A Reliable Hybrid Framework for Anomaly Detection in Secure and Robust Wireless Sensor Networks

Gajjala Savithri
Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India | Department of Animation, Dr. YSR Architecture and Fine Arts University, Kadapa, AP, India
savithrigreddy@gmail.com

N. Raghavendra Sai
Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Hyderabad-500075, Telangana, India
nallagatlaraghavendra@kluniversity.in (corresponding author)

Received: 14 April 2025 | Revised: 13 May 2025 | Accepted: 31 May 2025

 DOI: https://doi.org/10.48084/etasr.11494

ABSTRACT

The integration of the FireTG-Net model enables Firefly Swarm Optimization (FSO) to work with the Temporal-Gated Recurrent Unit-Network (Temporal-GRU-Net) for detecting anomalies in Wireless Sensor Networks (WSNs) resulting in 98.13% detection accuracy. The model employs FSO-optimized trust evaluation for local and global assessments that enables it to automatically adjust its detection methods to changing conditions and improve the efficiency of routing decisions. The model identifies immediate and changing malicious behaviors of blackhole, sinkhole, and jamming attacks through its 1D convolutional layers and advanced Gated Recurrent Units (GRUs) feature extraction capabilities. The FireTG-Net model exhibits superior evaluation scores compared to the Decision Tree (96%), Fuzzy Model (81%) and Trust-aware Routing Protocol (TRP) (96.791%) while facing disruptions better and showing restricted latency effects. FireTG-Net demonstrates excellent capabilities for enhancing the security and reliability of WSNs through its effective performance regarding high packet delivery ratio, enhanced energy efficiency, and reduced false positive rates.

Keywords-wireless sensor networks; trust; FSO; anomaly detection optimization; GRU

I. INTRODUCTION

Wireless Sensor Networks (WSNs) have emerged as a critical component in modern communication and monitoring systems, with applications in a variety of fields including environmental monitoring, healthcare, military, and smart cities [1-4]. These networks are made up of spatially distributed sensor nodes that communicate and work together to gather and transmit data [5-9]. However, WSNs' inherent resource constraints, such as limited energy, computational power, and bandwidth, combined with their deployment in open and frequently hostile environments, make them vulnerable to security threats [10-12]. Malicious attacks, such as blackhole, sinkhole, and jamming, can jeopardize network integrity, data confidentiality, and overall performance, necessitating the creation of strong and adaptable trust-based security mechanisms [13, 14].

Authors in [15] proposed a trust-aware clustering approach that uses the (Low-Energy Adaptive Clustering Hierarchy) LEACH protocol to achieve an impressive packet delivery ratio of 95.8%. This method demonstrated high reliability in cluster-based wireless communication systems, ensuring data integrity while transmitting. However, its reliance on LEACH limits its adaptability in highly dynamic network environments, where cluster-head selection mechanisms need more flexibility to accommodate frequent topology changes.

Authors in [16] developed a decision tree-based mechanism that achieved 96% detection accuracy. The approach effectively addressed decision-making challenges in trust management by developing a strong classification framework. While the model performed well in scenarios with well-defined decision parameters, its reliance on pre-determined feature hierarchies restricts scalability and generalization in complex and evolving datasets, where feature importance can change dynamically.

Authors in [17] investigated a data association algorithm using iterative clustering techniques, which demonstrated

improved performance in trust management scenarios. This method allowed for more effective data point association by iteratively refining cluster configurations. Despite its iterative design, which provides significant precision, the computational overhead introduced during multiple iterations presents challenges in real-time applications, particularly in resource-constrained environments.

Authors in [18] presented an adaptive trust model based on fuzzy logic, which achieved an 81% detection accuracy. The fuzzy logic system enabled more nuanced decision-making by capturing uncertainties and ambiguities in trust computations. However, the moderate detection accuracy highlights its limitations in addressing diverse or large-scale datasets, where the design of fuzzy membership functions and rule sets may become more complex and resource-intensive.

Authors in [19] proposed a Trust-aware Routing Protocol (TRP) that focuses on packet forwarding mechanisms, with a detection accuracy of 96.791%. This protocol effectively incorporated trust evaluation into routing decisions, which improved network security and data transmission reliability.

Several existing approaches have been proposed to improve the security and reliability of WSNs by utilizing trust evaluation frameworks and machine learning techniques. Unlike traditional intrusion detection methods that primarily rely on static rule sets or signature-based detection, trust-based models like FireTG-Net provide dynamic adaptability to evolving network behaviors. Trust-based approaches continuously assess node behavior over time, enabling early identification of subtle and emerging threats that static methods may overlook. This adaptability is crucial for WSNs, where node conditions and communication patterns can frequently change due to mobility, energy variations, or environmental factors, making trust-based systems inherently more effective and resilient.

The proposed FireTG-Net model aims to address these limitations by integrating Firefly Swarm Optimization (FSO) with the Temporal-Gated Recurrent Unit-Network (Temporal-GRU-Net) into a hybrid framework for anomaly detection and trust-based routing. FireTG-Net detects malicious nodes in real time by combining local and global trust evaluations with advanced spatial and temporal feature analysis. The model's ability to dynamically adapt to changing network conditions ensures resilience to disruptions, lower energy consumption, and faster packet delivery.

II. PROPOSED SYSTEM

FireTG-Net combines the benefits of FSO and the Temporal-GRU-Net deep learning architecture to improve the detection of malicious nodes and adapt to changing conditions in WSNs. The methodology, as illustrated in Figure 1, aims to improve security, resilience, and data transmission efficiency by utilizing both spatial and temporal information from network nodes. It combines local and global behavioral analysis to form a comprehensive trust model, which is then used for anomaly detection and adaptive routing to reduce the impact of malicious attacks and disruptions.

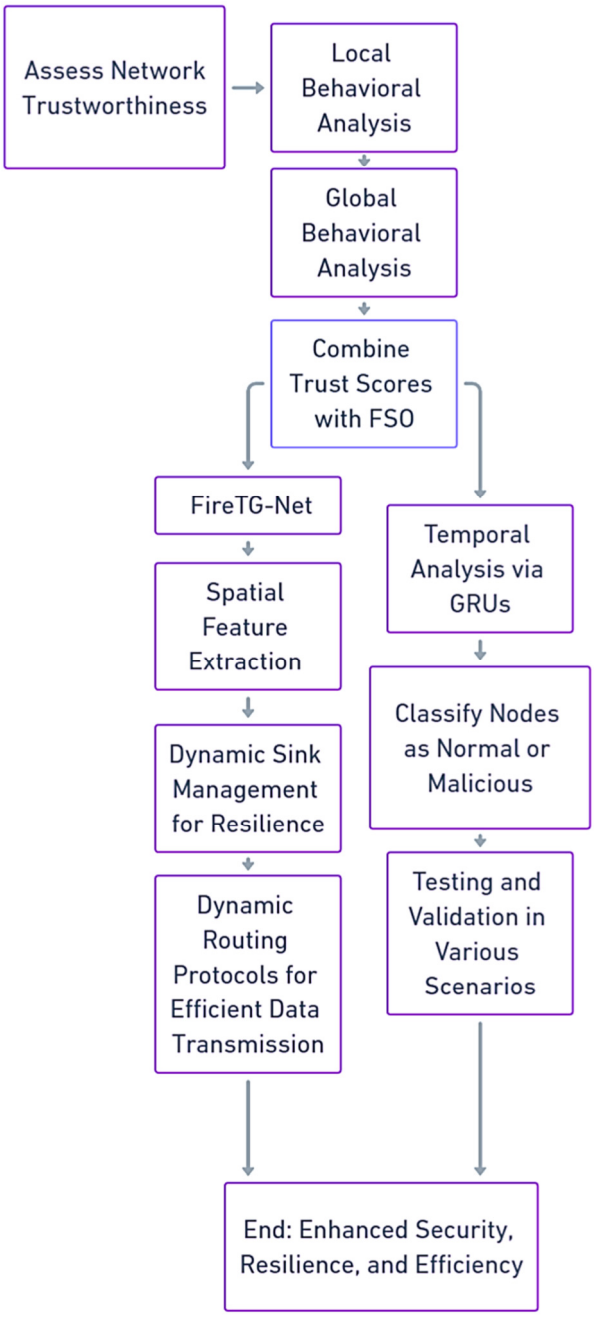

Fig. 1. Proposed FireTG-Net system methodology.

The first step in the methodology involves local and global behavioral analysis. Each node in the network assesses its trustworthiness by calculating trust scores for its immediate neighbors using spatial metrics such as packet delivery rates, routing consistency, and node response time:

$$TL = w1 \cdot PDR + w2 \cdot RC + w3 \cdot NRT \quad (1)$$

where:

- PDR is the packet delivery rate.
- RC it the routing consistency.

- NRT is the node response time.
- $w1,\ w2,\ w3$ are the weights assigned to each factor.

Similarly, the global trust score is calculated as:

$$TG = w4 \cdot NR + w5 \cdot EC + w6 \cdot TA \quad (2)$$

where:

- NR is the node reliability.
- EC is the energy consumption.
- TA are the traffic anomalies.
- $w4, w5, w6$ are the weights assigned to the global metrics.

Local trust evaluations enable nodes to assess the behavior of their neighbors in real time. Simultaneously, a central node or gateway collects network-wide metrics that reflect the network's overall behavior. This includes node reliability, activity patterns, energy consumption rates, and traffic anomalies. To provide a balanced and comprehensive understanding of the network, the local and global trust scores are combined. This combined trust score is optimized with FSO, which adaptively weighs local and global inputs based on the network's current state.

The combined trust score (TC) is calculated using FSO as follows:

$$TC = \alpha \cdot TL + \beta \cdot TG \quad (3)$$

where α and β are the dynamic weights optimized by FSO.

The second step involves hybrid anomaly detection via FireTG Net. Instead of relying solely on traditional neural networks, FireTG-Net employs a hybrid approach that combines FSO and Temporal-GRU-Net for advanced anomaly detection. The system accepts input features such as trust scores, packet drop rates, node energy levels, and traffic flow rates, processing them both spatially and temporally. FireTG-Net's architecture employs 1D convolutional layers to extract spatial features and identify node behaviors, as well as advanced Gated Recurrent Units (GRUs) for temporal analysis, which enables the model to track how node behavior changes over time.

The spatial feature extraction step applies 1D convolution:

$$Fs = Conv1D(Fi, K) \quad (4)$$

where:

- Fi is the input feature vector.
- K is the convolution kernel matrix.
- Fs denotes the extracted spatial features.

The temporal analysis step uses GRUs to track evolving behaviors over time:

$$h_t = GRU(Fs, h_{t-1}) \quad (5)$$

where:

- h_t denotes the GRU hidden state at time t.
- h_{t-1} is the previous GRU hidden state.

This combination allows the system to detect both immediate and evolving patterns in the network. FireTG-Net is trained on labeled data containing both normal and malicious behaviors, such as blackhole attacks, data tampering, and sink disruptions. Once trained, FireTG-Net classifies nodes as normal or malicious, assigning a probability score to each classification, allowing for precise identification of compromised nodes while minimizing false positives.

FireTG-Net outputs a malicious probability score (Pm):

$$Pm = \sigma(W \cdot h_t + b) \quad (6)$$

where:

- W is the weight matrix.
- b is the bias.
- σ is the sigmoid activation function.

In the third step, FireTG-Net ensures resilience against sink failures and network disruptions. Disruptions to WSNs, such as sink node failures, can have a significant impact on the network's operation. FireTG-Net addresses these issues using dynamic sink management.

The fourth step of the methodology focuses on the Efficient Routing Protocol (ERP). To select optimal data transmission paths, ERP considers trust scores, network topology, and traffic flow metrics. The routing algorithm selects paths dynamically based on several criteria, including maximizing packet delivery rates, minimizing routing latency, and avoiding malicious or compromised nodes. This ensures that the network remains efficient and secure, with consistent data transmission even in the event of an attack or disruption.

Finally, the testing and validation phase evaluates FireTG-Net's effectiveness in various network scenarios, such as different types of attacks and disruptions. These scenarios include blackhole attacks, sink node failures, and random node disruptions, which are common challenges for WSNs.

FireTG-Net offers a comprehensive approach for improving the security, resilience, and efficiency of WSNs. FireTG-Net can adapt to changing network conditions, detect malicious nodes, and ensure efficient routing, thereby improving the overall performance and reliability of WSNs in dynamic and challenging environments.

A. Proposed Model

The architecture of FireTG-Net, as depicted in Figure 2, integrates FSO with Temporal-GRU-Net, creating a hybrid model designed for dynamic anomaly detection in WSNs. The FSO component allows the system to optimize the trust scores by adjusting the weights of local and global information, making the model highly adaptive to changing network conditions. Temporal-GRU-Net combines 1D convolutional layers for spatial feature extraction with an advanced GRU for temporal analysis, enabling the model to track both immediate node behaviors and evolving patterns over time.

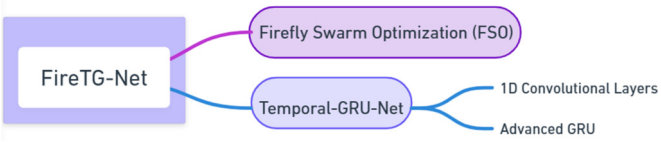

Fig. 2. Proposed FireTG-Net model architecture.

The novelty of FireTG-Net lies in its hybrid integration of FSO and Temporal-GRU-Net, combining the best of both worlds: adaptive optimization and advanced temporal feature learning. Compared to traditional anomaly detection systems that rely solely on static models or basic machine learning techniques, FireTG-Net provides a more dynamic and resilient solution for WSNs. FSO adapts the model in real-time to fluctuating network conditions, balancing local and global behavioral data. Temporal-GRU-Net, on the other hand, introduces a temporal dimension that captures evolving patterns of node behavior, which is a significant improvement over conventional models that typically analyze node behavior statically.

B. Algorithm of the Proposed Model

The following algorithm summarizes the core steps of the FireTG-Net model:

```
Algorithm: FireTG-Net model
Step 1: Initialize parameters
     %Set input features and model
     parameters
     InitializeModelParameters();
Step 2: Spatial feature extraction using
1D convolution
     %Input feature vector (Fi)
     Fs = conv1D(Fi, kernel); %Apply 1D
     convolution to extract spatial
     features
Step 3: Temporal analysis using GRU
     %Process spatial features (Fs)
     through GRU for temporal analysis
     ht = GRU(Fs, ht_prev); %Compute
     hidden state for time step t
Step 4: Node classification
     %Use GRU output to classify nodes
     Pm = sigmoid(W * ht + b); %Compute
     probability score for malicious
     behavior
Step 5: Output classification results
     disp('Malicious Node Probability:');
     disp(Pm); %Display probability score
```

C. Simulation Setup and Parameters

The simulation experiments were conducted using a custom network simulator developed in Python 3.8, utilizing TensorFlow 2.10 for deep learning components. The WSN consisted of 100 sensor nodes randomly deployed over a 500 m × 500 m area. The nodes were assumed to have a communication radius of 50 m and an initial energy of 2 J each. The attack models that were simulated included blackhole attacks, sinkhole attacks, selective forwarding, replay attacks, jamming, and sybil attacks. The dataset was synthetically generated based on network simulations, comprising 15,000 labeled records with features including packet delivery rates, routing consistency, node energy, traffic anomalies, and response time. For the FSO module, the following key parameters were set:

- Population size: 30 fireflies.
- Maximum iterations: 100.
- Absorption coefficient (γ): 1.0.
- Randomization parameter (α): 0.2.
- Attractiveness coefficient (β_0): 1.5.

The Temporal-GRU-Net was configured with the following architecture:

- 1D convolution layer: 64 filters, kernel size = 3, activation = ReLU.
- GRU layer 1: 128 units, activation = tanh.
- GRU layer 2: 64 units, activation = tanh.
- Dense layer: 1 output unit with sigmoid activation for binary classification.

The dataset was split into three sets: 70% for training, 15% for validation, and 15% for testing. All experiments were repeated over 10 independent simulation runs, and the average performance metrics were reported.

III. RESULTS AND ANALYSIS

The heatmap in Figure 3 provides a visual representation of trust scores for nodes over time, integrating both local (node-to-node) and global (network-wide) evaluations. Each row represents an individual node, and each column corresponds to a specific time point, with color intensity reflecting the trust level. Warmer colors, closer to red, indicate lower trust, whereas cooler colors, approaching blue, signify higher trust. This visualization highlights dynamic fluctuations in trust levels, with nodes exhibiting anomalies, such as consistently low trust (reddish areas), potentially signaling malicious or unreliable behavior.

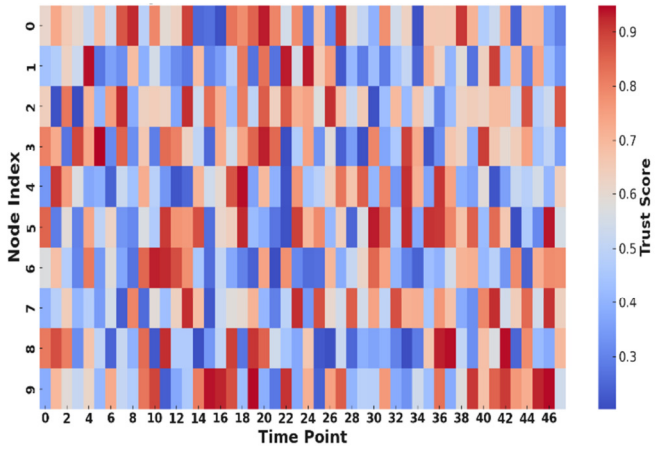

Fig. 3. Heatmap of combined trust scores.

The radar chart in Figure 4 illustrates the trust scores of individual nodes, with nodes maintaining consistently high trust levels. This indicates strong reliability and security, demonstrating that the network is functioning securely with minimal malicious activity. The confusion matrix in Figure 5 provides an in-depth evaluation of the model's performance in classifying nodes under various attack scenarios and normal behavior. It distinguishes between several types of attacks, including blackhole (nodes absorbing all packets), sybil (nodes presenting multiple identities), selective forwarding (nodes selectively dropping packets), replay (replayed packets causing confusion), jamming (nodes disrupting communication with interference), and sinkhole (malicious routing disrupting data flow), as well as normal nodes. The diagonal values (true positives) reflect the model's effectiveness in accurately identifying each attack type, with high values indicating strong classification performance.

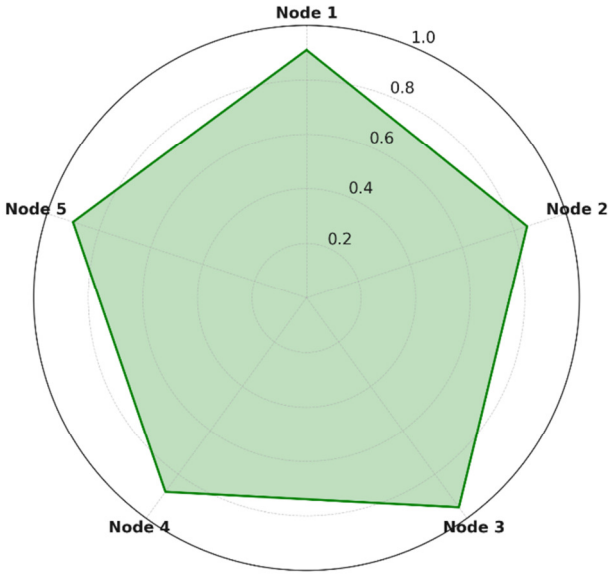

Fig. 4. Current trust levels of network nodes.

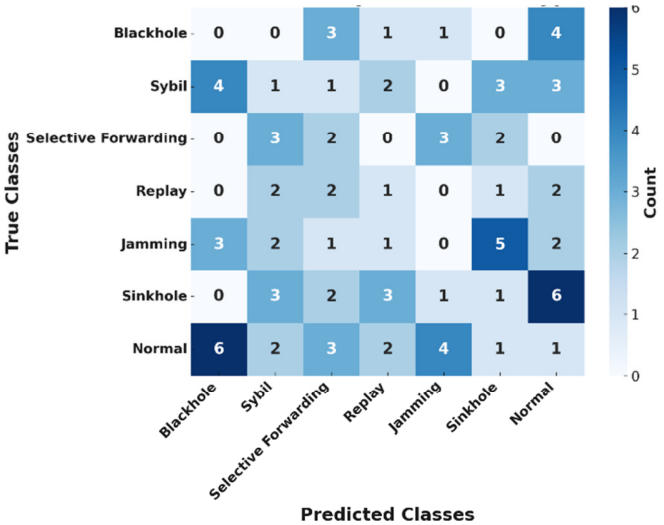

Fig. 5. Confusion matrix for specific attac types in WSNs.

The Precision-Recall (PR) curve in Figure 6 illustrates the trade-off between precision and recall for the model, highlighting its performance in anomaly detection. Precision represents the proportion of correctly identified anomalies among all predicted anomalies, whereas recall indicates the proportion of actual anomalies accurately detected by the model.

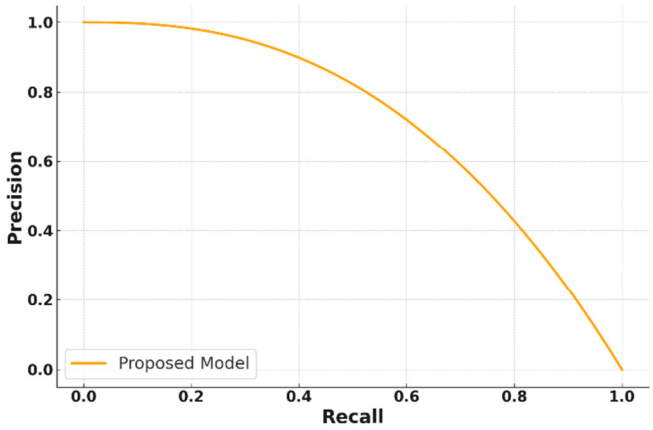

Fig. 6. Precision-recall curve of the proposed model.

The bar chart in Figure 7 illustrates the relative importance of key features used in the Adaptive Neural Detection (AND) model for anomaly detection, classifying nodes as normal or malicious under specific attack scenarios. The trust score (35%) is the most influential feature, reflecting the node's reliability based on both local and global evaluations. The packet drop rate (25%) is critical for identifying attacks like selective forwarding and blackhole, whereas the energy level (20%) plays a significant role in detecting energy-draining attacks such as replay and jamming. Traffic consistency (15%) helps monitor irregular traffic patterns caused by sybil or sinkhole attacks, and latency (5%) has a minor influence, primarily useful for detecting routing issues.

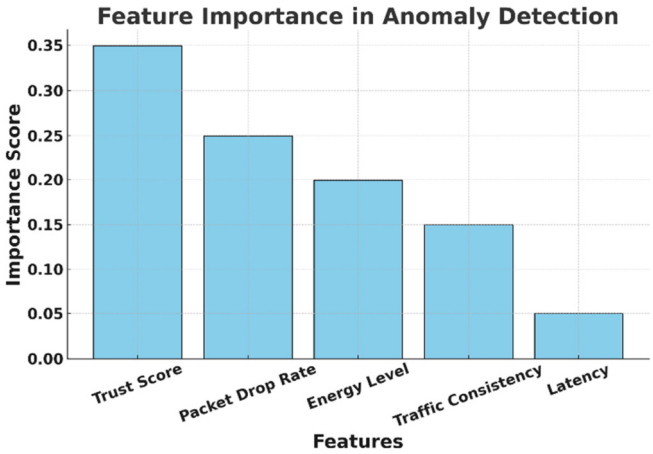

Fig. 7. Feature importance in anomaly detection.

Figure 8 illustrates the variation in trust scores for nodes during and after a disruption or attack, highlighting the resilience of the proposed model. During the disruption period (highlighted in red), the trust scores for specific nodes decrease due to the detection of malicious or abnormal behavior. Following the disruption, the recovery phase shows trust scores gradually recovering, reflecting the model's ability to restore trust through effective remediation and adaptive mechanisms.

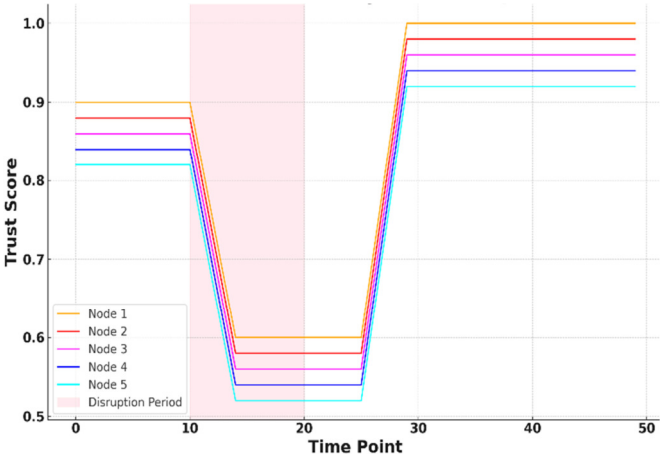

Fig. 8. Trust score variation during disruption and recovery.

Figure 9 illustrates the network throughput during both disruption and recovery phases. The disruption period, highlighted in red, shows only a slight decline in throughput during the attack, highlighting the proposed model's effectiveness in mitigating disruptions.

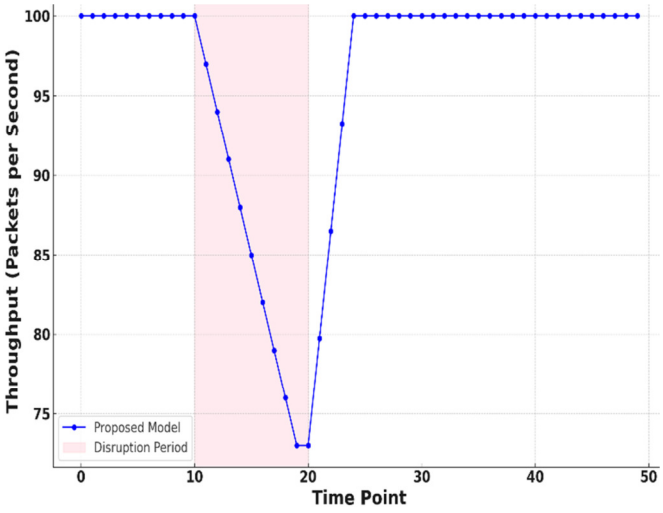

Fig. 9. Network throughput during disruption and recovery.

Figure 10 presents a bar chart (solid blue) demonstrating the minimal increase in latency during disruptions, thereby emphasizing the model's efficient handling of disruptions with a low delay impact.

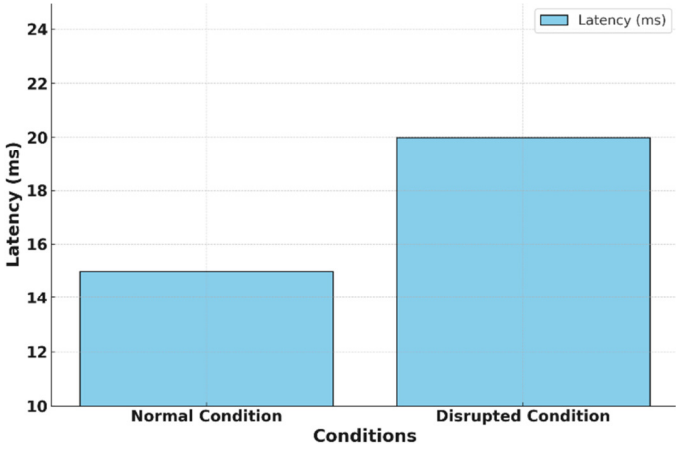

Fig. 10. Latency under normal and disrupted conditions.

The bar chart in Figure 11 (light green with hatching) highlights a high packet delivery ratio, with only a slight decline observed during disruptions. This demonstrates the model's robust performance in maintaining data integrity, ensuring that packet delivery remains strong even under adverse conditions, thereby confirming the model's resilience and reliability.

Fig. 11. Packet delivery ratio under normal and disrupted conditions.

The line plot in Figure 12 illustrates the frequency of detected anomalies across a 24-hour period. The steady and low rate of alerts reflects stable network behavior, with the system effectively detecting and minimizing anomalies.

The gauge chart in Figure 13 reflects a success rate of 98.2%, underscoring the superior performance of the proposed model in maintaining secure communications. The high success rate emphasizes the model's exceptional reliability in ensuring data confidentiality and integrity, with the dominance of the green section reinforcing the system's robustness. The minimal red zone indicates a negligible failure rate, further highlighting the model's effectiveness in securing communications and ensuring minimal risk of security breaches.

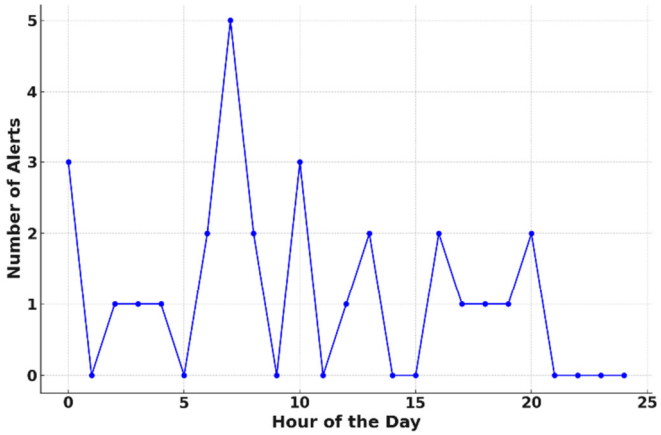

Fig. 12. Anomaly alerts over a 24-hour period.

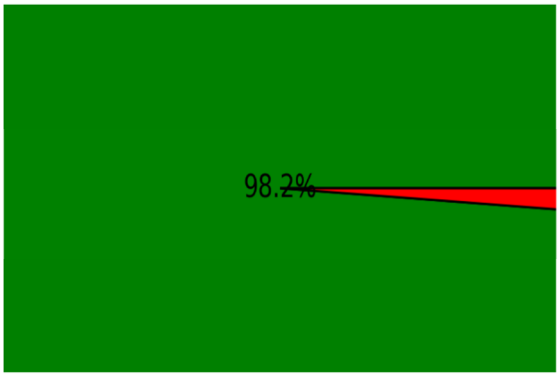

Fig. 13. Protocol integrity success rate.

Figure 14 shows the energy consumption under both normal and disrupted conditions. During normal operation, energy consumption remains consistent and low, reflecting the efficiency of the proposed model. In contrast, during the disruption period (highlighted in yellow), there is a slight increase in energy usage due to the additional computations required for anomaly detection and rerouting. However, the system quickly returns to normal energy consumption levels after the disruption. Figure 15 illustrates the detection accuracy of the proposed model over time, showing a consistent performance with an average accuracy of 98.13%. The minor fluctuations reflect the model's stable and reliable ability to identify anomalies, maintaining high accuracy throughout the evaluation period. Figure 16 presents a bar chart that showcases the model's detection accuracy for various attack types. The accuracy remains high across all attack scenarios, ranging from 98.0% to 98.25%, highlighting the model's robustness and reliability in handling diverse threats. To validate the consistency of the model's performance, 10 independent experimental runs were conducted and the standard deviation of detection accuracy was computed. The FireTG-Net model achieved an average detection accuracy of 98.13%, with a standard deviation of ±0.42%, indicating a high level of consistency and robustness across multiple runs. The narrow deviation range confirms that the model's performance is stable and reliable under varying experimental conditions. Incorporating this statistical validation further strengthens the confidence in the practical applicability of FireTG-Net for anomaly detection in WSNs.

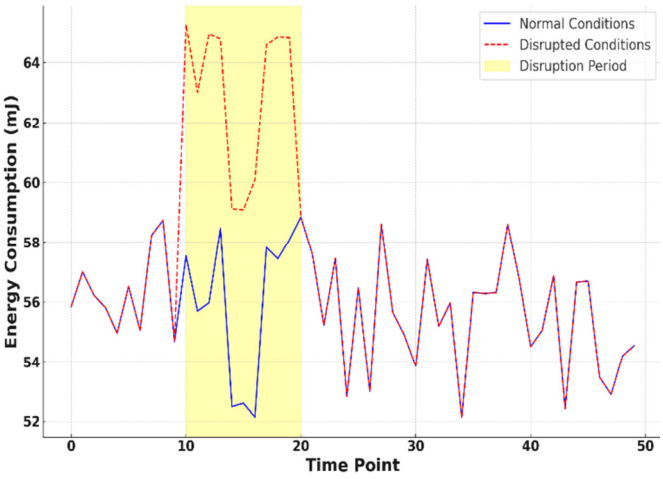

Fig. 14. Energy consumption during normal and disrupted conditions.

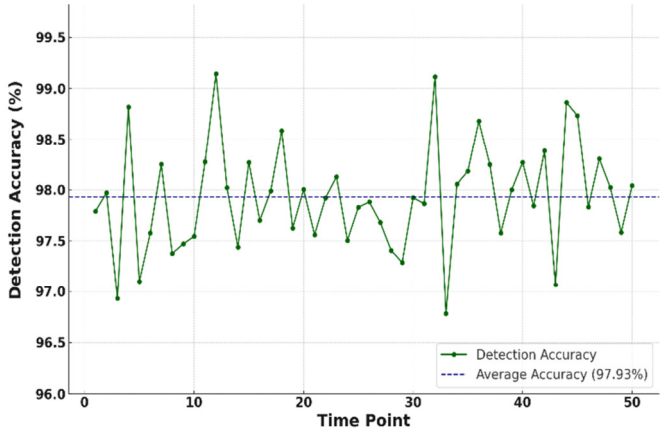

Fig. 15. Detection accuracy over time.

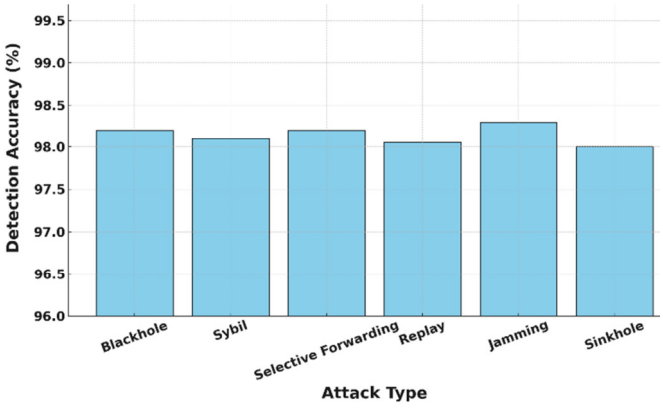

Fig. 16. Detection accuracy by attack type.

Table I and the bar plot in Figure 17 show the detection accuracy of different models, facilitating a comparison of their performance. The Decision Tree model achieved a 96% accuracy rate, demonstrating its reliability in trust evaluation

scenarios. The Fuzzy Model, despite leveraging nuanced decision-making through fuzzy logic, achieved a lower accuracy of 81%, highlighting potential limitations in complex environments. TRP achieved a slightly higher accuracy of 96.791%, demonstrating its ability to integrate trust metrics into routing mechanisms. The proposed model outperformed all other models, with an accuracy of 98.13%, demonstrating its superior ability to detect trust-related parameters.

TABLE I. DETECTION ACCURACY COMPARISON OF DIFFERENT MODELS

Model [Citation]	Detection accuracy (%)
Decision Tree [16]	96
Fuzzy Model [18]	81
TRP [19]	96.791
Proposed model	98.13

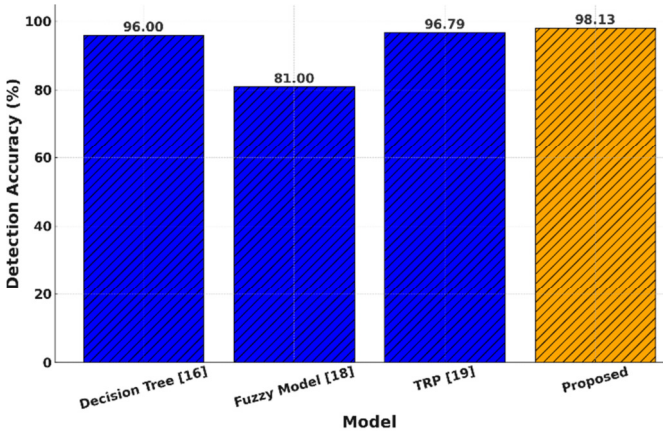

Fig. 17. Detection accuracy comparison of different models.

The practical applications of FireTG-Net extend across various domains in which WSNs are pivotal. For instance, in environmental monitoring, FireTG-Net can enhance the detection of anomalous sensor readings caused by faulty sensors or environmental interference, ensuring the accuracy and reliability of data crucial for real-time decision-making. In healthcare, FireTG-Net can be employed to secure WSNs used in patient monitoring systems, protecting sensitive health data from potential cyber-attacks while ensuring continuous operation. To evaluate the adaptability and scalability of FireTG-Net across different WSN scenarios, we conducted additional simulations under varying node densities and attack frequencies. The model maintained a high level of detection accuracy (above 97.5%) even when the node density was increased by 50% and when the attack frequency was doubled. This indicates that FireTG-Net effectively scales with network size and remains robust against intensified attack scenarios. Such adaptability demonstrates the model's practical viability for deployment in diverse WSN environments, including dense urban networks, large-scale environmental monitoring systems, and mission-critical sensor deployments.

IV. CONCLUSION AND SUMMARY

The FireTG-Net model has been demonstrated as an advanced approach to addressing security and reliability challenges in Wireless Sensor Networks (WSNs). By integrating local and global trust metrics with dynamic optimization through Firefly Swarm Optimization (FSO), the model effectively adapts to fluctuating network conditions. The Temporal-Gated Recurrent Unit-Network (Temporal-GRU-Net) enhances anomaly detection by capturing both immediate and evolving behaviors, enabling precise classification of attacks such as blackhole and sinkhole disruptions. The FireTG-Net model achieves a consistent detection accuracy of 98.13%, significantly improving the security and resilience of WSNs. It demonstrates strong capabilities in maintaining high packet delivery ratios, minimizing false positive rates, and ensuring efficient energy usage even under disruptive conditions. These findings imply that FireTG-Net is not only suitable for standard WSN scenarios but also highly effective for real-time and large-scale deployments where network dynamics and security threats are more pronounced. By enabling adaptive trust evaluation and robust anomaly detection, FireTG-Net contributes substantially to improving the reliability, scalability, and operational integrity of modern WSN infrastructures. For instance, the Decision Tree model, with a detection accuracy of 96%, and the Fuzzy Model, with an accuracy of 81%, demonstrate commendable capabilities yet fall short of addressing dynamic and complex network conditions as effectively as FireTG-Net, which achieves a detection accuracy of 98.13%. Furthermore, the Trust-aware Routing Protocol (TRP) exhibited a reduced performance with an accuracy of 96.791%. While FireTG-Net achieves a notable detection accuracy of 98.13% and demonstrates resilience against various cybersecurity threats in WSNs, it faces several challenges. The precision required in tuning the parameters of the FSO can be a limiting factor in environments with rapidly changing network conditions. Additionally, the computational intensity of the Temporal-GRU-Net may not be suitable for very resource-limited sensor nodes. During our experiments, we encountered difficulties related to these computational demands, particularly in real-time data processing, which highlighted the need for optimization strategies that can alleviate these constraints. Future research will focus on refining these aspects by exploring the potential of lightweight machine learning frameworks that maintain high accuracy while reducing the computational load.

Furthermore, managing dynamic network conditions, such as sudden node failures or unpredictable attack patterns, posed difficulties in maintaining real-time detection efficiency. The computational cost associated with training the Temporal-GRU-Net, particularly under large-scale network simulations, was another constraint that required careful resource management. Additionally, some assumptions were made during dataset generation, such as fixed communication ranges and uniform initial energy levels, which may differ from real-world deployments. Acknowledging these limitations not only enhances the transparency of this study but also highlights important areas for further optimization and real-world adaptation.

Several practical and research-oriented approaches are envisioned for future work to extend FireTG-Net's capabilities. Real-time deployment strategies will be explored to validate the framework under dynamic and operational WSN environments. Furthermore, the incorporation of energy-aware

trust modeling is planned to optimize network longevity by dynamically adjusting trust evaluations based on residual energy levels. Another promising direction involves enhancing the model's robustness against cross-layer attacks, where threats can simultaneously target multiple communication layers. Addressing these areas will further solidify FireTG-Net as a comprehensive and adaptable solution for securing large-scale and resource-constrained WSNs.

ACKNOWLEDGMENT

The author would like to thank N. Raghavendra Sai for his constant support and feedback. His remarks have made a significant contribution to this work.

REFERENCES

[1] N. Temene, C. Sergiou, C. Georgiou, and V. Vassiliou, "A Survey on Mobility in Wireless Sensor Networks," *Ad Hoc Networks*, vol. 125, Feb. 2022, Art. no. 102726, https://doi.org/10.1016/j.adhoc.2021.102726.

[2] H. Yang, X. Zhang, and F. Cheng, "A Novel Algorithm for Improving Malicious Node Detection Effect in Wireless Sensor Networks," *Mobile Networks and Applications*, vol. 26, no. 4, pp. 1564–1573, Aug. 2021, https://doi.org/10.1007/s11036-019-01492-4.

[3] A. Harbouche, D. Djabour, and A. Saiah, "Z-MSP: Zonal-Max Stable Protocol for Wireless Sensor Networks," *Engineering, Technology & Applied Science Research*, vol. 14, no. 6, pp. 18036–18041, Dec. 2024, https://doi.org/10.48084/etasr.8691.

[4] M. Huang, K. Zhang, Z. Zeng, T. Wang, and Y. Liu, "An AUV-Assisted Data Gathering Scheme Based on Clustering and Matrix Completion for Smart Ocean," *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 9904–9918, Oct. 2020, https://doi.org/10.1109/JIOT.2020.2988035.

[5] R. Liu, M. Xie, A. Liu, and H. Song, "Joint Optimization Risk Factor and Energy Consumption in IoT Networks With TinyML-Enabled Internet of UAVs," *IEEE Internet of Things Journal*, vol. 11, no. 12, pp. 20983–20994, Jun. 2024, https://doi.org/10.1109/JIOT.2023.3348837.

[6] N. Kumar and J.-H. Lee, "Peer-to-Peer Cooperative Caching for Data Dissemination in Urban Vehicular Communications," *IEEE Systems Journal*, vol. 8, no. 4, pp. 1136–1144, Dec. 2014, https://doi.org/10.1109/JSYST.2013.2285611.

[7] E. T. da Silva, A. L. D. Costa, and J. M. H. de Macedo, "On the realization of VANET using named data networking: On improvement of VANET using NDN-based routing, caching, and security," *International Journal of Communication Systems*, vol. 35, no. 18, Sep. 2022, Art. no. e5348, https://doi.org/10.1002/dac.5348.

[8] F. H. El-Fouly, M. Kachout, R. A. Ramadan, A. J. Alzahrani, J. S. Alshudukhi, and I. M. Alseadoon, "Energy-Efficient and Reliable Routing for Real-time Communication in Wireless Sensor Networks," *Engineering, Technology & Applied Science Research*, vol. 14, no. 3, pp. 13959–13966, Jun. 2024, https://doi.org/10.48084/etasr.7057.

[9] D. Manivannan, S. S. Moni, and S. Zeadally, "Secure authentication and privacy-preserving techniques in Vehicular Ad-hoc NETworks (VANETs)," *Vehicular Communications*, vol. 25, Oct. 2020, Art. no. 100247, https://doi.org/10.1016/j.vehcom.2020.100247.

[10] S. Mejjaouli and R. F. Babiceanu, "RFID-wireless sensor networks integration: Decision models and optimization of logistics systems operations," *Journal of Manufacturing Systems*, vol. 35, pp. 234–245, Apr. 2015, https://doi.org/10.1016/j.jmsy.2015.02.005.

[11] J. Zhang, X. Wang, B. Wang, W. Sun, H. Du, and Y. Zhao, "Energy-Efficient Data Transmission for Underwater Wireless Sensor Networks: A Novel Hierarchical Underwater Wireless Sensor Transmission Framework," *Sensors*, vol. 23, no. 12, Jun. 2023, Art. no. 5759, https://doi.org/10.3390/s23125759.

[12] F. Zijie, M. A. Al-Shareeda, M. A. Saare, S. Manickam, and S. Karuppayah, "Wireless sensor networks in the internet of things: review, techniques, challenges, and future directions," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 31, no. 2, pp. 1190–1200, Aug. 2023, https://doi.org/10.11591/ijeecs.v31.i2.pp1190-1200.

[13] D. Gangwani and P. Gangwani, "Applications of Machine Learning and Artificial Intelligence in Intelligent Transportation System: A Review," in *Applications of Artificial Intelligence and Machine Learning: Select Proceedings of ICAAAIML 2020*, Online, 2020, pp. 203–216, https://doi.org/10.1007/978-981-16-3067-5_16.

[14] J. Jiang, H. Wang, X. Mu, and S. Guan, "Logistics industry monitoring system based on wireless sensor network platform," *Computer Communications*, vol. 155, pp. 58–65, Apr. 2020, https://doi.org/10.1016/j.comcom.2020.03.016.

[15] Rekha and P. M. Sundaram, "Trust aware clustering approach for the detection of malicious nodes in the WSN," *The Scientific Temper*, vol. 15, no. spl-1, pp. 170–181, Oct. 2024, https://doi.org/10.58414/SCIENTIFICTEMPER.2024.15.spl.21.

[16] S. Shah *et al.*, "A Dynamic Trust evaluation and update model using advance decision tree for underwater Wireless Sensor Networks," *Scientific Reports*, vol. 14, no. 1, Sep. 2024, Art. no. 22393, https://doi.org/10.1038/s41598-024-72775-4.

[17] B. P. Valluri and N. Sharma, "Trusted head node for Node Behaviour Analysis for malicious node detection in wireless sensor networks," *Measurement: Sensors*, vol. 36, Dec. 2024, Art. no. 101159, https://doi.org/10.1016/j.measen.2024.101159.

[18] C. Liu, J. Ye, F. An, and W. Jiang, "An Adaptive Trust Evaluation Model for Detecting Abnormal Nodes in Underwater Acoustic Sensor Networks," *Sensors*, vol. 24, no. 9, May 2024, Art. no. 2880, https://doi.org/10.3390/s24092880.

[19] M. Asha Rani and H. R. Roopashree, "Enhancing Wireless sensor network security with Trust-aware Routing protocol(TRP)Based on packet Forwarding Ratio Analysis to detect malicious nodes," in *2024 International Conference on Knowledge Engineering and Communication Systems*, Chikkaballapur, India, 2024, vol. 1, pp. 1–7, https://doi.org/10.1109/ICKECS61492.2024.10616466.

AUTHORS PROFILE

G. Savithri is a research scholar in the Department of Computer Science and Engineering at Koneru Lakshmaiah Education Foundation, Vaddeswaram. She completed her M.Tech at AITS Rajampet, affiliated with JNTU Anantapur. She passed the UGC NET in December 2023. Currently, she serves as an Academic Consultant in the Department of Animation at Dr. YSR Architecture and Fine Arts University, Kadapa, Andhra Pradesh, India. Savithri has a notable academic career and substantial teaching experience at both undergraduate and postgraduate levels. Her research interests include deep learning, wireless sensor networks, computer networks, and blockchain technology. She has published numerous papers in international journals and conferences.

Dr. N. Raghavendra Sai is currently working as an Associate Professor in the Department of Computer Science and Engineering, KL University, Vaddeswaram. He completed his Ph.D. from Bharathiar University Coimbatore, and received his Master's Degree from Acharya Nagarjuna University. He is dedicated to the teaching field for the past 12 years and has published more than 60 papers in national and international journals and conferences. He also serves as a member of editorial boards and as a reviewer for various international journals. His research interests include artificial neural networks, artificial intelligence, data mining, support vector machines, face recognition, and classification algorithms.