BiLSTM-Attention Seeking Intrusion Detection System for SWIPT-Enabled IoT Systems

Vishalya Sooriarachchi
UNINOVA-CTS
Lusofona University
Lisbon, Portugal
a22211643@alunos.ulht.pt

Dushantha Jayakody
UNINOVA-CTS
Lusofona University
Lisbon, Portugal
dushantha.jayakody@ulusofona.pt

Stefan Panic
Department of Informatics
University of Pristina in Kosovska Mitrovica
Kosovska Mitrovica, Kosovo
stefan.panic@pr.ac.rs

Abstract

Integration of simultaneous wireless information and power transfer (SWIPT) into Internet of Things (IoT) network require unique security requirements. These systems operate in energy-constrained environments, where traditional intrusion detection systems (IDS) are mostly unable to perform as expected. In SWIPT-systems, information transmission as well as energy harvesting and allocation systems are vulnerable to attacks, thereby requiring more sophisticated security systems to support continued operation. The study proposes an unsupervised BiLSTM attention autoencoder-based IDS model designed specifically for SWIPT-enabled IoT systems operating with a sequence-to-sequence framework.

CCS Concepts

• **Security and privacy → Intrusion detection systems**.

Keywords

SWIPT, IoT, unsupervised learning, BiLSTM, Intrusion detection systems

ACM Reference Format:
Vishalya Sooriarachchi, Dushantha Jayakody, and Stefan Panic. 2025. BiLSTM-Attention Seeking Intrusion Detection System for SWIPT-Enabled IoT Systems. In *International Conference on Future Networks and Distributed Systems (ICFNDS '25), December 08–09, 2025, Dubai, United Arab Emirates.* ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3789692.3789844

1 Introduction

The increased advancements in Internet of Things (IoT) and its associated technologies, a higher level of importance is placed on the maintenance of data security. The increasing number of applications such as smart cities, healthcare, industrial automation, and smart agriculture rely on interconnected IoT networks that are reliant on real-time data exchange and system security [1]. Yet, the increased adoption of IoT networks towards highly sensitive use-cases expands the threat surface of the networks, thereby exposing the systems towards diverse security threats such as data breaches, unauthorized access, and distributed denial-of-service (DDoS) attacks. The high-value and sensitive nature of data managed by these systems amplifies the potential impact of possible security violations, thereby creating a significant need to implement robust and adaptive security mechanisms [4].

On the other hand, the integration of simultaneous wireless information and power transfer (SWIPT) into IoT systems have been widely studied - which is an aspect that introduces additional complexity to the security and operational requirements [8]. SWIPT has been introduced to allow IoT devices to harvest energy from radio frequency (RF) signals, simultaneously conducting information decoding (ID) and energy harvesting (EH) - thereby extending device longevity and reducing the dependence on power sources [7]. However, SWIPT-enabled IoT systems face unique vulnerabilities related to energy-based attacks which can disrupt operations, manipulate power transfer to devices, and/or eavesdropping attacks exploiting the dual-purpose RF signals. Since these systems are implemented in a decentralized manner within energy-constrained environments, the risks associated to maintaining system security are further increased [6, 10].

Traditional intrusion detection systems (IDS) which rely on static rule-based or signature-based approaches are unable to address the dynamic and heterogeneous nature of SWIPT-based IoT networks. These approaches depend on predefined patterns and learnt threat-types, hence are unable to detect novel or zero-day attacks. The computational overhead of traditional IDS methods often exceed the capabilities of SWIPT-based IoT systems, which already operates under maximum energy management [2, 3, 9].

Figure 1 showcase the effect of some of the most common anomaly types - spike, drift, and dropout - within time-series data from IoT devices. Thus, recent studies have highlighted the requirement of intelligent, lightweight, and adaptive IDS, capable of real-time anomaly detection without extensive prior knowledge.

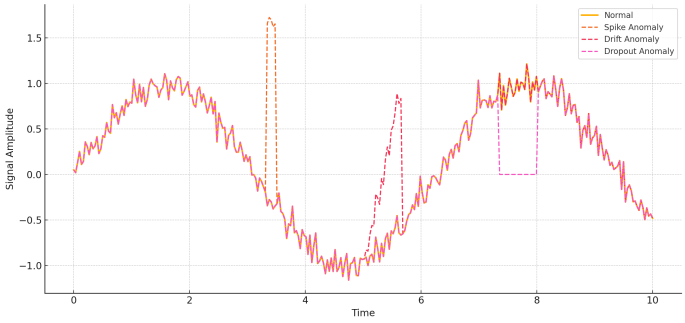

Figure 1: Effect of anomalies on normal IoT signal data. Spike, drift, and dropout patterns are shown.

ICFNDS '25, Dubai, United Arab Emirates

ACM ISBN 979-8-4007-2091-8/25/12
https://doi.org/10.1145/3789692.3789844

Machine learning (ML) and deep learning (DL) techniques have emerged as promising solutions to address the security requirements of rural IoT systems. Unsupervised learning approaches are considered well-suited for IoT environments with the high amount of raw data generated from the sensors which are both dynamic and subjected to changes with the operational environment. Among the DL methods, bidirectional long short-term memory (BiLSTM) networks have shown promising efficiency in processing sequential data, making them ideal to analyze time-series network traffic in IoT devices. The unique ability of BiLSTM models to capture temporal variations in both forward and backward directions make the model capable of handling complex patterns and detecting subtle anomalies [5, 11].

This paper proposes a BiLSTM-attention autoencoder based IDS designed for SWIPT-enabled IoT networks. The system uses unsupervised learning to detect anomalies in network traffic, considering the unique data types related to SWIPT-enabled IoT systems. The remainder of the paper is organized as follows: Section 2 introduces the system model and problem formulation, and presents the proposed BiLSTM- attention autoencoder based IDS architecture. The training results of the model and performance evaluation is provided in Section 3 and discussion of the results are presented in Section 4. Finally, Section 5 concludes the paper with future research directions.

2 Model Training Approach

An unsupervised BiLSTM-attention autoencoder model is implemented to develop a lightweight and effective anomaly detection system for SWIPT-enabled edge IoT devices. This model uses sequential reconstruction capability through a learned attention mechanism implemented for interpretability and increased anomaly sensitivity.

2.1 Input Data and Pre-processing

The input data consists of time-series network traffic or sensor observations with n_{features} number of features spread across n_{samples} number of time steps, which is represented as, $\mathbb{X} \in \mathbb{R}^{n_{\text{samples}} \times n_{\text{features}}}$ standardized as:

$$X_{\text{scaled}} = \frac{X - \mu}{\sigma}. \tag{1}$$

A single sequence starting at time step is defined as $\mathbb{X}_{\text{seq}}^{(t)} = [x_{\text{scaled}}(t), \ldots, x_{\text{scaled}}(t+T-1)] \in \mathbb{R}^{T \times n_{\text{features}}}$, which gives, $\mathbb{X}_{\text{seq}} \in \mathbb{R}^{N \times T \times n_{\text{features}}}$, where $N = n_{\text{samples}} - T + 1$.

Sequence labels are given as,

$$y_{\text{seq}}^{(t)} = \begin{cases} 1 & \text{if } \frac{1}{T} \sum_{i=t}^{t+T-1} y(i) > y_{th} \\ 0 & \text{otherwise} \end{cases} \tag{2}$$

2.2 BiLSTM Encoder Model

For an input $x_t \in \mathbb{R}^{n_{\text{features}}}$ at time t, where the previous hidden state is $h_{t-1} \in \mathbb{R}^h$, and cell state is $c_{t-1} \in \mathbb{R}^h$, the LSTM computes the LSTM computes the following gates,

$$\text{(Forget gate)} f_t = \sigma(W_f x_t + U_f h_{t-1} + b_f) \tag{3}$$

$$\text{(Input gate)} i_t = \sigma(W_i x_t + U_i h_{t-1} + b_i) \tag{4}$$

$$\text{(Candidate cell state)} \tilde{c}_t = \tanh(W_c x_t + U_c h_{t-1} + b_c) \tag{5}$$

$$\text{(Updated cell state)} c_t = f_t \odot c_{t-1} + i_t \odot \tilde{c}_t \tag{6}$$

$$\text{(Output gate)} o_t = \sigma(W_o x_t + U_o h_{t-1} + b_o) \tag{7}$$

$$\text{(Hidden state)} h_t = o_t \odot \tanh(c_t) \tag{8}$$

Here, $W_f, W_i, W_c, W_o \in \mathbb{R}^{h \times (n_{\text{features}}+h)}$ are the weight metrices, $b_f, b_i, b_c, b_o \in \mathbb{R}^h$ represent the bias vectors, $\sigma(\cdot)$ denotes the sigmoid activation function, and $\odot$ is element-wise multiplication.

In the LSTM model, the forward setup produces $\vec{h} \in \mathbb{R}^h$ with parameters $[W_f^{\vec{f}}, W_i^{\vec{f}}, W_c^{\vec{f}}, W_o^{\vec{f}}, b_f^{\vec{f}}, b_i^{\vec{f}}, b_c^{\vec{f}}, b_o^{\vec{f}}]$, while the backward model produces $h_t \in \mathbb{R}^h$ with parameters $[W_f^f, W_i^f, W_c^f, W_o^f, b_f^f, b_i^f, b_c^f, b_o^f]$. With these inputs, the BiLSTM output is $h_t = [\vec{h}_t; h_t] \in \mathbb{R}^{2h}$, and the sequence output can be given as $H = [h_1, h_2, ..., h_T] \in \mathbb{R}^{T \times 2h}$.

An attention mechanism is used in the system to compute a context vector where the score for time step t is,

$$e_t = \tanh(W_a h_t + b_a). \tag{9}$$

The attention weights of the mechanism are,

$$a_t = \frac{\exp(e_t)}{\sum_{j=1}^{T} \exp(e_j)}, \tag{10}$$

and the context vector c is given as,

$$c = \sum_{t=1}^{T} \alpha_t h_t \in \mathbb{R}^{2h}. \tag{11}$$

2.3 Attention Mechanism

To capture the varying importance of time steps, we introduce an attention mechanism. For the BiLSTM output sequence $\mathbb{Z} \in \mathbb{R}^{T \times h}$, the attention score for each time step t is computed as,

$$e_t = \tanh(W_{\text{att}} z_t + b_{\text{att}}) \tag{12}$$

$$\alpha_t = \frac{\exp(e_t)}{\sum_{j=1}^{T} \exp(e_j)} \tag{13}$$

$$c = \sum_{t=1}^{T} \alpha_t z_t \tag{14}$$

Here, α_t represents the normalized importance of each time step, and $\mathbf{c} \in \mathbb{R}^h$ is the context vector fed to the decoder.

2.4 Decoding and Anomaly Scoring

The LSTM decoder with a rectified linear unit (ReLU), is used, and the decoder activation produces,

$$h_t^{\text{dec}} = \text{LSTM}_{\text{decoder}}(C_t, h_{t-1}^{dec}; W_d, b_d). \tag{15}$$

Instead of a sequence-to-sequence decoder, the context vector $\mathbf{c}$ is passed through fully connected layers:

$$h_{\text{dense}} = \text{ReLU}(W_1 c + \mathbf{b}_1) \quad (16)$$
$$\hat{x} = W_2 h_{\text{dense}} + b_2 \quad (17)$$
$$\hat{X} = \text{Reshape}(\hat{x}) \in \mathbb{R}^{T \times d} \quad (18)$$

The reshape operation maps the flat output vector back to a time-feature format.

The reconstruction error is defined as,

$$e^{(t)} = \frac{1}{T \cdot n_{\text{features}}} \sum_{t=1}^{T} \sum_{f=1}^{n_{\text{features}}} \left(X_{\text{seq},t,f} - \hat{X}_{\text{seq},t,f} \right)^2. \quad (19)$$

Through the reconstruction error in Eq. (19), and the log-transformed error defined as $e^{(t)}_{\log} = \log(e^{(t)} + \epsilon)$ and the smooth error of the system $e^{(t)}_{\text{smooth}} = \frac{1}{w} \sum_{j=-w/2}^{w/2} e^{(t+j)}_{\log}$, the anomaly score is derived as,

$$s^{(t)} = \alpha . e^{(t)}_{\log} + (1 - \alpha) e^{(t)}_{\text{smooth}}. \quad (20)$$

To reduce sensitivity to noise and stabilize anomaly detection, we compute a smoothed anomaly score using log-reconstruction error:

$$e^{(i)} = \log(\mathcal{L}^{(i)}_{\text{rec}} + \epsilon) \quad (21)$$
$$s^{(i)} = \alpha e^{(i)} + (1 - \alpha) s^{(i-1)} \quad (22)$$

Here, $\alpha \in [0, 1]$ is a smoothing factor, and $s^{(i)}$ represents the final anomaly score at sequence i. Threshold τ is then determined using F1-score maximization or Youden's J-statistic.

3 Training Results

The BiLSTM-Attention Autoencoder model was trained for 40 epochs on normal sequences for a batch size of 32, anomalies were synthetically injected into the test set at a rate of approximately 15%. Anomaly scores were derived using reconstruction error combined with smoothed log-error dynamics, and optimal detection thresholds were determined via F1-score optimization. Performance was evaluated using precision, recall, F1-score, ROC-AUC, and confusion matrix.

The training and validation loss curves for the BiLSTM-attention autoencoder is shown in Fig. 2. As can be seen BiLSTM achieves convergence in under five epochs and both loss curves flatten below 0.02. This shows that the system has better reconstruction capability without overfitting and proves that the model performs well under unsupervised settings.

Figure 3 illustrates the anomaly detection output of the proposed BiLSTM-Attention Autoencoder. As can be seen, the reconstruction error closely follows the dynamics of the underlying signal which corresponds to the actual data, while it peaks during anomalous behavior. The learned threshold separates true anomalies with high accuracy. Also, the model captures subtle shifts in signal behavior and maintains consistency in detection due to the attention-weighted latent summarization.

To compare the performance of the BiLSTM-attention autoencoder model when implemented under SWIPT systems, the same

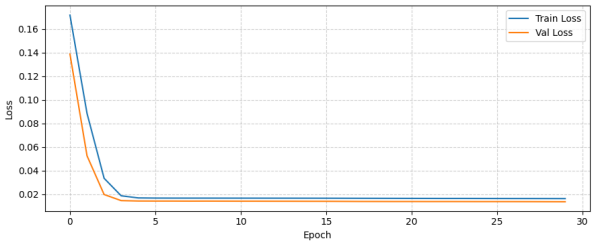

Figure 2: Training and validation losses of the proposed model.

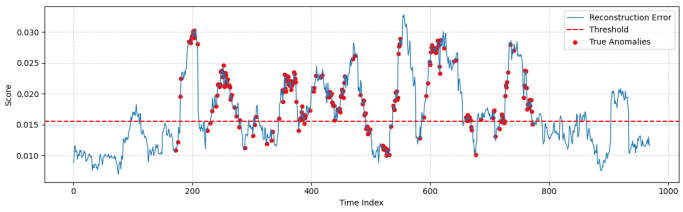

Figure 3: Anomaly detection output of the proposed model.

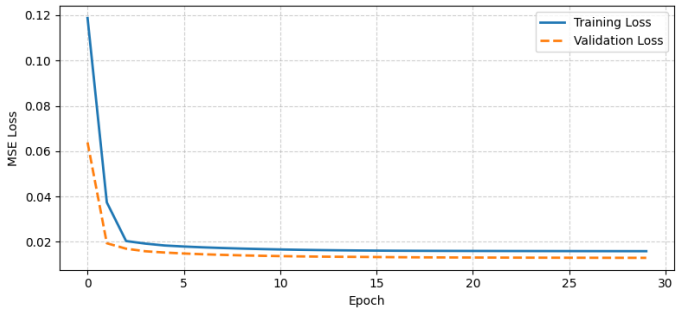

Figure 4: Training and validation losses of the GRU-based model.

data was considered with a gated recurrent unit (GRU) model, and a supervised learning model.

The loss curves for the GRU Autoencoder is shown in Fig. 4. This model too achieves faster convergence which is comparable with the BiLSTM model, yet the final validation loss is marginally higher. Also there is an early difference between training and validation curves, which suggests a weaker generalization ability. This limitation maybe arising due to GRU's limited expressiveness compared to BiLSTM.

Anomaly detection of the GRU model under identical data and training settings, is given in Fig. 5. The model shows capability of capturing most of the high-amplitude anomalies, yet there are more false positives in the lower-magnitude segments. The GRU model does not have a bidirectional mechanism, and the attention layer in the model limits its ability to prioritize significant temporal features. Therefore the reconstruction error profile of the model is less discriminative, compared with the BiLSTM-attention autoencoder.

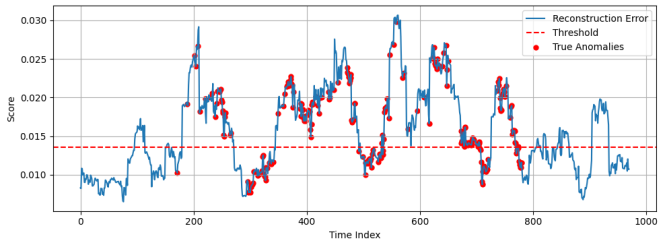

Figure 5: Anomaly detection output of the GRU-based model.

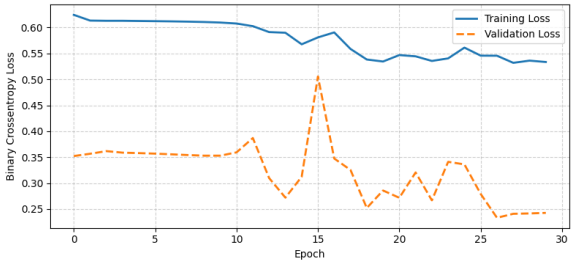

Figure 6: Training and validation losses of the supervised BiLSTM model.

The supervised learning model is also used to compare with the BiLSTM model in order to determine the performance of supervised vs unsupervised models under edge-IoT components. As can be seen from the training and validation loses in Fig. 7, though the training loss decreases, the validation loss exhibits noticeable fluctuations. This instability showcase a label imbalance with the newer data being added to the IoT system, showing that there are overfitting risks within the model. Due to these concerns, the use of supervised models for real-time edge deployments deem less suitable, and comparatively, the unsupervised BiLSTM model shows better performance.

Figure 7 demonstrates the anomaly scoring output of the supervised BiLSTM classifier. The output is defined through the binary supervision of the model and therefore a step-like anomaly detection is seen. Also, the sensitivity of the system is higher for stronger anomalies, however for low-intensity anomalies the frequency of misclassification is high. The model maintains a rigid threshold, which can be often viewed as a limitation of overall supervised models when generalizing performance towards unseen or unknown anomalies.

4 Discussion

The model training and the evaluation metrics included utilized to evaluate the model were selected in a manner which would provide a comprehensive understanding of the trade-offs when deploying each of the architectures in a SWIPT-enabled IoT system. More focus was laid on the edge-based SWIPT systems since these devices are the highest vulnerable to possible cyber attacks.

As was seen through the simulation results, the proposed model demonstrates a strong balance between detection accuracy and performance along with the lightweight design. The model achieves

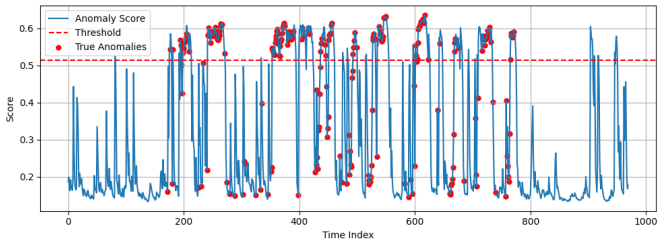

Figure 7: Anomaly detection output of the supervised BiLSTM model.

the highest F1-score (0.522), while significantly outperforming the other two models and provides that the attention mechanism provides opportunity to enhance the capability of the model to focus on temporally salient features.

Moreover, the proposed model achieved a recall of 0.814, the highest among the tested models, indicating its robustness in capturing a broad spectrum of anomalous patterns. Though the precision of the model - 0.384 is slightly lower than that of the supervised BiLSTM (0.448), this is an expected decrement since there is a trade-off between supervised and unsupervised learning models based on the anomaly labels are not present in the latter during training.

The operational time of the proposed model can be considered efficient compared with the other models. Mainly, the supervised learning model had a higher inference time compared with the proposed model - making the proposed system ideal for deployment in constrained environments. However, the GRU model had a marginally faster inference, yet this came with a compromise of accuracy.

The ROC-AUC score, which is a threshold-independent value which evaluates the model's ability to distinguish between normal and anomalous samples across all possible decision thresholds shows that the proposed model has better capability to distinguish between normal and anomalous patterns when compared with the other models.

The summary of the performance metrics of the proposed model in comparison with the GRU and BiLSTM-supervised model are presented in Table 1.

Table 1: Performance Comparison of Anomaly Detection Models

Model	Prec.	Rec.	F1	AUC	Time (ms)	Size (KB)
BiLSTM-Attn	0.384	**0.814**	**0.522**	**0.720**	80.10	102.70
GRU	0.359	0.782	0.489	0.694	72.55	89.50
Supervised	**0.448**	0.673	0.452	0.648	95.20	108.00

5 Conclusion

This paper presented an unsupervised BiLSTM-based IDS for SWIPT-enabled IoT networks. The proposed model was designed as an

autoencoder to reconstruct temporal input sequences and identify anomalies using reconstruction error metrics. The attention-augmented BiLSTM encoder was shown to effectively capture forward and backward dependencies in IoT signal sequences. The model achieved competitive performance without requiring labeled data, making it suitable for deployment in decentralized, resource-constrained SWIPT systems implemented in energy-depleted and rural environments. F1-score and ROC-AUC were used as evaluation metrics, and the results show that the model is capable of reliably flagging anomalous behaviors, including spikes, drifts, and dropouts in the network data.

Future research directions include incorporating federated learning, adaptive threshold tuning, and deploying the system on embedded devices for real-time energy-efficient detection.

Acknowledgments

This work was supported, in part, by the European Commission via Marie Skłodowska-Curie Actions (MSCA) as part of the project REMARKABLE (No. 101086387), by the Scheme for Promotion of Academic & Research Collaboration (SPARC), Government of India, via grant no. SPARC/2024-2025/NXTG/P3524, by the Sri Lanka Institute of Information Technology through the grant PVC(R&I)/RG/2024/12, by the COFAC - Cooperativa de Formação e Animação Cultural, C.R.L. (University of Lusófona University), via the project PortuLight (COFAC/ILIND/COPELABS/2/2023), by the national funds through FCT - Fundação para a Ciência e a Tecnologia - as part of the projects URLLC-UAV (2023.08191.CEECIND), UNINOVA-CTS (UIDB/00066/2020) and COPELABS (no. UIDB/04111/2020).

References

[1] Mumin Adam, Mohammad Hammoudeh, Rana Alrawashdeh, and Basil Alsulaimy. 2024. A Survey on Security, Privacy, Trust, and Architectural Challenges in IoT Systems. *IEEE Access* 12 (2024), 57128–57149. doi:10.1109/ACCESS.2024.3382709

[2] Mansi H. Bhavsar, Yohannes B. Bekele, Kaushik Roy, John C. Kelly, and Daniel Limbrick. 2024. FL-IDS: Federated Learning-Based Intrusion Detection System Using Edge Devices for Transportation IoT. *IEEE Access* 12 (2024), 52215–52226. doi:10.1109/ACCESS.2024.3386631

[3] Weibin Jiang, Jun Wang, Kan-Lin Hsiung, and Hsin-Yu Chen. 2024. GRNN-Based Detection of Eavesdropping Attacks in SWIPT-Enabled Smart Grid Wireless Sensor Networks. *IEEE Internet of Things Journal* 11, 22 (2024), 37381–37393. doi:10.1109/JIOT.2024.3443277

[4] Farhana Reza. 2024. DDoS-Net: Classifying DDoS Attacks in Wireless Sensor Networks with Hybrid Deep Learning. In *2024 6th International Conference on Electrical Engineering and Information & Communication Technology (ICEEICT)*. 487–492. doi:10.1109/ICEEICT62016.2024.10534545

[5] Rana Sabah, Meng Chun Lam, Faizan Qamar, and B. B. Zaidan. 2024. A BiLSTM-Based Feature Fusion With CNN Model: Integrating Smartphone Sensor Data for Pedestrian Activity Recognition. *IEEE Access* 12 (2024), 142957–142978. doi:10.1109/ACCESS.2024.3468470

[6] Sundaresan Sabapathy, Surendar Maruthu, and Dushantha Nalin K. Jayakody. 2025. Multi-User Sparse Vector Coding for eXtreme Ultra-Reliable Low-Latency Communication in Beyond 5G. *IEEE Access* 13 (2025), 56780–56792. doi:10.1109/ACCESS.2025.3551398

[7] Vishalya P. Sooriarachchi and Dushantha Nalin K. Jayakody. 2024. Model for Advanced Sensor Placement in Wildfire Detection Systems. In *2024 IEEE Wireless Communications and Networking Conference (WCNC)*. 1–6. doi:10.1109/WCNC57260.2024.10570764

[8] Vishalya P Sooriarachchi, P T D Perera, and D N K Jayakody. 2025. Ambient Backscatter- and Simultaneous Wireless Information and Power Transfer-Enabled Switch for Indoor Internet of Things Systems. *Applied Sciences* 15 (2025), 478. doi:10.1109/ACCESS.2025.3551398

[9] Didik Sudyana, Ying-Dar Lin, Miel Verkerken, Ren-Hung Hwang, Yuan-Cheng Lai, Laurens D'Hooge, Tim Wauters, Bruno Volckaert, and Filip De Turck. 2024. Improving Generalization of ML-Based IDS With Lifecycle-Based Dataset, Auto-Learning Features, and Deep Learning. *IEEE Transactions on Machine Learning in Communications and Networking* 2 (2024), 645–662. doi:10.1109/TMLCN.2024.3402158

[10] Gehan Sathsara Vithanage and Dushantha Nalin K. Jayakody. 2024. Rectifier Non-Linearity Exploitation for Performance Gains in SWIPT. In *2024 2nd International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES)*. 1–6. doi:10.1109/SCOPES64467.2024.10990923

[11] Jun Xie, Bo Chen, Xinglong Gu, Fengmei Liang, and Xinying Xu. 2019. Self-Attention-Based BiLSTM Model for Short Text Fine-Grained Sentiment Classification. *IEEE Access* 7 (2019), 180558–180570. doi:10.1109/ACCESS.2019.2957510