The study explores the complexities of enhancing the lifetime and security of Wireless Sensor Networks (WSNs) in precision agriculture, with a primary focus on sink configuration optimization, intrusion tolerance, and the integration of machine learning models. Through a systematic exploration, valuable insights have been uncovered and novel solutions proposed to address critical challenges in WSN deployment.

Comparative analysis of sink configurations (1 sink, 2 sinks, and 3 sinks) within a 5x5 grid deployment illuminates the profound impact on network longevity. The results prove that deploying three sinks significantly outperforms alternatives, leading to extended operational lifespans.

Classifier	Accuracy
Decision Tree	95.87%
Random Forest	97.18%
KNN classifier	98.11%
Ensemble	98.70

Table 4. Performance Summary of Classifiers

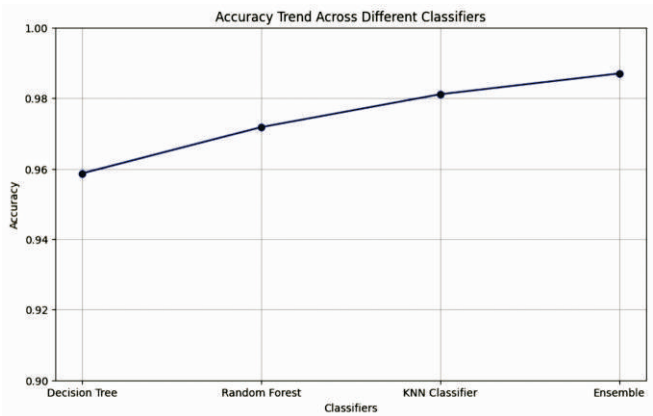

Figure 7. Classifier Performance Overview

This finding challenges conventional approaches, suggesting a potential strategy for addressing energy hole challenges and optimizing WSN performance in precision agriculture.

The introduction of an intrusion-aware sink configuration strategy serves as a robust defence mechanism against potential intrusions. The proposed protocol, complemented by a backup routing strategy, PROVES its effectiveness in mitigating the impact of compromised nodes. The visual representation of energy consumption across different scenarios underscores the importance of intrusion-aware routing methodologies in sustaining network performance and energy efficiency.

In the realm of machine learning for intrusion detection, the study contributes a detailed approach. The developed neural network, in conjunction with ensemble learning, proves to be a powerful tool for identifying and mitigating security threats in WSNs. The KNN classifier emerges as a standout performer, achieving an impressive accuracy of 98.11%. The ensemble, incorporating diverse classifiers, attains a remarkable accuracy of 98.70%, showcasing the robustness and reliability of our intrusion detection system.

The research bridges critical gaps in existing literature by combining varying sink configurations, intrusion tolerance mechanisms, and tailored machine learning models. The proposed solutions provide a comprehensive framework for optimizing network lifetime, addressing security concerns, and ensuring the resilience and efficiency of WSNs in precision agriculture.

The findings lay the groundwork for future research directions. Exploring the adaptability of the approach to diverse deployment patterns, considering additional environmental factors, and enhancing the computational efficiency of machine learning models are promising avenues for further investigation. Overall, this study contributes to the advancement of WSN research and offers practical insights for designing robust and efficient systems in precision agriculture and beyond.

References

[1]. Ananthakumar, A., Ganediwal, T., & Kunte, A. (2015). Intrusion detection system in wireless sensor networks: A review. *International Journal of Advanced Computer Science and Applications,* 6(12), 131-139.

[2]. Chen, S., Huang, Q., Zhang, Y., & Li, X. (2020). Double sink energy hole avoidance strategy for wireless sensor network. *EURASIP Journal on Wireless Communications and Networking,* 2020(1), 226.

https://doi.org/10.1186/s13638-020-01837-8

[3]. Cheng, P., & Zhu, M. (2015). Lightweight anomaly detection for wireless sensor networks. *International Journal of Distributed Sensor Networks,* 11(8), 653232.

https://doi.org/10.1155/2015/653232

[4]. Corke, P., Wark, T., Jurdak, R., Hu, W., Valencia, P., & Moore, D. (2010). Environmental wireless sensor networks. *Proceedings of the IEEE,* 98(11), 1903-1917.

https://doi.org/10.1109/JPROC.2010.2068530

[5]. Deng, J., Han, R., & Mishra, S. (2006). INSENS: Intrusion-tolerant routing for wireless sensor networks. *Computer Communications,* 29(2), 216-230.

https://doi.org/10.1016/j.comcom.2005.05.018

[6]. Díaz, S. E., Pérez, J. C., Mateos, A. C., Marinescu, M. C., & Guerra, B. B. (2011). A novel methodology for the monitoring of the agricultural production process based

on wireless sensor networks. *Computers and Electronics in Agriculture,* 76(2), 252-265.

https://doi.org/10.1016/j.compag.2011.02.004

[7]. Ferentinos, K. P., Tsiligiridis, T. A., & Arvanitis, K. G. (2005, July). Energy optimization of wireless sensor networks for environmental measurements. In *Proceedings of the International Conference on Computational Intelligence for Measurment Systems and Applicatons (CIMSA)* (Vol. 51, pp. 1031-1051).

[8]. Galmes, S. (2006, October). Lifetime issues in wireless sensor networks for vineyard monitoring. In *2006 IEEE International Conference on Mobile Ad Hoc and Sensor Systems* (pp. 542-545). IEEE.

https://doi.org/10.1109/MOBHOC.2006.278605

[9]. Ghosh, K., Neogy, S., Das, P. K., & Mehta, M. (2018). Intrusion detection at international borders and large military barracks with multi-sink wireless sensor networks: An energy efficient solution. *Wireless Personal Communications,* 98, 1083-1101.

https://doi.org/10.1007/s11277-017-4909-5

[10]. Heinzelman, W. R., Chandrakasan, A., & Balakrishnan, H. (2000, January). Energy-efficient communication protocol for wireless microsensor networks. In *Proceedings of the 33rd Annual Hawaii International Conference on System Sciences* (pp. 10-pp). IEEE.

https://doi.org/10.1109/HICSS.2000.926982

[11]. Pan, J. S., Fan, F., Chu, S. C., Zhao, H. Q., & Liu, G. Y. (2021). A lightweight intelligent intrusion detection model for wireless sensor networks. *Security and communication Networks,* 2021(1), 5540895.

https://doi.org/10.1155/2021/5540895

[12]. Rathod, V., & Mehta, M. (2011). Security in wireless sensor network: A survey. *Ganpat University Journal of Engineering & Technology,* 1(1), 35-44.

[13]. Wang, N., Zhang, N., & Wang, M. (2006). Wireless sensors in agriculture and food industry—Recent development and future perspective. *Computers and Electronics in Agriculture,* 50(1), 1-14.

https://doi.org/10.1016/j.compag.2005.09.003

[14]. Yick, J., Mukherjee, B., & Ghosal, D. (2008). Wireless sensor network survey. *Computer Networks,* 52(12), 2292-2330.

https://doi.org/10.1016/j.comnet.2008.04.002

[15]. Zhang, W., Liu, Y., Das, S. K., & De, P. (2008). Secure data aggregation in wireless sensor networks: A watermark based authentication supportive approach. *Pervasive and Mobile Computing,* 4(5), 658-680.

https://doi.org/10.1016/j.pmcj.2008.05.005

ABOUT THE AUTHORS

D