Journal of Engineering Strategy and Innovation
Volume 1, Issue 1, July – September (2026) Arrived: 08/06/2026: Accepted: 27/06/2026

RESEARCH ARTICLE

An Adaptive Lightweight Energy Efficient AI Assisted Nomaly Detection with Real Time Threat Mitigation for Resource Constrained Wireless Networks

Sivakami S [1], Ariharan K [2], Kishore Raj D K [3]

[1] Department of Electronics and communication Engineering, New Prince Shri Bhavani College of Engineering and Technology Chennai, Tamil Nadu, India
[2] Department of Electronics and communication Engineering, New Prince Shri Bhavani College of Engineering and Technology Chennai, Tamil Nadu, India
[3] Department of Electronics and communication Engineering, New Prince Shri Bhavani College of Engineering and Technology Chennai, Tamil Nadu, India

[1] sivakami@newprinceshribhavani.com

Abstract—**Because of their restricted processing power, memory capacity, and battery limitations, resource-constrained wireless networks are more vulnerable to sophisticated cyberattacks. For wireless networks with limited resources, this study suggests a lightweight AI-assisted adaptive anomaly detection framework combined with an energy-efficient real-time threat mitigation mechanism. The suggested framework minimizes computing complexity by effectively analyzing both global traffic dependencies and sequential attack patterns using a lightweight hybrid Transformer-Gated Recurrent Unit (Transformer-GRU) model. In order to minimize false alarms, an adaptive anomaly threshold method dynamically modifies detection sensitivity in response to shifting network traffic patterns. In order to maintain network lifetime, an energy-aware mitigation technique also optimizes communication routing and selectively isolates harmful nodes. The suggested framework delivers better detection accuracy, a lower false positive rate, minimal computing overhead, and increased energy economy, according to experimental evaluation.**

Keywords—*Resource constrained networks, security, energy efficiency, anomaly detection, Gated Recurrent Unit (GRU).*

1. INTRODUCTION

Today's smart surroundings, such as the Internet of Things (IoT), smart healthcare, manufacturing mechanization, intelligent transportation systems, and environmental monitoring applications, rely heavily on resource-constrained wireless communication technologies [1]. These networks are often made up of devices with limited memory, battery life, processing power, and communication capacity. These systems create serious cybersecurity risks even though they facilitate effective real-time connectivity [2]. With optimal resource management, the use of WSN for data communication can be improved, significantly satisfying data transfer requirements and conserving energy. Artificial Intelligence (AI) can improve the efficiency and reliability of energy systems through new data analysis and ongoing monitoring [3]. AI has become a revolutionary force in IoT network security due to its capacity for intelligent analysis, pattern recognition, and decision-making [4]. AI includes a wide range of methods that allow machines to behave intelligently, such as deep learning (DL), machine learning (ML), and natural language processing. Security solutions can transition from static rule-based systems to dynamic and adaptive entities that can learn from network data, spot anomalies, and proactively mitigate attacks by utilizing AI [5]. An essential step toward decentralized, autonomous, and resilient security systems is the incorporation of lightweight AI models into edge cybersecurity frameworks [6]. Ensuring the security and integrity of these dispersed settings using effective, AI-powered methods is crucial as edge computing becomes more commonplace [7].

AI and other cutting-edge enabling technologies also make data processing, analysis, and decision-making

automated and quicker. But in the face of massive data creation from IoT devices, maintaining authentication, security, and privacy is still essential. Strong security measures, such as anomaly detection systems (ADS), are necessary because of security vulnerabilities such Distributed Denial of Service (DDoS) assaults and eavesdropping anxieties in wireless IoT communications [8]. Even though DL for anomaly detection has advanced, many current methods are still inappropriate for low-power IoT devices because of their high latency, massive memory requirements, and reliance on cloud connectivity. These restrictions make it more difficult to operate in real time and raise communication overhead, which is crucial for applications that are safety or mission-oriented. Lightweight signal processing and ML methods that can function in the vicinity while retaining respectable detection accuracy and resilience are therefore desperately needed [9] [10].

Transformer-based learning models have recently shown impressive results when it comes to extracting global contextual information from sequential data. Comparably, compared to conventional recurrent architectures, Gated Recurrent Unit (GRU) models effectively capture temporal interactions while retaining a lower computational complexity.

This research suggests a lightweight Transformer-GRU hybrid anomaly detection framework combined with energy-efficient real-time threat mitigation and adaptive threshold optimization to overcome current constraints. While the GRU module effectively depicts sequential attack behavior, the Transformer module captures long-range traffic dependencies. The suggested framework preserves excellent detection accuracy while reducing computing overhead and improving energy economy.

The following are this work's principal contributions:

1. To create a lightweight framework for anomaly identification using Transformer-GRU.
2. To implement malicious node isolation via an adaptive anomaly threshold optimization.
3. To create a real-time threat mitigation strategy that uses less energy.

The remainder of the paper is structured as follows: an overview of some recent studies introduced for anomaly detection is presented in section 2. The system model presented in section 3 is accompanied by a solid theoretical basis. The algorithmic phases of the proposed work are explained in Section 4, and the findings and performance analysis are shown in Section 5. The suggested work is concluded in Section 6, emphasizing its importance.

2. LITERATURE SURVEY

The Preprocessed Isolation Forest technique for anomaly detection was introduced by Prarthi Jain et al. [11]. The iForest method served as the foundation for PiForest, which included a pre-processing step to handle streaming data efficiently. Principal Component Analysis (PCA) was initially used in the pre-processing phase to drastically diminish the size and dimension of the data. The data's flowing attribute was then managed by a sliding window technology that generates consecutive data chunks for methodical processing. Despite having significantly lower storage and prediction complexity, PiForest was able to detect anomalies just as successfully as iForest and supplementary cutting-edge anomaly detection methods.

A distributed anomaly detection architecture was proposed by Sutharshan Rajasegarar et al. [12]. It builds the data at each sensor node using several hyperellipsoidal clusters in order to detect both local and comprehensive anomalies in the network. To give each hyperellipsoidal model a score based on how far away the ellipsoid is from its neighbors, an anomaly scoring system was specifically put out.

The intricacy and concurrent performance of popular ML models and Autoencoders were assessed by Romarick Yatagha et al. [13]. Additionally, they offered a structured evaluation methodology and decision matrix to help choose effective anomaly detection models that are suited to particular operational limitations.

An AIDS created especially for IoMT networks' resource-constrained devices was proposed by Georgios Zachos et al. [14]. Rather of using traditional classification techniques, the suggested lightweight AIDS uses novelty discovery and outlier detection algorithms.

An ML detection method for classifying and identifying resource-constrained assaults in IoT devices was proposed by Zainab Alwaisi et al. [15]. They used EdgeML and CloudML for detection, viewing IoT devices as vital elements of the edge and cloud computing continuum. They performed a comparative study of ML models, concentrating on memory and energy usage in IoT applications.

An agent-enabled anomaly detection system was proposed by Usman, Muhammad [16], wherein mobile agents verify sensor nodes in situ to confirm the origin of anomalies. Furthermore, because transmission is hundreds of times more expensive than computation, mobile representatives cannot be independently transmitted through the network. Using the 2-sigma technique, we maximize agent transmission. Petri net theory was used to conduct the formal behavior analysis of the 2-sigma approach in order to assess its accuracy.

The particular issue of isolated anomaly identification based on signals that fit into the latter type across wireless channels with resource-embarrassed sensors was examined by Anders et al. [17]. We investigate how source coding affects the detection accuracy using an autoencoder-based anomaly detector and one based on Principal Component Analysis.

In resource-constrained WSNs, Zhiguo Ding et al. [18] presented a unique dispersed operational anomaly detection technique. First, a number of single anomaly detectors based on ensemble learning theory were constructed in each dispersed positioning sensor node by taking use of the spatiotemporal correlation found in the sensed data. Second, the initial ensemble detector was constructed by broadcasting these trained detectors to the cluster's member sensor nodes and mixing them with their own trained detectors. Thirdly, collaborative cropping based on biogeographical optimization was used in the cluster head node to get an optimum subset of collaborative members, taking into account WSNs with limited resources.

Quantized autoencoder (QAE) models were introduced by Sharmila and Rohini Nagapadma [19] to identify anomalies in intrusion detection systems. Pruning, clustering, and integer quantization techniques are all incorporated into QAE, an optimization model that is based on autoencoders. Two variations of QAE designed to implement computationally costly AI models into Edge devices are quantized autoencoder uint8 (QAE-u8) and quantized autoencoder float16 (QAE-f16). Initially, we created a Real-Time Internet of Things 2022 dataset for both typical and malicious traffic. Regular traffic is used by the autoencoder model during training. The same model is then used to reconstruct anomalous traffic, assuming that the anomaly's reconstruction will be high, in order to detect the assaults.

The Enhanced mobile Agent-enabled Anomaly Detection System (EAADS) is developed by Usman et al. [20] with the use of a holistic system approach and two new algorithms. A bottom-up synthesis of the numerous Petri net modules was carried out in order to produce a consistent model that has helped identify and eliminate discrepancies in the system design. This approach provides a formal description of the EAADS's general workflow and behavioral attributes. The typical unified Petri net model is then expanded into a corresponding high class Generalized Stochastic Petri Net model in order to codify and analyze the temporal behavior of the EAADS in a highly nondeterministic communication environment.

3. THEORETICAL BACKGROUND AND SYSTEM MODELLING

Wireless networks with limited resources display dynamic traffic patterns, erratic communication behavior, packet variations, and quickly changing attack characteristics. Such constantly shifting network environments are beyond the capabilities of traditional static intrusion detection systems. Thus, to improve detection robustness under changing traffic conditions, the suggested system uses adaptive learning and dynamic threshold tuning.

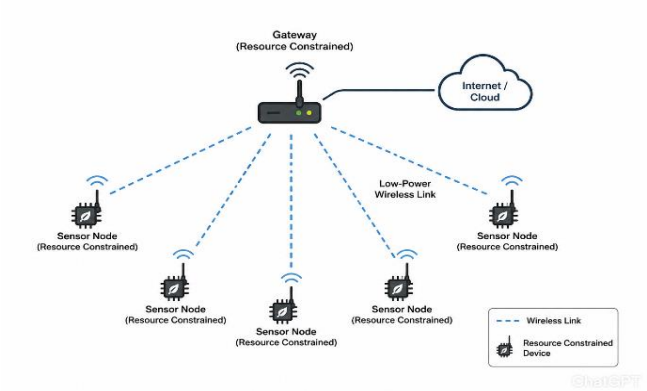

Figure 1. Resource constrained wireless network architecture

3.1. Network Model

The behavior of traffic in wireless networks can be described as a multidimensional stochastic process. Packet rate, delay, signal intensity, residual energy, and communication patterns are all included in each network traffic pattern. This can be stated numerically as:

$$NT_t = \{nt_{1,}nt_{2,}nt_3 \ldots., nt_n\} \quad (1)$$

Where NT_t is the network traffic at time t and $nt_{1,}nt_{2,}nt_3 \ldots., nt_n$ is the extracted attributes of the traffic network.

3.2. Energy Efficiency Model

Because sensor nodes in wireless IoT systems have limited battery resources, energy preservation is a crucial concern. The theoretical design of the suggested mitigation approach makes use of residual energy-aware communication concepts. The residual energy $E_R$of the node is calculated as:

$$E_R = E_0 - E_{consumed} \quad (2)$$

Where E_0 is the initial energy and $E_{consumed}$ is the consumed energy.

3.3. Objective function

The proposed framework's overarching optimization goal is to minimize computing complexity and energy usage while concurrently maximizing detection accuracy. The function for multi-objective optimization is described as:

$$f(x) = \max(Acc) + \min\left(w_1 E_{consumed} + w_2 C_{complex} + w_3 FPR\right) \quad (3)$$

Where w_1, w_2 and w_3 are the weighting factors, Acc is the accuracy, $C_{complex}$ is the computational complexity and FPR is the false positive rate.

4. LIGHTWEIGHT TRANSFORMER-GRU BASED ADAPTIVE ANOMALY DETECTION FRAMEWORK

The suggested lightweight anomaly detection approach effectively detects malicious activity in resource-constrained wireless contexts by combining GRU-based temporal sequence analysis with Transformer-based contextual learning. In order to detect anomalous activity in real time, the framework dynamically analyzes traffic changes and continually tracks wireless communication behavior. The suggested framework's processing stages are depicted in Figure 2.

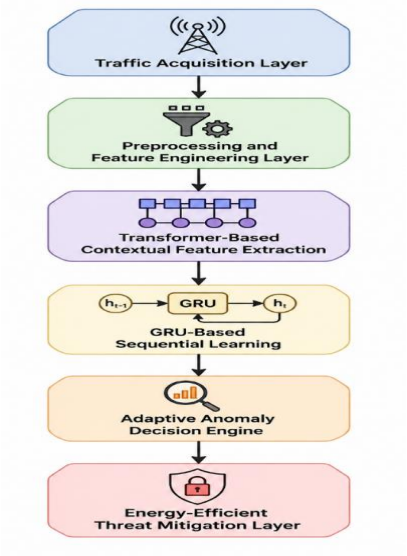

Figure 2. Proposed Lightweight Transformer-GRU Based Adaptive Anomaly Detection Framework

4.1. Traffic Data Acquisition

Real-time network traffic data is gathered by the traffic acquisition module from wireless nodes, edge devices, IoT sensors, and gateways. Equation (1) expresses the valid and harmful communication patterns seen in the recorded traffic data. To remove scale imbalance among traffic characteristics, these derived network traffic attributes NT_t are normalized. The procedure of normalization is carried out as:

$$NT_{norm} = \frac{NT_t - NT_{min}}{NT_{max} - NT_{min}} \quad (4)$$

WhereNT_{norm} is the normalized network traffic attributes, NT_{min} is the minimum attribute value and $NT_{max}$is the maximum attribute value.

4.2. Transformer-Based Attribute Extraction

Using self-attention processes, the Transformer module extracts global contextual correlations between network traffic aspects. Transformer models effectively assess long-range traffic dependencies in parallel, which lowers sequential processing overhead in contrast to traditional recurrent systems. The self-attention system determines the significance of attributes as:

$$Attention(Q, K, V) = Softmax\left(\frac{QK^T}{\sqrt{d_k}}\right)V \quad (5)$$

Where Q denotes query matrix, K represents key matrix, V indicates value matrix, and $d_k$is the scaling dimension. The contextual attribute embedding generated by the Transformer encoder is represented as:

$$CT_t = transformer(NT_{norm}) \quad (6)$$

Where CT_t is the contextual traffic representation.

4.3. GRU based sequential learning

Due to the dynamic evolution of attack behavior over time, wireless network anomalies show high temporal connections. In order to capture sequential traffic variations, the suggested system incorporates a GRU module.

The GRU's update gate $z_t$of is shown as:

$$z_t = \sigma(W_z x_t + U_z h_{t-1}) \quad (7)$$

The reset gate r_t is defined as:

$$r_t = \sigma(W_r x_t + U_r h_{t-1}) \quad (8)$$

The candidate hidden state h_t is computed as:

$$h'_t = tanh(W_h x_t + U_h(r_t \odot h_{t-1}) \quad (9)$$

The final hidden state update is expressed as:

$$h_t = (1 - z_t) \odot h_{t-1} + z_t \odot h'_{t-1} \quad (10)$$

4.4. Adaptive Anomaly Detection Mechanism

An adaptive anomaly determination engine is introduced by the suggested architecture, which dynamically modifies detection sensitivity in response to changes in traffic in real time. The computation of the anomaly score A_{score} is:

$$A_{score} = |P_{observed} - P_{expected}| \quad (11)$$

Where $P_{observed}$ is the observed traffic pattern and $P_{expected}$ is the expected traffic pattern. The adaptive threshold $T_{adaptive}$ is defined as:

$$T_{adaptive} = \mu + \alpha\sigma \quad (12)$$

Where α indicates threshold adjustment coefficient, μ is the mean traffic behaviour and σ is the standard deviation of the traffic behaviour. The network anomaly is detected using the following rule:

$$Network_{decision} = \begin{cases} malicious, if\ A_{score} > T_{adaptive} \\ normal,\ otherwise \end{cases} \quad (13)$$

Under varying wireless traffic conditions, the adaptive technique enhances detection robustness.

4.5. Lightweight Resource optimization

The suggested framework reduces resource consumption in limited wireless devices by utilizing lightweight optimization techniques. The optimal computational complexity CC_{opt} is estimated as:

$$CC_{opt} = \frac{E_{reduced}}{T_{reduced}} \quad (14)$$

Where $T_{reduced}$ is the reduced time and $E_{reduced}$ is the reduced execution. The routing optimization cost R_{cost} is expressed as:

$$R_{cost} = \frac{D_{transmission}}{E_R} \quad (15)$$

Where E_R is the residual energy and $D_{transmission}$ is the transmission delay.

5. RESULTS AND ANALYSIS

The benchmark intrusion detection datasets CICIDS2017 Dataset and NSL-KDD Dataset were used to assess the suggested lightweight Transformer-GRU anomaly detection architecture.

5.1. Dataset description

The CICIDS2017 dataset includes traffic created under realistic network settings, both benign and malicious. DDoS, Brute Force Attacks, Botnet Attacks, Port Scanning, Web Attacks, and Infiltration Attacks are only a few of the attack types covered by the dataset. In a similar vein, the NSL-KDD dataset was created to increase the accuracy of intrusion detection evaluations and remove redundant records. The types of attacks are User-to-Root (U2R), Remote-to-Local (R2L), Probe Attacks, and DoS.

5.2. Simulation setup

TensorFlow and Python environments were used to implement the suggested framework. The NS-3 wireless network simulator was used to model network communication behavior. The other simulation settings are displayed in Table 1.

Table 1. Simulation Parameters

Parameter	Value
Number of Sensor Nodes	25,50, 100,200,250, 500,750 ,1000
Simulation Area	1000 m × 1000 m
Transmission Range	50 m
Training Ratio	80%
Testing Ratio	20%
Batch Size	64
Learning Rate	0.001
Optimizer	Adam
Epochs	100
Processor	Intel Core i7
RAM	16 GB

5.3. Performance evaluation

Fig. 2 shows the performance of the transformer based GRU framework.

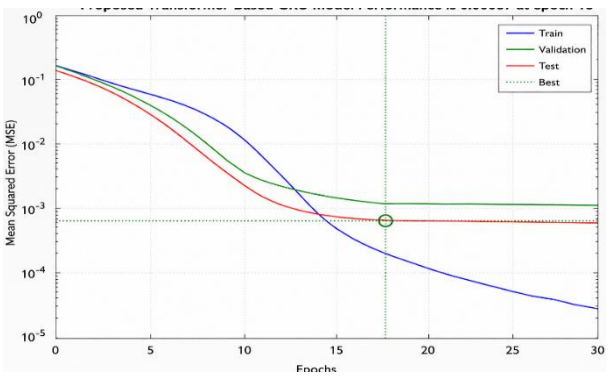

Figure 3. Performance of transformer based GRU

Due to insufficient attribute adaptation and random parameter initialization, both the training and validation transition losses initially show comparatively greater values in Figure 3. The GRU module gradually learns temporal attack behavior from sequential wireless network traffic, while the Transformer-based contextual learning mechanism effectively captures global traffic dependencies as the number of epochs increases. As a result, the transition state error gradually declines, indicating steady optimization and enhanced attribute representation capacity. The training and validation transition curves closely overlap, indicating good generalization performance with little overfitting.

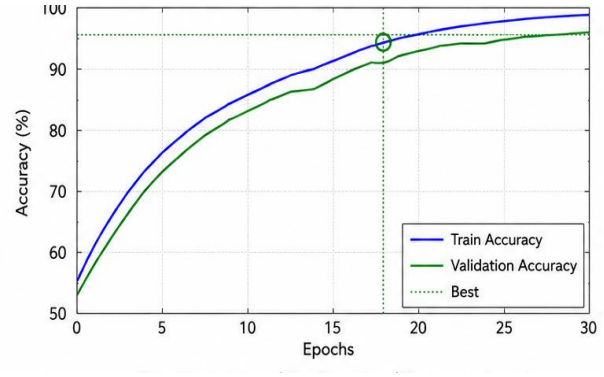

Figure 4. Training Vs validation accuracy

The accuracy curves in Figure 4 progressively stabilize and converge close to the ideal zone around epoch 18, when the model reaches its highest validation accuracy. Additionally, the smooth convergence behavior validates the stability and learning effectiveness of the suggested lightweight Transformer-GRU framework for anomaly detection in real time.

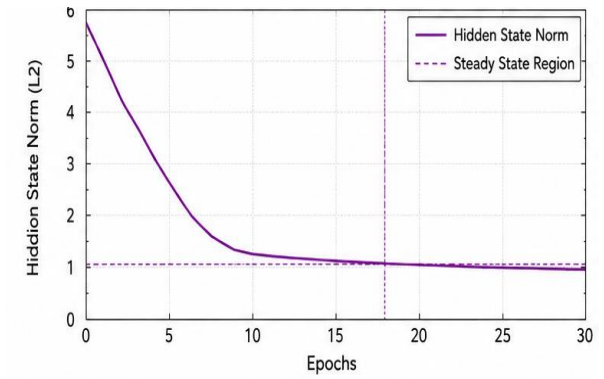

Figure 5. Transition state behavior of the hidden state in the proposed Transformer-based GRU model

The GRU model effectively learns stable temporal traffic patterns and eventually lowers internal state fluctuations, as evidenced by the steady drop in the hidden state norm as training goes on. The curve shows successful convergence and stable sequential learning at epoch 18, when it approaches the steady-state region where the hidden state values stabilize with little variation.

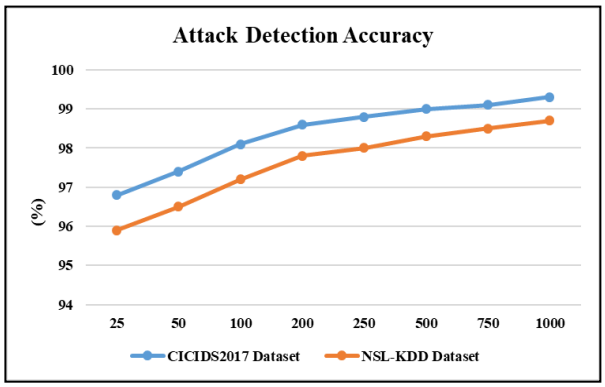

Figure 6. Detection Accuracy of the proposed transformer based GRU model

Figure 6 illustrates the scalability and resilience of the suggested anomaly detection methodology by showing how the detection accuracy progressively improves for both datasets as the number of sensor nodes rises from 25 to 1000. The CICIDS2017 dataset outperforms the NSL-KDD dataset in terms of accuracy because of its more realistic and varied traffic characteristics, which improve contextual learning capacity. While the GRU module successfully learns temporal attack behavior, the Transformer module effectively captures global traffic dependencies, as evidenced by the steady improvement in accuracy.

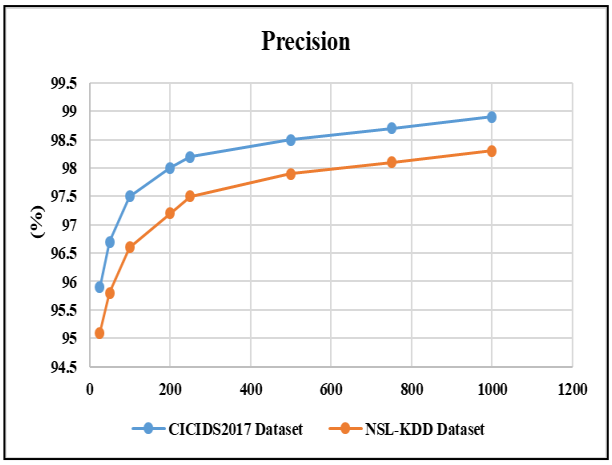

Figure 7. Precision of the proposed transformer based GRU model

Figure 7 shows enhanced hostile traffic categorization with fewer false positives as the precision progressively rises with the number of sensor nodes. Because of its varied and realistic traffic patterns, the CICIDS2017 dataset delivers a little greater precision.

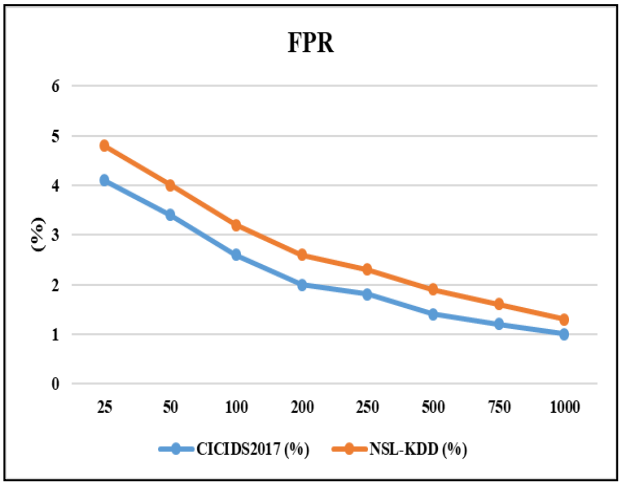

Figure 8. FPR of the proposed transformer based GRU model

Figure 8 shows that as the number of sensor nodes rises, the FPR continuously declines, indicating better anomaly detection accuracy with fewer false alarms. When compared to NSL-KDD, the CICIDS2017 dataset achieves a reduced FPR, indicating improved detection reliability and adaptive learning capabilities of the suggested model in large-scale wireless network situations.

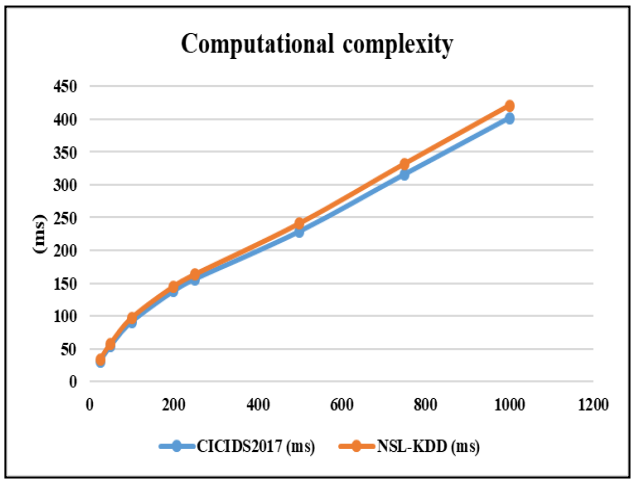

Figure 9. Computational complexity of the proposed transformer based GRU model

Figure 9 shows that both datasets have good scalability, with processing time increasing almost linearly with the number of records. At 1000 records, the NSL-KDD dataset consistently takes a little longer to process than CICIDS2017 roughly 420 ms as opposed to 400 ms for CICIDS2017. This minor variation implies that the suggested approach exhibits steady and predictable computing increase while maintaining effective performance across various datasets.

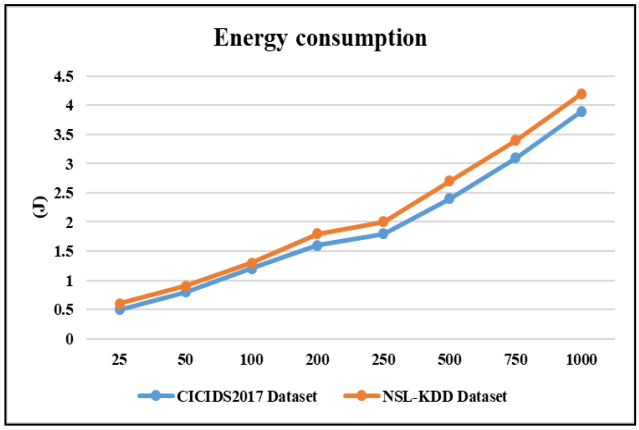

Figure 10. Energy Consumption of the proposed transformer based GRU model

Figure 10 shows that the NSL-KDD dataset continuously uses a little bit more energy than CICIDS2017, reaching roughly 4.2 J at 1000 records as opposed to 4.0 J for CICIDS2017. The suggested model is scalable and energy-efficient, maintaining low energy overhead even when processing bigger datasets, as evidenced by the slow and nearly linear growth.

6. CONCLUSION

In this paper, an energy-efficient real-time threat mitigation mechanism for resource-constrained wireless networks was combined with a lightweight AI-assisted adaptive anomaly detection system. Transformer-based contextual attribute extraction and GRU-based temporal learning are successfully combined in the suggested Transformer-GRU hybrid architecture to reliably detect fraudulent activity with minimal computing overhead. Additionally, as network conditions change, the adaptive threshold optimization technique dynamically modifies detection sensitivity, which lowers false alarms and increases detection reliability. Through effective malicious node isolation and residual energy-based communication route optimization, the energy-aware mitigation technique improves network sustainability. High detection accuracy, enhanced precision, decreased false positive rate, low computing complexity, and low energy consumption were shown by experimental assessment utilizing the CICIDS2017 and NSL-KDD datasets. The outcomes verify that the suggested architecture offers a scalable, reliable, and energy-efficient security solution appropriate for real-time deployment in wireless and Internet of Things contexts with limited resources.

REFERENCES

[1] Gudala, Leeladhar, Mahammad Shaik, Srinivasan Venkataramanan, and Ashok Kumar Reddy Sadhu.

"Leveraging artificial intelligence for enhanced threat detection, response, and anomaly identification in resource-constrained iot networks." *Distributed Learning and Broad Applications in Scientific Research* 5 (2019): 23-54.

[2] Parameswari, M., Nancy P, and R. Jeya Malar. "Next generation AI powered framework for autonomous energy optimization and real time anomaly detection in IoT driven wireless sensor networks." *Scientific Reports* 15, no. 1 (2025): 41104.

[3] S. Sowmiya, B. Muthu Archana, and Dr. C. Mythili, "WILDLIFE SAFETY AND HUNTER MONITORING SYSTEM USING AI CAMERAS AND GEOFENCING FOR REAL-TIME ALERTS," Int. J. Adv. Eng. Manag. Syst., vol. 1, no. 2, pp. 150-169, 2025. doi: 10.65379/tpsn2013/ijaemsv01i02p1.

[4] Babalola, Olufunbi, Olaitan Miriam Olufisayo Raji, Jamiu Olamilekan Akande, Abdullahi Olalekan Abdulkareem, Vincent Anyah, Adeladan Samson, and Steve Folorunso. "AI-powered cybersecurity in edge computing: Lightweight neural models for anomaly detection." *International Journal of Multidisciplinary Research and Growth Evaluation* 5, no. 2 (2024): 1130-1138.

[5] Reis, Manuel JCS. "Lightweight Signal Processing and Edge AI for Real-Time Anomaly Detection in IoT Sensor Networks." *Sensors* 25, no. 21 (2025): 6629.

[6] Nti, Isaac Kofi, Miriyala Sai Manikanta, Clark Alex, and Lee Jo Ning. "Lightweight Neural Anomaly Detection for Resource-Constrained Edge-ICN Environments: A Systematic Literature Review." (2025).

[7] Pelc, Mariusz, Dawid Galus, Magda Zolubak, Stepan Ozana, Wojciech Chlewicki, Katarzyna Cichon, Michal Podpora, and Aleksandra Kawala-Sterniuk. "Behavioural approach to network anomaly detection for resource-constrained system–presentation of the novel solution–preliminary study." *IFAC-PapersOnLine* 52, no. 27 (2019): 121-126.

[8] Ge, Di, Zheng Dong, Yuhang Cheng, and Yanwen Wu. "An enhanced spatio-temporal constraints network for anomaly detection in multivariate time series." *Knowledge-Based Systems* 283 (2024): 111169.

[9] Lauf, Adrian P., Richard A. Peters, and William H. Robinson. "A distributed intrusion detection system for resource-constrained devices in ad-hoc networks." *Ad Hoc Networks* 8, no. 3 (2010): 253-266.

[10] Serban, Codruta Maria, Madalin Neagu, Anca Hangan, and Gheorghe Sebestyen. "Towards Trustworthy IoT Ecosystems: Efficient Encryption and Anomaly Detection for Resource-Constrained Devices." In *2025 25th International Conference on Control Systems and Computer Science (CSCS)*, pp. 404-411. IEEE, 2025.

[11] Gan, Wei, Lei Lei, Jun Su, Luocheng Shen, Yuhao Xiao, Conghong Liu, and Yaoran Huo. "A Lightweight Deep Learning Model for Efficient Traffic Anomaly Detection in Resource-Constrained Power System Networks." In *2024 4th International Conference on Smart Grid and Energy Internet (SGEI)*, pp. 280-284. IEEE, 2024.

[12] Jain, Prarthi, Seemandhar Jain, Osmar R. Zaïane, and Abhishek Srivastava. "Anomaly detection in resource constrained environments with streaming data." *IEEE Transactions on Emerging Topics in Computational Intelligence* 6, no. 3 (2021): 649-659.

[13] Rajasegarar, Sutharshan, Alexander Gluhak, Muhammad Ali Imran, Michele Nati, Masud Moshtaghi, Christopher Leckie, and Marimuthu Palaniswami. "Ellipsoidal neighbourhood outlier factor for distributed anomaly detection in resource constrained networks." *Pattern recognition* 47, no. 9 (2014): 2867-2879.

[14] Yatagha, Romarick, Oumayma Mejri, Karl Waedt, and Christoph Ruland. "Assessing the complexity and real-time performance of anomaly detection algorithms in resource-constrained environments." In *2024 IEEE 20th International Conference on Intelligent Computer Communication and Processing (ICCP)*, pp. 1-8. IEEE, 2024.

[15] Maria Priska A, Dr.K.Madhan Kumar, Mrs.X.M.Binisha, & Ms.K.Sneha. (2025). Novel And Hybrid Frameworks for Attack Detection And Secure Transmission in Manet. International Journal of Advanced Engineering and Management System, 1(3), 204-213. https://doi.org/10.65379/tpsn2013/ijaemsv01i03p3

[16] Alwaisi, Zainab, Tanesh Kumar, Erkki Harjula, and Simone Soderi. "Securing constrained IoT systems: A lightweight machine learning approach for anomaly detection and prevention." *Internet of Things* 28 (2024): 101398.

[17] Usman, Muhammad. "Agent-enabled anomaly detection in resource constrained wireless sensor networks." In *Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014*, pp. 1-2. IEEE, 2014.

[18] Kalør, Anders E., Daniel Michelsanti, Federico Chiariotti, Zheng-Hua Tan, and Petar Popovski. "Remote anomaly detection in industry 4.0 using resource-constrained devices." *arXiv preprint arXiv:2110.05757* (2021).

[19] Ding, Zhiguo, Haikuan Wang, Minrui Fei, and Dajun Du. "A novel distributed online anomaly detection method in resource-constrained wireless sensor networks." *International Journal of Distributed Sensor Networks* 11, no. 10 (2015): 146189.

[20] S.Chermakabi, Dr.R.S.Ganesh, K.Rahmath Nisha, B. Rejila, 5G-NR Based Physical Layer Techniques for High-Speed 6G NTN Connectivity (2025), International Journal of Advanced Engineering and Management System, https://doi.org/10.65379/tpsn2013/ijaemsv01i03p4