Routing attacks detection in IoT networks using LSTM autoencoder*

Nataliia Petliak[1,†], Yurii Klots[1,*,†], Dmytro Tymoshchuk[2,*,†], Mikolaj Karpinski[3,†] and Vira Titova[1,†]

[1] Khmelnytskyi National University, 11, Instytuts'ka str., Khmelnytskyi, 29016, Ukraine
[2] Ternopil Ivan Puluj National Technical University, 56, Ruska str. Ternopil, 46001, Ukraine
[3] University of the National Education Commission, 2 Podchorążych str, Krakow, 30084, Poland

Abstract

The article discusses the problem of detecting routing attacks in wireless sensor networks, which are an important component of the Internet of Things (IoT) infrastructure. In particular, the vulnerabilities of the RPL protocol, which is widely used in low-power networks, are investigated. A method for detecting anomalies is proposed, based on the use of an LSTM autoencoder capable of modeling the time sequence of routing parameters such as delay, etx, charge level, hop count, and parent ID. The model is trained on "normal" samples and allows identifying deviations in node behavior characteristic of blackhole, wormhole, and other types of attacks. Experimental modeling using the CICIoT2023 dataset was performed, which demonstrated the high accuracy of the model (98.4%) and its ability to effectively classify anomalous situations. The results indicate the promise of using recurrent deep learning architectures to ensure cybersecurity in resource-constrained IoT environments.

Keywords

machine learning, IoT, routing attacks, WSN, RPL protocol, LSTM autoencoder, anomaly detection, cybersecurity, deep learning, energy-constrained networks, time series analysis

1. Introduction

The Internet of Things (IoT) is a complex network of interconnected devices that provides continuous exchange of information between various "smart" objects, such as mobile phones, household appliances, security systems, medical sensors, etc. [1–3]. With the development of IoT, the number of connected devices is growing significantly, transforming traditional methods of collecting, transmitting, and using data in various fields of activity [4]. However, along with the growing popularity of IoT, cyber threats are also increasing, creating a need for in-depth study of potential vulnerabilities and the development of appropriate protective measures [5–8]. This is especially true for low-power wireless networks, where limited device resources create additional challenges for implementing effective security measures.

The modern development of IoT is impossible to imagine without the use of protocols optimized for operation in conditions of limited resources and energy efficiency. One such protocol is IPv6 over Low Power Wireless Personal Area Networks (6LoWPAN), which enables devices with limited computing power to be integrated into the Internet using IP addressing. Although 6LoWPAN contributes to the expansion of the functionality of IoT systems [9], it is also vulnerable to a number of attacks, including routing attacks, which can compromise data integrity and availability, disrupt communication between devices, and threaten the confidentiality of transmitted information. The difficulty of detecting such attacks is compounded by the dynamic and frequently

*BAITmp'2025: The 2nd International Workshop on "Bioinformatics and Applied Information Technologies for medical purpose", November 12-13, 2025, Ben Guerir, Morocco
[1,*] Corresponding author.
[†] These authors contributed equally.
npetlyak@khmnu.edu.ua (N. Petliak); klots@khmnu.edu.ua (Y. Klots); dmytro.tymoshchuk@gmail.com (D. Tymoshchuk); mikolaj.karpinski@uken.krakow.pl (M. Karpinski); titovav@khmnu.edu.ua (V. Titova)
0000-0001-5971-4428 (N. Petliak); 0000-0002-3914-0989 (Y. Klots); 0000-0003-0246-2236 (D. Tymoshchuk); 0000-0002-8846-332X (M. Karpinski); 0000-0001-8668-4834 (V. Titova)

changing network topology, as well as the limited computing resources and energy capabilities of most IoT devices [9].

An important element of the infrastructure of wireless sensor networks, which are an integral part of the IoT, are routing protocols that ensure the proper functioning of the communication process. The Routing Protocol for Low-Power and Lossy Networks (RPL) is one of the most common solutions for routing in low-power networks [10]. RPL is adapted to the conditions of limited device resources and the characteristics of wireless networks with high loss rates, which makes it attractive for widespread use in IoT environments [11]. However, this protocol is not without its drawbacks, as it is vulnerable to numerous types of attacks that can target various network components, causing resource depletion, routing integrity violations, and data transmission interference. As a result, the service life of individual devices and the network as a whole can be significantly reduced, and the stability of the system can be threatened.

Wireless sensor networks, which are often used in the IoT, are important in many application areas, such as environmental monitoring, agricultural management, healthcare, military control, industrial surveillance, traffic management, etc. [12]. The nodes of such networks consist of sensors, power sources, controllers, and communication devices, which enable the collection, processing, and transmission of information. However, due to limited energy and computing resources, as well as the peculiarities of the distributed structure, these systems are vulnerable to numerous technical and organizational problems, including energy efficiency, communication reliability, security, synchronization, and node localization. Extending the network's service life is achieved, in particular, by selecting optimal nodes as cluster heads that support routing while ensuring security, which is an important aspect in the design of large IoT networks. There are various methods for solving secure routing problems, which, depending on the network architecture, are divided into protocols based on node location, linear and hierarchical algorithms [13]. Location-based protocols use the geographical coordinates of nodes to determine routes, linear algorithms assign equal functional roles to each node, and hierarchical algorithms distribute different roles among nodes to improve efficiency and security. However, traditional routing methods often do not take into account the risks associated with network congestion, which arises due to insufficient bandwidth, long data processing delays, packet loss, and energy depletion. Congestion negatively affects the overall quality of service, reducing network performance and reliability. Traditional overload control mechanisms in wireless sensor networks do not sufficiently account for the impact of attacks by malicious actors who can initiate and maintain overload conditions, making it difficult to detect and counter threats. Malicious nodes, which often operate covertly, can carry out Sybil attacks and node replication. They can also generate excessive traffic through repeated messages. This leads to increased computational load and accelerated battery depletion of nodes. As a result, the overall service life of the network is significantly reduced, with a simultaneous decrease in stability and reliability. The ability of IoT devices to collect and analyze data in real time enables more efficient resource management, process automation, and improved security and control systems. The rapid development of IoT is accompanied by growing challenges in the field of cybersecurity. With the widespread adoption of IoT devices, the number of cyberattacks is also growing. The vulnerability of the RPL protocol to various types of attacks remains one of the security issues. Such attacks can cause large-scale network failures, service disruptions, and significant financial losses [14]. Ensuring comprehensive protection of IoT networks requires not only the development of new protocols and routing methods, but also the integration of attack detection mechanisms.

2. Similar works

Routing attacks are a separate class of cyberattacks aimed at disrupting or manipulating the data transmission process in computer networks, particularly in the context of IoT, corporate infrastructures, mobile ad hoc networks, and the global Internet. The main goal of such attacks is to redirect, replace, or destroy network traffic, which can lead to a breach of communication

integrity, leakage of confidential information, disruption of service availability, or increased vulnerability to secondary attacks [15].

Classic examples of routing attacks include Man-in-the-Middle attacks, in which an attacker integrates into the communication channel between two nodes to intercept or modify data; routing table poisoning, in which false routing announcements are sent to the network in order to distort the network map; black hole attacks, in which a malicious node announces the presence of an optimal route to any node and destroys the received traffic; wormhole attack, which involves creating a tunnel between two nodes to deceive routing mechanisms; and BGP hijacking, which is particularly significant at the global level because it allows traffic to be redirected through third-party, potentially dangerous autonomous systems.

Approaches to protecting against such attacks include routing information authentication mechanisms, route filtering, monitoring for anomalous activity, cryptographic protection of traffic, and the implementation of trust models in wireless and mobile networks. For example, protocols such as IPsec ensure the integrity and authenticity of routing messages, while BGPsec extends the functionality of the basic BGP protocol with digital signing of routes. Prefix-based route filtering or the use of access control lists (ACLs) can reduce the risk of accepting malicious routes, although these methods often require manual configuration and do not scale well in large networks. Monitoring systems such as BGPMon or RIPE RIS are used to observe changes in routes on a global scale, but they usually only kick in after an attack has already taken place. Data encryption using VPN or TLS/SSL protocols prevents unauthorized reading of packet contents, but does not guarantee protection against route manipulation. In the context of mobile networks, trust-based routing models are used, which are based on the evaluation of node behavior (trust-based or reputation-based routing), but such systems have low accuracy in the face of Sybil attacks and depend on the availability of centralized validation mechanisms, which contradicts the principle of decentralization. The limitations of modern protection methods include the high computational complexity of cryptographic protocols, the need for manual configuration of route filters, the limited effectiveness of threat detection systems, and dependence on the correct configuration of secure connections.

The study [16] proposes the HTCCR (Hybrid Trust-based Congestion-aware Cluster Routing) protocol as a solution for improving security and routing efficiency in wireless sensor networks. The solution is based on a hybrid clustering mechanism using trust metrics, residual energy, queue status, and distance to the base station, which allows for adaptive route formation and detection of malicious nodes. The implementation of priority routing for different types of traffic reduces delays, congestion, and packet loss. The simulation results demonstrate the superiority of HTCCR over other protocols in terms of energy efficiency, delivery reliability, and attack detection accuracy. In article [17], the authors propose an Optimized Reporting Module (ORM) based on delta-oriented trust computation to detect and isolate nodes involved in black hole attacks in Green IoT networks. The solution is based on a combined approach using direct and indirect trust, which is calculated using indicators such as energy, similarity, and behavior dynamics, taking into account the forgetting curve to prioritize recent node actions. The main advantage of the proposed model is the reduction in the number of false positives and the reduction in the load on the root node of the network by transmitting reports only when there is a critical decrease in trust, which ensures stability and scalability in networks with limited resources. However, among the disadvantages, it should be noted that integration into real systems may be difficult due to the need for precise configuration of trust parameters, as well as the dependence of effectiveness on the accuracy and objectivity of the collected feedback. In article [18], the authors proposed a distributed intrusion detection mechanism that combines the accumulation phase of activity variables with multidimensional evaluation using fuzzy logic and two-stage verification before blocking suspicious nodes. The system shows high adaptability for both static and mobile RPL networks, providing extremely accurate attack detection with a high F_1 measure, while reducing power consumption and latency and increasing packet delivery rates compared to current IDS solutions. The advantages of the solution include the ability to process multiple metrics with a

single fuzzy mechanism, which minimizes false positives, and the presence of a confirmation mechanism before blocking, which reduces the risk of excluding legitimate nodes. At the same time, the presented model has limitations, including increased computational complexity of the activity analysis phase and fuzzy logic, which does not take into account the resources of very limited nodes. The effectiveness of the system depends on the accuracy of the selected fuzzy rules and threshold values, which requires careful calibration taking into account the specific characteristics of the network. Thanks to their ability to reveal hidden patterns in large data sets, machine learning methods are actively used in various fields, including materials science [19–23], cybersecurity [24–27], medicine [28–31], computer vision [32–35], and finance [36–39]. The complexity of the topology, limited computing resources, and the dynamic nature of attacks complicate the application of traditional protection methods in IoT networks. This makes machine learning a promising tool in the context of IoT network security. In [40], the authors propose a mechanism for detecting routing attacks for wireless sensor networks based on a multilayer neural network with a direct layer that analyzes the dynamic behavior of the network and recognizes threats such as black hole, gray hole, and wormhole attacks using learning and general model generalization. The proposed solution is capable of adapting to unknown attack patterns, which makes it promising for real-world application in resource-constrained environments. However, the architecture of the solution requires computations in an NS2-supported environment and significant computing power, which can be difficult to implement on embedded WSN nodes. In addition, the effectiveness of the mechanism largely depends on the quality of the CICIDS2017 training set, which may reduce overall reliability when transferred to other types of networks. In [41,42], the authors also propose methods for detecting network attacks using neural networks, but these require computational resources and retraining when the network topology changes. In article [43], the authors propose a method for detecting attacks in IoT networks based on a combination of routing metric analysis (in particular, ETX, hop count, delay) and classification using a multilayer neural network configured for the specifics of the 6LoWPAN environment. The main advantage of this approach is the ability to process complex anomaly patterns without using rule sets, thanks to an adaptive self-learning neural network. However, the integration of such a system can be complicated by the need to determine the optimal network architecture and select hyperparameters, which requires significant computing resources. The authors [44] propose a hybrid anomaly detection system based on RPL, which combines an autoencoder for detecting atypical patterns in network metrics and Similarity Network Fusion (SNF) for integrating information from multiple data sources. The solution demonstrates high sensitivity to wormhole and gray hole attacks. However, the algorithm has high computational complexity and depends on the configuration of the autoencoder and SNF hyperparameters, which can complicate integration on embedded devices with limited resources. Studies [45–47] also apply machine learning methods to detect routing attacks, such as black holes, gray holes, and wormholes, which were mentioned above. Their approaches focus on analyzing anomalous node behavior in IoT and 6LoWPAN networks using classification algorithms such as artificial neural networks, decision trees, and support vector machines.

3. Basics

Routing parameters have a sequential temporal nature. This means that each node in the network generates not separate independent records, but dynamic time series that describe the change in its state over a certain period. In this regard, traditional autoencoders based on fully connected layers are not effective enough, as they do not take into account temporal dependencies between events [48]. Instead, Long Short-Term Memory (LSTM) is a specialized architecture capable of retaining long-term dependencies in time series, which is important for analyzing the behavioral patterns of network nodes. The LSTM autoencoder architecture combines the advantages of two approaches: compressing sequences into a representation using an encoding module (LSTM encoder) and restoring these sequences using a decoding module (LSTM decoder). At the same time, the model is

trained only on “normal” samples, i.e., network behavior in the absence of attacks. As a result, it learns patterns of standard routing activity. After training, such a model is capable of comparing input sequences with the expected normal pattern. If the behavior of a node differs significantly from the trained one (i.e., has a high reconstruction error), it is automatically classified as anomalous, allowing the potential attack to be localized. It is also worth noting that LSTM autoencoders are effective in cases where anomalies are complex or hidden in nature, as is typical for routing attacks. Thanks to the ability of the LSTM structure to remember temporal relationships, the model can recognize not only instantaneous deviations, but also slow drifts in node behavior, which are typical for distributed attacks with a delayed effect. Therefore, the use of LSTM autoencoders is appropriate for detecting routing attacks in IoT environments, as this approach combines the ability to model the sequential nature of data, detect complex anomalies without prior attack labeling, and provides adaptability to different types of threats in distributed networks with limited resources.

In the context of building models for detecting routing attacks in IoT networks, especially those based on the RPL protocol, the choice of input parameters is essential for accurately representing both normal and abnormal behavior of network nodes. This study uses five main characteristics: data transmission delay (delay), expected number of transmissions (etx), device charge level (battery), number of hops to the gateway (hop_count), and parent node identifier (parent_id). These characteristics were chosen because of their ability to reflect critical aspects of RPL protocol functioning, as well as their sensitivity to abnormal influences caused by external or internal threats. Delay is an indicator of the efficiency of data transmission along a route. In a stable network environment, the value of this parameter is relatively constant, while sudden changes in it may signal routing failures or interference from third-party nodes. The expected number of transmissions (etx), which reflects the average number of attempts required for successful packet delivery, is a direct indicator of the quality of the communication channel. In the context of the RPL protocol, which uses etx as one of the key metrics in its objective functions (e.g., MRHOF — Minimum Rank with Hysteresis Objective Function), abnormally high values of this parameter may indicate route disruptions, packet loss, or attempts at malicious traffic interception. The battery parameter, which indicates the charge level of a node, is important for analyzing the behavior of energy-dependent devices. Under normal conditions, nodes with low energy levels avoid participating in routing, but in cases of attacks such as black hole or sinkhole, malicious nodes can ignore their own energy status and artificially attract traffic for interception or destruction. The number of hops to the gateway (hop_count) is another topological parameter that determines how far a node is from the root device (DAG root) in the routing tree. Sudden changes in this metric may be the result of falsification of routing information or the appearance of “wormholes,” i.e., tunnels created between separate parts of the network to deceive the routing logic. The parent node identifier (parent_id) provides information about the current route of the node towards the root. In networks operating under RPL control, the parent node is selected based on a comprehensive assessment of availability, connection quality, and energy efficiency. A change of parents for no apparent reason or at a high frequency may indicate an attempt to redirect traffic, particularly in the context of black hole or routing table poisoning attacks. That is why the parent_id parameter is useful for detecting topological instability caused by malicious influences. The above parameters allow us to cover both dynamic routing characteristics and stability indicators, connection quality, and energy resource status. This provides sufficient information for effective training of anomaly detection models, in particular neural networks based on autoencoders or recurrent architectures. Given that the RPL protocol supports adaptation based on several metrics simultaneously, the combination of delay, etx, battery, hop_count, and parent_id forms a representative feature space for analyzing both normal and attacked behavior of nodes in IoT networks.

For each node $i \in \{1,2,\ldots,n\}$ we have a sequence of T vectors of features of dimension d. Let us represent time series in the form:

$$X^i = \left\{ x_1^i, x_2^i, \ldots, x_T^i \right\}, x_t^i \in R^d \quad (1)$$

where X^i – i-th sequence of length T; $x_t^i = \left[x_{t,1}^i, x_{t,2}^i, \ldots, x_{t,d}^i \right]$ – i-th feature vector at time t; $d = 5$ – number of signs: delay, etx, battery, hop_count, parent_id.

Min-Max Scaling converts the values of each feature from an arbitrary range to a range [0,1]:

$$x_{scaled} = \frac{x - x_{min}}{x_{max} - x_{min}}, \ \forall x \in X \quad (2)$$

At the input of LSTM, we have a tensor $X \in R^{n \times T \times d}$, where n – number of nodes (batch size); T – time series length; d – dimension of the feature vector (input_size).

For each node (sequence), LSTM processes elements in time:

$$h_t^i, c_t^i = LSTM\left(x_t^i x_t, h_{t-1}^i, c_{t-1}^i \right) \quad (3)$$

where $h_t^i \in R^d$ – hidden state; $c_t^i \in R^d$ – memory status; d – dimension of the hidden layer of LSTM (hyperparameter).

In the last step, we obtain the representation vector:

$$z^i = h_T^i \in R^{64} \quad (4)$$

The sequence is decoded from the initialized vector:

$$\hat{h}_t = LSTM_{dec}\left(z^i, \hat{h}_{t-1}, \hat{c}_{t-1} \right) \quad (5)$$

Restoration to the space of signs:

$$\hat{x}_t = W \hat{h}_t + b, \ \forall t \in \left\{ 1, \ldots, T \right\}, \quad (6)$$

where $W \in R^{5 \times 64}, b \in R^5$.

Training is performed only on normal data. The mean square error of reconstruction is optimized:

$$L = \frac{1}{T * d} \sum_{t=1}^{T} \sum_{j=1}^{d} \left(x_{t,j}^i - \hat{x}_{t,j}^i \right)^2 \quad (7)$$

Reconstructed vector:

$$\hat{X}^i = \left\{ \hat{x}_1^i, \ldots, \hat{x}_T^i \right\} \quad (8)$$

Mean square error for each sequence:

$$MSE^i = \frac{1}{T * d} \sum_{t=1}^{T} \sum_{j=1}^{d} \left(x_{t,j}^i - \hat{x}_{t,j}^i \right)^2 \quad (9)$$

The threshold value is determined by the 95th percentile of errors in the training sample:

$$\tau = Percentile_{95}\left(\left\{ MSE^i \right\}_{train} \right) \quad (10)$$

Classification:

$$\hat{y}^i = \begin{cases} 0, if \ MSE^i \le \tau \\ 1, if \ MSE^i > \tau \end{cases} \quad (11)$$

Figure 1 shows a block diagram of attack detection using LSTM Autoencoder.

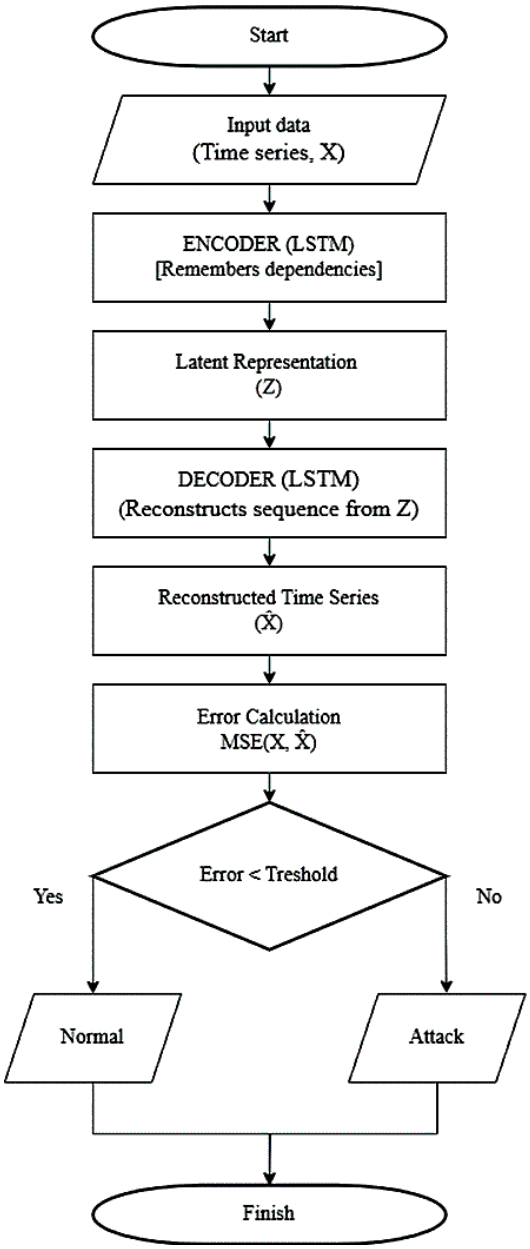

Figure 1: Block diagram of attack detection using LSTM Autoencoder.

The paper implements an architecture for detecting anomalies in time series of routed IoT data based on an LSTM autoencoder. The model combines deep learning with preprocessing of data and statistical evaluation of deviations. The architecture is based on an LSTM layer with 64 neurons and a ReLU activation function, which allows the model to take into account dependencies in the time dimension. At the encoder stage, the input sequence of size 10×5 (10 time steps with 5 features: delay, etx, battery, hop_count, parent_id) is compressed into a latent vector of fixed length. The vector is repeated using the RepeatVector layer, which forms a sequence of ten repetitions of the latent representation. The decoder reconstructs the original sequence through another LSTM layer with 64 neurons and a ReLU function, after which a TimeDistributed layer with a fully connected layer is applied, returning the output in the same format as the input data.

The model is compiled with the Adam optimizer and a loss function in the form of mean square error. Training is performed on normal samples selected from 80% of the sample, with subsequent division into training and validation subsets. The number of training epochs was 50, and the batch size was 32. MinMaxScaler was used to normalize the features, which guarantees scaling of values within [0,1], which is important for the stable operation of LSTM layers.

After training was completed, the model was applied to the test sample to reconstruct the sequences. The error rate of each sample was calculated as the average square difference between the initial and reconstructed data across all features and time steps. To separate normal and abnormal examples, an error threshold was determined based on the 95th percentile of MSE values on the training set. All samples that showed a reconstruction error higher than this threshold were classified as anomalies.

4. Reliability assessment

The CICIoT2023 dataset was used to generate the data for this anomaly detection task. During the experimental study, a system for detecting routing anomalies in IoT networks was modeled based on an LSTM autoencoder, which was trained exclusively on normalized (safe) data (Table 1). The total size of the initial sample was 10,000 records, evenly distributed between the "safe" and "unsafe" classes (5,000 each). To train the model, 80% of the sample (8,000 records) was selected, including 4,000 normal and 4,000 abnormal samples, but the training process itself was performed only on normal samples. The remaining 2,000 records (1,000 for each class) were used to evaluate the quality of classification during the testing phase.

Table 1
Distribution of records in the dataset by training and testing stages

Records	Total	Safe	Unsafe
Train	8,000	4,000	4,000
Test	2,000	1,000	1,000
All data	10,000	5,000	5,000

The LSTM autoencoder model was trained for 50 epochs using the Adam optimizer and a loss function in the form of mean squared error (MSE). After training, a classification threshold was determined based on the 95th percentile of MSE for the training set, which allowed the test samples to be divided into normal and abnormal without the need to label attacks during training.

Analysis of the confusion matrix for the test set showed high classification accuracy (Table 2). The model correctly classified 981 out of 1000 abnormal samples (True Positive), with only 19 false negatives (False Negative). At the same time, it correctly identified 984 normal samples (True Negative), with only 16 false positives (False Positive). Thus, the model's accuracy was 98.4%, which indicates its high ability to detect atypical behavior of routed IoT nodes.

Table 2
Classification error matrix for the test sample

Records	Total	Test			
		TP	TN	FP	FN
Safe	1,000	0	984	16	0
Unsafe	1,000	981	0	0	19

Based on the data obtained, the following performance indicators can be calculated.

Recall – the ratio of correctly classified positive samples to the total number of positive samples:

$$Recall = \frac{TP}{TP + FN} \quad (12)$$

Precision – the proportion of correctly identified malicious events among all events that the system identified as malicious:

$$Precision = \frac{TP}{TP + FP} \quad (13)$$

Accuracy – the proportion of correctly detected and correctly undetected events among all events:

$$Accuracy = \frac{TP + TN}{TP + FP + FN + TN} \quad (14)$$

The results presented in Figure 2 demonstrate the high efficiency of the constructed classification model according to the main quality assessment metrics. In particular, the accuracy is 98.25%, which indicates the model's overall ability to correctly classify both safe and unsafe records. A recall of 98.10% indicates the model's ability to detect the vast majority of truly dangerous cases without significant losses. At the same time, a precision of 98.40% indicates that most objects classified as dangerous are indeed so. In general, the obtained metric values indicate the balanced and reliable operation of the model, which allows for the effective detection of threats with a minimum number of false positives and false negatives.

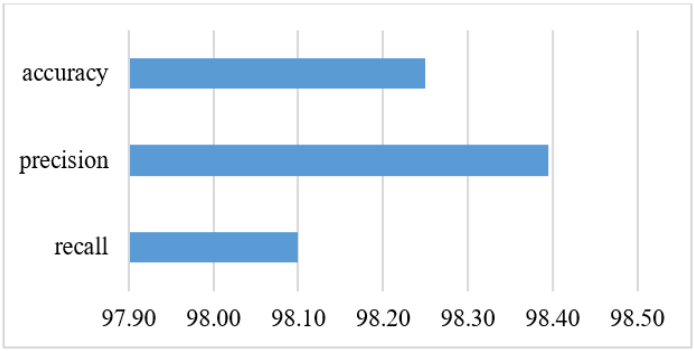

Figure 2: Model evaluation results by key metrics.

For a more visual analysis of the effectiveness of the constructed LSTM autoencoder model, the distribution of the reconstruction error (MSE) and the dynamics of loss changes during training were visualized.

Figure 3 shows the distribution of reconstruction error for normal (marked in blue) and abnormal (marked in orange) sequences. As can be seen from the histogram, the MSE values for safe (normal) samples are concentrated in the range from 0 to 0.06, while the errors for abnormal samples are mainly in the range of 0.32–0.38. Such a clear gap between the two distributions indicates effective training of the autoencoder on normal behavior patterns and allows setting a threshold value for sample classification. The position of the 95th percentile on the training set of normal samples is between these groups, which ensures high sensitivity and specificity of the model in detecting anomalies.

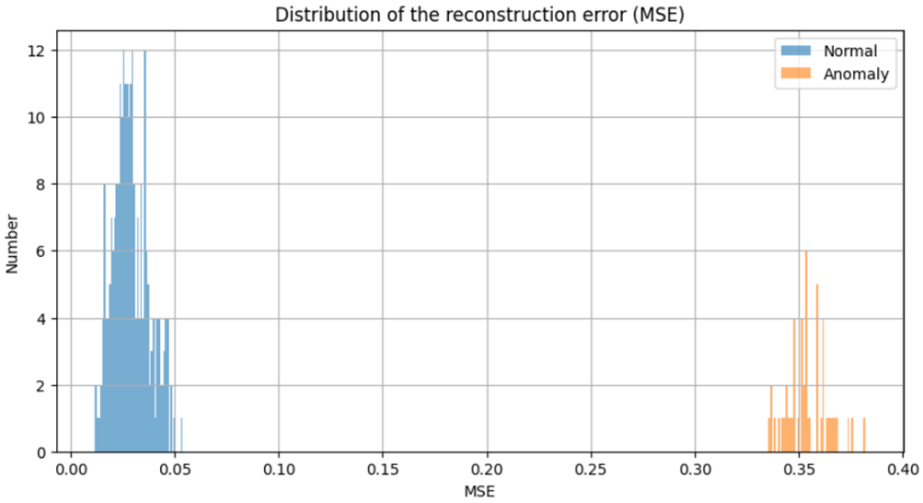

Figure 3: Visualization of reconstruction errors for anomaly detection.

Figure 4 shows a graph of the change in the root mean square error on the training and validation samples over 50 training epochs.

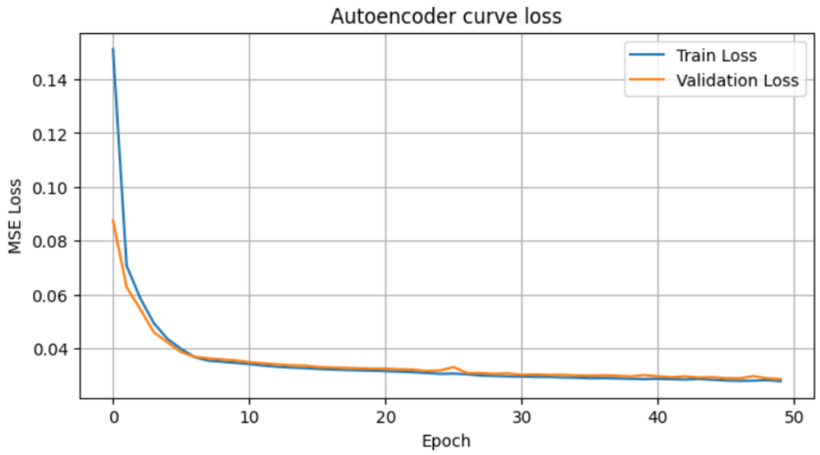

Figure 4: Dynamics of model loss MSE during training.

A rapid decrease in loss is observed during the first 10 epochs, after which the curve approaches a plateau, indicating model convergence. The absence of a significant difference between the Train Loss and Validation Loss curves indicates stable training without overfitting. The final loss values on both sets are at the level of ≈0.03, which indicates a high level of the model's ability to reproduce the normal behavior of IoT nodes.

5. Conclusions

The paper implemented and experimentally investigated a model for detecting routing anomalies in IoT networks based on an LSTM autoencoder trained on normal data. The proposed model demonstrated high efficiency in detecting atypical behavior of network nodes, achieving a classification accuracy of 98.4%. The main advantage of this approach is the model's ability to detect both obvious and hidden anomalies without prior attack labeling, which is especially relevant for real IoT environments with limited resources.

The use of the LSTM recurrent architecture made it possible to effectively model time dependencies between routing parameters such as transmission delay, number of hops, expected number of transmissions, device charge level, and parent node identifier. Setting the threshold

value at the 95th percentile of the root mean square error allowed us to adaptively identify anomalous patterns in the test set without additional tuning to the specifics of the attacks.

Thus, the results of the study confirm the feasibility of using LSTM autoencoders as a basis for building systems for detecting routing anomalies in RPL-type protocols in the context of IoT. Further work includes optimizing the computational complexity of the model for its integration into real sensor nodes, as well as extending the approach by combining it with other methods, in particular, trust models, statistical analysis, and hybrid deep networks to detect more complex attacks in distributed networks.

Declaration on Generative AI

During the preparation of this work, the authors used Grammarly in order to grammar and spell check, and improve the text readability. After using the tool, the authors reviewed and edited the content as needed to take full responsibility for the publication's content.

References

[1] P. Matthew, S. Mchale, X. Deng, G. Nakhla, M. Trovati, N. Nnamoko, E. Pereira, H. Zhang, M. Raza, A Review of the State of the Art for the Internet of Medical Things, Sci 7.2 (2025) 36. doi:10.3390/sci7020036.

[2] A. Palamar, M. Karpinski, M. Palamar, H. Osukhivska, M. Mytnyk, Remote Air Pollution Monitoring System Based on Internet of Things, CEUR Workshop Proceedings, 2022, 3309, pp. 194–204.

[3] Koroliuk, R., Nykytyuk, V., Tymoshchuk, V., Soyka, V., Tymoshchuk, D. Automated monitoring of bee colony movement in the hive during winter season. CEUR Workshop Proceedings, 2024, 3842, pp. 147-156

[4] I. Ficili, M. Giacobbe, G. Tricomi, A. Puliafito, From Sensors to Data Intelligence: Leveraging IoT, Cloud, and Edge Computing with AI, Sensors 25.6 (2025) 1763. doi:10.3390/s25061763.

[5] Klots Y., Petliak N., Martsenko S., Tymoshchuk V., Bondarenko I. Machine Learning system for detecting malicious traffic generated by IoT devices. CEUR Workshop Proceedings, 2024, 3742, pp. 97 – 110

[6] Y. Yan, Y. Yang, S. Fang, M. Gao, Y. Chen, MUS Model: A Deep Learning-Based Architecture for IoT Intrusion Detection, Comput., Mater. & Contin. (2024) 1–10. doi:10.32604/cmc.2024.051685.

[7] Tymoshchuk, D., Yasniy, O., Mytnyk, M., Zagorodna, N., Tymoshchuk, V. Detection and classification of DDoS flooding attacks by machine learning method. CEUR Workshop Proceedings, 2024, 3842, pp. 184 – 195

[8] S. Elouardi, A. Motii, M. Jouhari, A. N. H. Amadou, M. Hedabou, A survey on Hybrid-CNN and LLMs for intrusion detection systems: Recent IoT datasets, IEEE Access (2024) 1. doi:10.1109/access.2024.3506604.

[9] T. A. Al-Amiedy, M. Anbar, B. Belaton, A. H. H. Kabla, I. H. Hasbullah, Z. R. Alashhab, A Systematic Literature Review on Machine and Deep Learning Approaches for Detecting Attacks in RPL-Based 6LoWPAN of Internet of Things, Sensors 22.9 (2022) 3400. doi:10.3390/s22093400.

[10] P. Maurya, V. Kushwaha, DSNFyS: Deep Stacked Neuro Fuzzy System for Attack Detection and Mitigation in RPL based IoT, Int. J. Inf. Eng. Electron. Bus. 17.3 (2025) 62–83. doi:10.5815/ijieeb.2025.03.05.

[11] R. Sahay, A. Nayyar, R. K. Shrivastava, M. Bilal, S. P. Singh, S. Pack, Routing attack induced anomaly detection in IoT network using RBM-LSTM, ICT Express (2024). doi:10.1016/j.icte.2024.04.012.

[12] P. Phalaagae, A. M. Zungeru, B. Sigweni, S. Rajalakshmi, H. Batte, O. S. Eyobu, An Energy Efficient Authentication Scheme for Cluster-based Wireless IoT Sensor Networks, Sci. Afr. (2024) e02287. doi:10.1016/j.sciaf.2024.e02287.
[13] N. Alfriehat, M. Anbar, S. Karuppayah, S. D. A. Rihan, B. A. Alabsi, A. M. Momani, Detecting Version Number Attacks in Low Power and Lossy Networks for Internet of Things Routing: Review and Taxonomy, IEEE Access (2024) 1. doi:10.1109/access.2024.3368633.
[14] K. Ahmadi, R. Javidan, A Trust Based Anomaly Detection Scheme Using a Hybrid Deep Learning Model for IoT Routing Attacks Mitigation, IET Inf. Secur. 2024.1 (2024). doi:10.1049/2024/4449798.
[15] P. P. Ioulianou, V. G. Vassilakis, S. F. Shahandashti, A Trust-Based Intrusion Detection System for RPL Networks: Detecting a Combination of Rank and Blackhole Attacks, J. Cybersecur. Priv. 2.1 (2022) 124–152. doi:10.3390/jcp2010009.
[16] S. N. Bhukya, C. S. R. Annavarapu, Hybrid Reliable Clustering Algorithm with Heterogeneous Traffic Routing for Wireless Sensor Networks, Sensors 25.3 (2025) 864. doi:10.3390/s25030864.
[17] M. A. Khan, R. N. B. Rais, O. Khalid, S. Ahmad, Trust-Based Optimized Reporting for Detection and Prevention of Black Hole Attacks in Low-Power and Lossy Green IoT Networks, Sensors 24.6 (2024) 1775. doi:10.3390/s24061775.
[18] C. Kim, C. So-In, Y. Kongsorot, P. Aimtongkham, FLSec-RPL: a fuzzy logic-based intrusion detection scheme for securing RPL-based IoT networks against DIO neighbor suppression attacks, Cybersecurity 7.1 (2024). doi:10.1186/s42400-024-00223-x.
[19] Stukhliak, P., Totosko, O., Vynokurova, O., & Stukhlyak, D. (2024). Investigation of tribotechnical characteristics of epoxy composites using neural networks. CEUR Workshop Proceedings, 3842, 157–170.
[20] D. Tymoshchuk, O. Yasniy, P. Maruschak, V. Iasnii, I. Didych, Loading frequency classification in shape memory alloys: A machine learning approach, Computers 13.12 (2024) 339. doi:10.3390/computers13120339.
[21] O. Totosko, P. Stukhliak, D. Stukhliak, O. Yasniy, Comprehensive Research of Physical and Mechanical Characteristics of Composite Materials Using Neural Networks, Adv. Mater. Sci. Eng. 2025.1 (2025). doi:10.1155/amse/9142300.
[22] O. Yasniy, D. Tymoshchuk, I. Didych, V. Iasnii, I. Pasternak, Modelling the properties of shape memory alloys using machine learning methods, Procedia Struct. Integr. 68 (2025) 132–138. doi:10.1016/j.prostr.2025.06.033.
[23] O. Yasniy, P. Maruschak, A. Mykytyshyn, I. Didych, D. Tymoshchuk, Artificial intelligence as applied to classifying epoxy composites for aircraft, Aviation 29.1 (2025) 22–29. doi:10.3846/aviation.2025.23149.
[24] Y. Klots, N. Petliak, V. Titova, Evaluation of the efficiency of the system for detecting malicious outgoing traffic in public networks, in: 2023 13th International Conference on Dependable Systems, Services and Technologies (DESSERT), IEEE, 2023. doi:10.1109/dessert61349.2023.10416502.
[25] T. E. Ali, Y.-W. Chong, S. Manickam, Machine Learning Techniques to Detect a DDoS Attack in SDN: A Systematic Review, Appl. Sci. 13.5 (2023) 3183. doi:10.3390/app13053183.
[26] Lypa, B., Horyn, I., Zagorodna, N., Tymoshchuk, D., Lechachenko T. Comparison of feature extraction tools for network traffic data. CEUR Workshop Proceedings, 2024, 3896, pp. 1-11.
[27] P. S. Saini, S. Behal, S. Bhatia, Detection of DDoS Attacks using Machine Learning Algorithms, in: 2020 7th International Conference on Computing for Sustainable Global Development (INDIACom), IEEE, 2020. doi:10.23919/indiacom49435.2020.9083716.
[28] Herasymiuk, A. Sverstiuk, I. Kit, MULTIFACTOR REGRESSION MODEL FOR PREDICTION OF CHRONIC RHINOSINUSITIS RECURRENCE, Wiadomosci Lek. 76.5 (2023) 928–935. doi:10.36740/wlek202305106.
[29] O. Chukur, N. Pasyechko, A. Bob, A. Sverstiuk, Prediction of climacteric syndrome development in perimenopausal women with hypothyroidism, Menopausal Rev. (2022). doi:10.5114/pm.2022.123522.

[30] O. Nykytyuk, A. S. Sverstiuk, D. S. Pyvovarchuk, S. I. Klymnyuk, A multifactorial model for predicting severe course and organ and systems damage in Lyme borreliosis in children, Mod. Pediatr. Ukr. No. 2(130) (2023) 6–16. doi:10.15574/sp.2023.130.6.
[31] G. Battineni, N. Chintalapudi, F. Amenta, Machine learning in medicine: Performance calculation of dementia prediction by support vector machines (SVM), Inform. Med. Unlocked 16 (2019) 100200. doi:10.1016/j.imu.2019.100200.
[32] A. I. Khan, S. Al-Habsi, Machine Learning in Computer Vision, Procedia Comput. Sci. 167 (2020) 1444–1451. doi:10.1016/j.procs.2020.03.355.
[33] O. Yasniy, A. Menou, A. Mykytyshyn, V. Kubashok, I. Didych. Application of neural network platforms for text-based image generation. CEUR Workshop Proceedings, 2024, 3842, pp. 232–240
[34] 2. V. Zhukovskyy, S. Shatnyi, N. Zhukovska, A. Sverstiuk, Neural Network Clustering Technology for Cartographic Images Recognition, in: IEEE EUROCON 2021 - 19th International Conference on Smart Technologies, IEEE, 2021. doi:10.1109/eurocon52738.2021.9535544
[35] E. A. Holm, R. Cohn, N. Gao, A. R. Kitahara, T. P. Matson, B. Lei, S. R. Yarasi, Overview: Computer Vision and Machine Learning for Microstructural Characterization and Analysis, Metall. Mater. Trans. A 51.12 (2020) 5985–5999. doi:10.1007/s11661-020-06008-4.
[36] P. Gogas, T. Papadimitriou, Machine Learning in Economics and Finance, Comput. Econ. 57.1 (2021) 1–4. doi:10.1007/s10614-021-10094-w.
[37] M. F. Dixon, I. Halperin, P. Bilokon, Machine Learning in Finance, Springer International Publishing, Cham, 2020. doi:10.1007/978-3-030-41068-1.
[38] S. Aziz, M. Dowling, H. Hammami, A. Piepenbrink, Machine learning in finance: A topic modeling approach, Eur. Financ. Manag. (2021). doi:10.1111/eufm.12326.
[39] T. Warin, A. Stojkov, Machine Learning in Finance: A Metadata-Based Systematic Review of the Literature, J. Risk Financ. Manag. 14.7 (2021) 302. doi:10.3390/jrfm14070302.
[40] S. Khan, M. A. Khan, N. Alnazzawi, Artificial Neural Network-Based Mechanism to Detect Security Threats in Wireless Sensor Networks, Sensors 24.5 (2024) 1641. doi:10.3390/s24051641.
[41] Klots, Y., Titova, V., Petliak, N., Cheshun, V., Salem, A.-B.M. Research of the Neural Network Module for Detecting Anomalies in Network Traffic. CEUR Workshop Proceedings, 2022, 3156, pp. 378–389
[42] Titova, V., Klots, Y., Cheshun, V., Petliak, N., Salem, A.-B.M. Detection of network attacks in cyber-physical systems using a rule-based logical neural network. CEUR Workshop Proceedings, 2024, 3736, pp. 255–268
[43] A. Alazab, A. Khraisat, S. Singh, S. Bevinakoppa, O. A. Mahdi, Routing Attacks Detection in 6LoWPAN-Based Internet of Things, Electronics 12.6 (2023) 1320. doi:10.3390/electronics12061320.
[44] S. M. Muzammal, R. K. Murugesan, N. Z. Jhanjhi, M. Humayun, A. O. Ibrahim, A. Abdelmaboud, A Trust-Based Model for Secure Routing against RPL Attacks in Internet of Things, Sensors 22.18 (2022) 7052. doi:10.3390/s22187052.
[45] Y. Al Sawafi, A. Touzene, R. Hedjam, Hybrid Deep Learning-Based Intrusion Detection System for RPL IoT Networks, J. Sens. Actuator Netw. 12.2 (2023) 21. doi:10.3390/jsan12020021.
[46] A. Abdelhamid, M. S. Elsayed, A. D. Jurcut, M. A. Azer, A Lightweight Anomaly Detection System for Black Hole Attack, Electronics 12.6 (2023) 1294. doi:10.3390/electronics12061294.
[47] F. Zahra, N. Z. Jhanjhi, N. A. Khan, S. N. Brohi, M. Masud, S. Aljahdali, Protocol-Specific and Sensor Network-Inherited Attack Detection in IoT Using Machine Learning, Appl. Sci. 12.22 (2022) 11598. doi:10.3390/app122211598.
[48] Stetsiuk, M., Anikin, V., Pyrch, O., Kozelskiy, O., Salem, A.-B.M. Method of detecting anomalies in IOT device traffic based on statistical analysis using the modified z score. CEUR Workshop Proceedings, 2025, 3963, pp. 284–298