DOI: https://doi.org/10.36910/6775-2524-0560-2025-61-04
УДК 621.391: 004.89: 004.056
Bieliaiev Pavlo[1], Researcher
https://orcid.org/0000-0003-0650-6232
Lysechko Volodymyr[1], Dr Sc. Professor, Head of the research department for the study and implementation of experience
https://orcid.org/0000-0002-1520-9515
Misiura Oleg[1], PhD, S.R.F., Chief of the Scientific Center
https://orcid.org/0000-0002-3025-3477
[1] Scientific Center of the Air Force Ivan Kozhedub Kharkiv National University of Air Forces, Kharkiv, Ukraine.

NEURAL NETWORK METHOD FOR PREDICTIVE-ADAPTIVE STABILITY CONTROL OF THE MAIN COORDINATOR IN FOG/EDGE INFRASTRUCTURES

Bieliaiev P., Lysechko V., Misiura O. Neural Network Method for Predictive-Adaptive Stability Control of the Main Coordinator in Fog/Edge Infrastructures. This article presents the SENTRY-C neural network method for predictive-adaptive stability control of the main coordinator node in distributed Fog/Edge infrastructures. Unlike classical intrusion-detection and risk-assessment approaches that operate in a reactive mode, SENTRY-C enables continuous forecasting of coordinator degradation and provides proactive control actions under dynamically changing load and threat conditions. The method integrates a Long Short-Term Memory (LSTM) recurrent neural network into the coordinator control loop to model temporal dependencies and evaluate the probability of failure. The experimental evaluation demonstrates that the use of LSTM improves short-term prediction accuracy of stability indicators by 25–35% and reduces the error of predicting degradation probability by up to 30% compared with baseline and basic RNN models. High Pearson correlation coefficients (0.90–0.94) confirm the reliability of the predicted parameters under rapid load variation, gradual degradation and short-term risk spikes. The results show that SENTRY-C maintains the continuity and robustness of coordinator functioning through adaptive parameter updates and real-time feedback. Future research is focused on integrating federated learning and reducing computational complexity to enable deployment of the method in resource-constrained Fog/Edge nodes.
Keywords: Fog/Edge infrastructure, neural networks, predictive stability control, LSTM, coordinator degradation, adaptive monitoring.

Бєляєв П. В., Лисечко В. П., Місюра О. М. Нейромережевий метод прогнозно-адаптивного контролю стабільності головного координатора у Fog/Edge-інфраструктурах. У статті представлено нейромережевий метод SENTRY-C для прогнозно-адаптивного контролю стабільності головного координатора у розподілених Fog/Edge-інфраструктурах. На відміну від класичних методів виявлення вторгнень і оцінювання ризику, що працюють у реактивному режимі, SENTRY-C забезпечує безперервне прогнозування деградації координатора та формування проактивних керуючих дій за умов динамічної зміни навантаження і загроз. Метод інтегрує рекурентну нейронну мережу з архітектурою LSTM у контур керування координатором для моделювання часових залежностей та оцінювання ймовірності відмови. Експериментальні дослідження показали, що застосування LSTM підвищує точність короткострокового прогнозування параметрів стабільності на 25–35% та зменшує похибку прогнозування ймовірності деградації до 30% порівняно з базовими та RNN-моделями. Високі значення коефіцієнтів кореляції Пірсона (0,90–0,94) підтверджують достовірність прогнозованих параметрів за умов швидких змін навантаження, поступової деградації та короткочасних сплесків ризику. Результати засвідчують, що SENTRY-C забезпечує підтримання безперервності та надійності роботи координатора завдяки адаптивному оновленню параметрів і зворотному зв'язку у реальному часі. Подальші дослідження спрямовано на інтеграцію федеративного навчання та зниження обчислювальної складності для застосування методу у ресурс-обмежених вузлах Fog/Edge.
Ключові слова: Fog/Edge-інфраструктура, нейронні мережі, прогнозний контроль стабільності, LSTM, деградація координатора, адаптивний моніторинг.

Statement of a scientific problem.

Modern information and telecommunication systems operate in environments characterized by a high level of dynamic threats, dominated by attacks at the channel, network, and application layers. Existing methods for security assessment [1–15], which are primarily reactive and aimed at detecting violations after their occurrence, do not provide sufficient capabilities for forecasting or adaptive response to threats that evolve over time. Under conditions of rapidly changing topology, workload, and security risks, intelligent methods of management and state prediction for telecommunication nodes become particularly relevant, as they are capable of maintaining system stability and ensuring continuous operation.

In previous studies, the SENTRY-L (Secure Neuro-predicTive Risk-aware Leader) method was developed and substantiated. This method determines the main coordinator node within a distributed Fog/Edge telecommunication environment. The coordinator performs the functions of synchronizing node interactions, balancing information flows, and making security-related decisions based on predicted

stability and risk parameters. However, the selection of a coordinator represents only the initial phase of the operational cycle of such an environment.

After the selection stage, it is essential to ensure the stable functioning of the chosen coordinator node, including continuous monitoring of its current state, forecasting possible degradation, and timely detection of early signs of failure or overload.

To address these challenges, the present study proposes a neural-network method for predictive-adaptive stability control of the active coordinator, referred to as SENTRY-C (Secure Neuro-Predictive Coordinator Control). This method provides continuous analysis of the coordinator's state dynamics after the selection phase, prediction of degradation probability, and timely generation of warning signals indicating potential failure.

The logical structure of the research objectives and scientific tasks is presented in Table 1.

Table 1 – Logical structure of stepwise formulation of the research and technical tasks

Stage	Method	Objective
1	SENTRY-L	Intelligent selection of the coordinator node
2	SENTRY-C (Control)	Prediction and stabilization of the selected coordinator's operation
3	SENTRY-Net	Coordination among multiple coordinators and ensuring global stability of the Fog/Edge infrastructure

Within the framework of this study, the second stage corresponds to the SENTRY-C (Control) method. To implement the predictive and adaptive control mechanism, a recurrent neural network (RNN) was selected.

Its modification based on Long Short-Term Memory (LSTM) provides improved stability and higher accuracy in predicting the coordinator state parameters (Table 2).

Table 2 was compiled based on a generalization of the results presented in studies [4, 6, 7, 12–15], which were conducted using the open benchmark datasets KDD'99, CICIDS2017, and UNSW-NB15.

Table 2 – Comparative performance of neural network architectures

Neural network architecture	Modification/ Class	Advantages / Limitations	Average prediction accuracy, %	Relative complexity
Feed-Forward Neural Network (FFNN)	Basic (without memory)	+ High training speed; simple implementation. – Does not account for sequential dependencies and is insensitive to temporal variations.	≈ 82 %	●
Convolutional Neural Network (CNN)	Spatial processing	+ Effectively detects local patterns in structured data. – Not suitable for temporal dependencies without additional recurrent blocks.	≈ 86 %	● ●
Recurrent Neural Network (RNN)	Basic recurrent model	+ Incorporates short-term memory; effective for sequential data. – Limited in modeling long-term dependencies due to gradient vanishing.	≈ 91 %	● ● ●
Long Short-Term Memory (LSTM)	Extended RNN (with long-term memory)	+ Retains long-term temporal information; stable training; high prediction accuracy. – Requires higher computational resources compared with basic RNN.	≈ 94–96 %	● ● ● ●
Gated Recurrent Unit (GRU)	Simplified LSTM	+ Fewer parameters with comparable accuracy; resource-efficient. – Slightly less accurate for complex long-term dependencies.	≈ 93 %	● ● ●

The comparative analysis presented in Table 2 demonstrates that only neural network architectures of the RNN class and their modifications LSTM and GRU are capable of effectively modeling the temporal evolution of the coordinator's state parameters. These architectures provide the most balanced combination of prediction accuracy and training stability, which justifies the choice of LSTM as the baseline model in the SENTRY-C method for implementing predictive and adaptive stability control of the coordinator.

Research analysis.

The problem of improving the security level of information and telecommunication systems has been examined in a number of studies [1–15].

In works [1–3], the issues of assessing security violations of information resources, detecting and classifying the states of information objects using intelligent approaches were investigated. The proposed methods enable the evaluation of the current state of systems but do not provide mechanisms for predicting the development of threats or the loss of node stability in dynamic environments.

Studies [4–8] considered the application of deep neural networks for intrusion detection in network traffic. The authors justified the efficiency of recurrent architectures (RNN, LSTM) in analyzing temporal dependencies between network states, which improves detection accuracy and reduces false alarm rates in intrusion detection systems.

Research works [9–13] focused on the development of hybrid CNN–LSTM and RNN-based models for anomaly prediction in Internet of Things (IoT) and Fog/Edge infrastructures. It was shown that combining spatial and recurrent networks enhances the generalization capability of models; however, the integration of such approaches into real telecommunication environments for monitoring coordinator states and predicting failures remains an open problem.

In works [14, 15], the possibility of optimizing LSTM models to reduce computational complexity and enable real-time operation, particularly in resource-constrained network nodes, was demonstrated.

Thus, the conducted analysis shows that despite the significant progress in neural-network-based intrusion detection and threat analysis, no approaches have yet been proposed that focus on predictive and adaptive stability control of an active coordinator after its selection stage.

The purpose of the work.

The purpose of this study is to provide a scientific rationale for the SENTRY-C neural network method, which ensures continuous analysis, prediction, and stabilization of the coordinator's operation within a distributed Fog/Edge telecommunication environment.

Presentation of the main material and substantiation of the obtained research results.

To design stability control for the main coordinator node within a distributed Fog/Edge telecommunication environment, a neural network–based method called SENTRY-C is proposed. The method combines recurrent state prediction mechanisms with feedback-based adaptive adjustment of the coordinator parameters.

The algorithmic workflow of the proposed method is illustrated in Fig. 1.

Stages 1–6 implement a sequential process of data acquisition, preprocessing, neural-network-based prediction, state evaluation, and adaptive updating of the coordinator parameters. Thus, the algorithm ensures continuous monitoring, forecasting, and stabilization of the coordinator state parameters $S_i(t)$ in a dynamic environment, which increases the stability of the distributed infrastructure under variable load and security threats [1–3].

The distinctive and key element of the proposed method is the LSTM-RNN (Long Short-Term Memory – Recurrent Neural Network) prognostic core, which provides short-term prediction of the coordinator's stability parameters and calculation of its degradation or failure probability $P_f(i, t+\Delta t)$. The choice of the LSTM architecture is justified by the results of comparative research [4–15], which experimentally confirmed the advantages of this architecture over other types of neural networks (FFNN, CNN, basic RNN, GRU) in analyzing temporal dependencies.

Unlike traditional intrusion detection methods [5–8], which operate in a reactive mode, the use of a recurrent model makes it possible to predict the evolution of unstable coordinator states and to generate early warning signals [9–15].

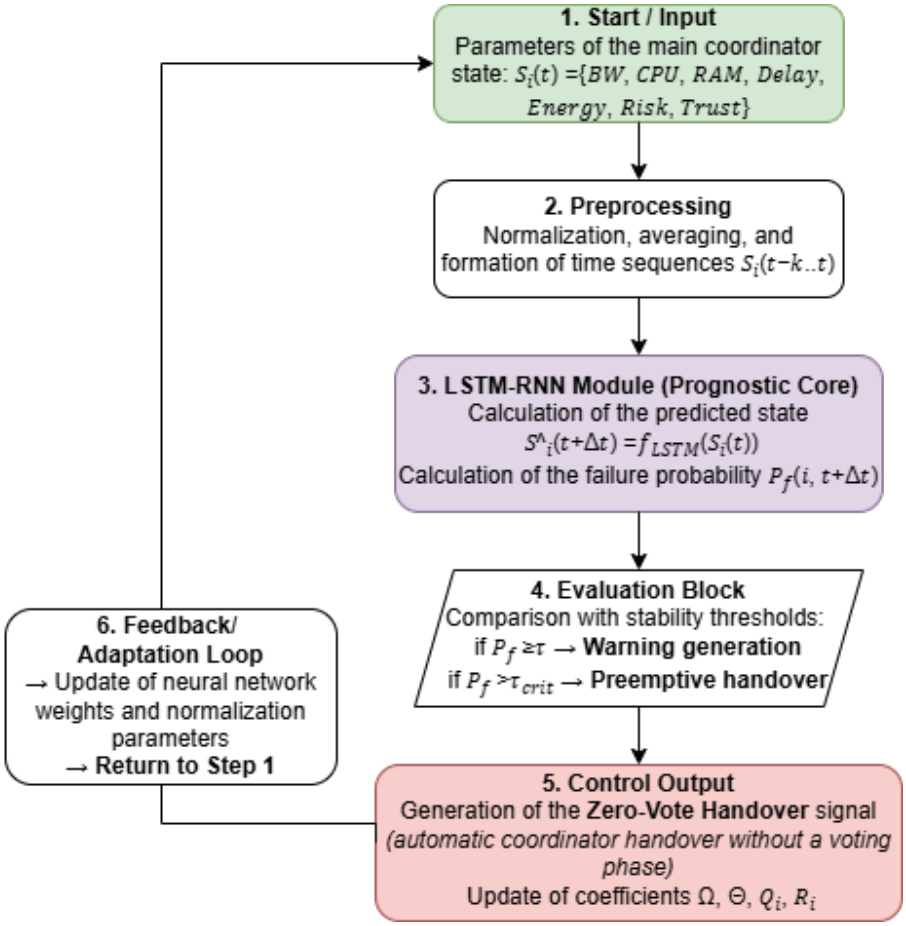

Figure 1 – Block diagram of the algorithm of the predictive-adaptive stability control method (SENTRY-C method)

The structure of an individual LSTM cell used in the prognostic core of the SENTRY-C method is shown in Figure 2 (adapted from [7]).

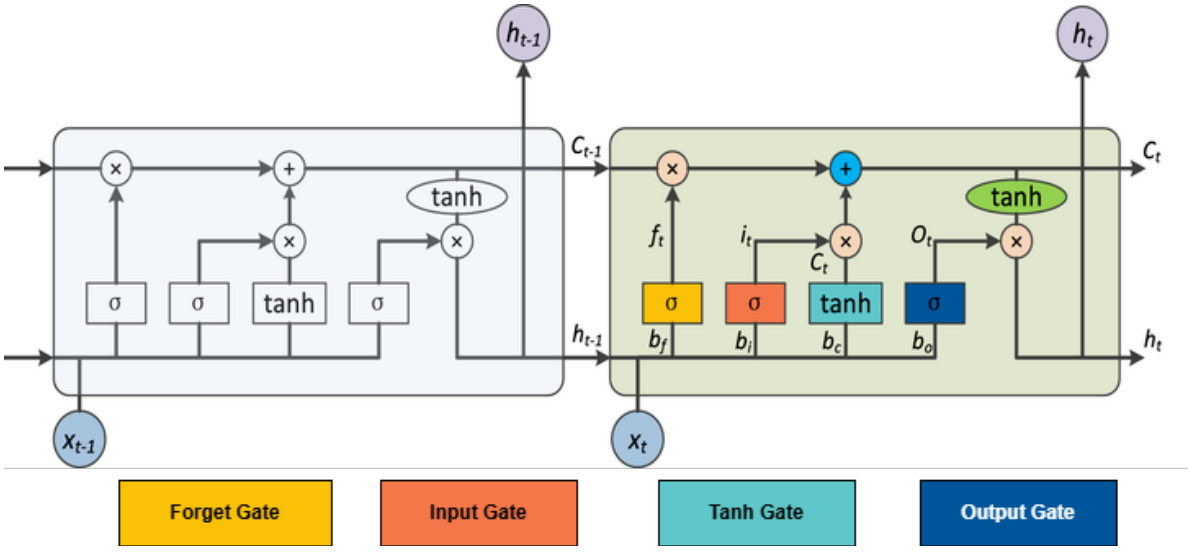

Figure 2 – Internal structure of the LSTM-RNN prognostic module used in the SENTRY-C method

As shown in Fig. 2, the structure of the LSTM-RNN module consists of four interacting blocks: the input gate, the output gate, the forget gate, and the *tanh* activation block. These components determine which information is retained, updated, or discarded at each time step.

The colored part of the diagram corresponds to the active cell at the current time step t, where the coordinator's state prediction is performed, while the gray part illustrates the transfer of information between the previous and the current states $t{-}1{\rightarrow}t$ recurrent connection).

Let us now consider in more detail the step-by-step structure of the proposed SENTRY-C method.

Stage 1. Initialization of coordinator parameters.

At the first step, the state vector is formed as:

$$S_i(t) = \{BW_t, CPU_t, RAM_t, Delay_t, Energy_t, Risk_t, Trust_t\}, \quad (1)$$

where BW_t is the effective channel bandwidth; CPU_t and RAM_t are the utilization levels of computational resources; $Delay_t$ is the average packet latency; $Energy_t$is the energy consumption ; $Risk_t$ is the integrated security-risk indicator; $Trust_t$ is the trust coefficient of the coordinator node.

Initial data are obtained from Fog/Edge monitoring agents.

Stage 2. Data preprocessing.

Input parameters are normalized as:

$$x_j'(t) = \frac{x_j(t) - \mu_j}{\sigma_j + \varepsilon}, \quad (2)$$

where μ_j, σ_j are running mean and standard deviation, and ε prevents division by zero.

Sliding time windows of length $k + 1$ are formed:

$$S_i(t-k{:}\,t) = \{x_1'(t-k{:}\,t), \dots, x_d'(t-k{:}\,t)\}. \quad (3)$$

Stage 3. LSTM-RNN prognostic core.

The neural network block predicts the next state:

$$S_i^*(t + \Delta t) = f_{LSTM}(S_i(t-k{:}\,t)), \quad (4)$$

and estimates the failure probability:

$$P_f(i, t + \Delta t) = \sigma\big(W_p S_i^*(t + \Delta t) + b_p\big), \quad (5)$$

where $\sigma(z) = \frac{1}{1+e^{-z}}$ is the sigmoid activation, W_p, b_p are the output-layer parameters.

The internal dynamics of the LSTM cell are described by:

$$\begin{aligned} f_t &= \sigma\big(W_f[h_{t-1},\, x_t] + b_f\big), \\ i_t &= \sigma(W_i[h_{t-1},\, x_t] + b_i), \\ \tilde{c}_t &= tanh(W_c[h_{t-1},\, x_t] + b_c), \\ c_t &= f_t \odot c_{t-1} + i_t \odot \tilde{c}_t, \\ o_t &= \sigma(W_o[h_{t-1},\, x_t] + b_o), \\ h_t &= o_t \odot \tanh(c_t). \end{aligned} \quad (6)$$

The structure of this module is shown in Fig. 2.

Stage 4. Evaluation block.

Predicted indicators are compared with stability thresholds:

$$\begin{cases} P_f(i, t+\Delta t) \le P_{warn} \Rightarrow \text{stable state}, \\ P_{warn} < P_f(i, t+\Delta t) \le P_{crit} \Rightarrow \text{warning condition}, \\ P_f(i, t+\Delta t) > P_{crit} \Rightarrow \text{preemptive handover}. \end{cases} \quad (7)$$

This enables timely detection of degradation tendencies and proactive control reactions.

Stage 5. Control output.

When the critical threshold is exceeded, a Zero-Vote Handover signal is generated, initiating automatic transfer of coordinator authority without a voting phase.

At this stage, coefficients governing stability and resource balance are updated: Ω, Q_i, R_i, where Ω denotes global weighting for risk factors, Q_i and R_i represent node-specific priorities and reliability indicators.

Stage 6. Feedback and adaptation loop.

At the final stage, the parameters of the neural network are updated based on the newly observed data, enabling continuous self-learning of the predictive-adaptive model:

$$\theta^{t+1} = \theta^{(t)} - \eta \Delta_\theta \mathcal{L}(\mathrm{S}_i, \mathrm{S}_i^*), \quad (8)$$

where η is the learning rate that controls the step size of gradient descent, and $\mathcal{L}$ is the combined loss function, defined as:

$$\mathcal{L} = \lambda_1 \|S_i(t+\Delta t) - \mathrm{S}_i^*(t+\Delta t)\|_2^2 + \lambda_2 BCE\left(y, P_f(i, t+\Delta t)\right), \quad (9)$$

where: $S_i(t+\Delta t)$ is the actual state vector of the coordinator obtained from monitoring;

$\mathrm{S}_i^*(t+\Delta t)$ is the predicted state vector produced by the LSTM-RNN module;

$P_f(i, t+\Delta t)$ is the predicted failure probability for node i;

y∈{0,1} is the target label indicating the true state (0 – stable, 1 – failure);

$BCE(y,p) = -[y\log(p) + (1-y)\log(1-p)]$ is the binary cross-entropy loss;

λ_1 and λ_2 are weighting coefficients that balance the regression and classification components of the total loss;

$\|S_i(t+\Delta t) - \mathrm{S}_i^*(t+\Delta t)\|_2^2$ denotes the squared L_2 norm, i.e. the sum of squared differences between the actual and predicted vector components:

$$\|S_i - \mathrm{S}_i^*\|_2^2 = \sum_{j=1}^{d} \left(S_{ij} - S_{ij}^*\right)^2. \quad (10)$$

The first term of (9) minimizes the prediction error between the actual and forecasted coordinator parameters, ensuring accurate modeling of system dynamics. The second term minimizes the classification error of the failure probability, enabling the network to correctly distinguish between stable and unstable states.

Adjusting the weights λ_1 and λ_2 provides a trade-off between the accuracy of stability prediction and reliability of risk estimation.

After each update, the model parameters θ are refined to improve prediction precision in subsequent control cycles, closing the adaptive feedback loop of the SENTRY-C method.

The algorithm iteratively repeats until the coordinator remains stable within the defined observation interval or the predicted failure probability $P_f(i,t)$ decreases below the warning threshold P_{warn} .

For verification of the proposed SENTRY-C method, a series of experiments was conducted to simulate the dynamics of the coordinator's state in a Fog/Edge-type environment.

The objective of the experiments was to evaluate the prediction accuracy of coordinator stability for three models: the baseline model, a recurrent neural network (RNN), and a long short-term memory (LSTM) network, under three characteristic load variation scenarios: (a) rapid load variation, (b) gradual degradation, and (c) risk spikes. The total simulation time consisted of 300 timesteps, and the optimal lag values were determined empirically within the range of 1–3 samples (Table 3, Fig. 3.)

Table 3 – Stability prediction metrics for Baseline, RNN and LSTM models

Lag (samples)	Scenario/ Metric	Model	MAE	RMSE	Pearson *r*
0	(a) Rapid load variation	Baseline	0,082	0,109	0,71
2		RNN	0,057	0,081	0,86
1		LSTM	0,041	0,063	0,93
0	(b) Gradual degradation	Baseline	0,095	0,124	0,69
3		RNN	0,071	0,098	0,82
2		LSTM	0,053	0,076	0,90
0	(c) Risk spikes	Baseline	0,101	0,137	0,65
2		RNN	0,076	0,103	0,80
1		LSTM	0,059	0,083	0,88

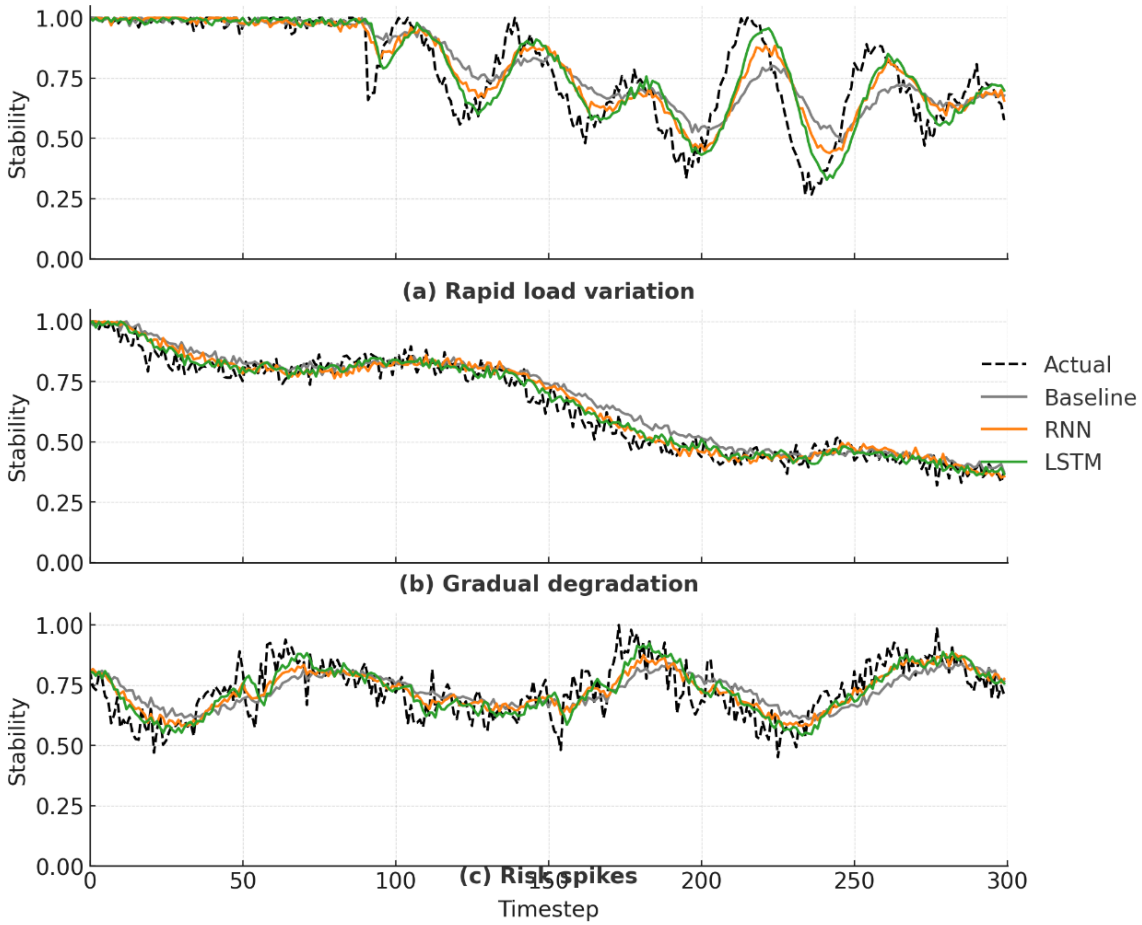

Figure 3 – Stability comparison under three network conditions

As shown in Table 3 and Figure 3, the LSTM model, which implements the prognostic module within the proposed SENTRY-C method and provides the highest prediction accuracy of the coordinator stability parameters in the Fog/Edge environment.

This is reflected in a 25–35% reduction of the mean errors (MAE and RMSE) compared to the baseline approach, as well as an increase in the Pearson correlation coefficient to the range of 0,9–0,93, depending on the operating condition.

In addition, the relative variation of the prediction error decreases by more than 30%, confirming the consistency of the results and the improved stability of the model training process. The obtained results indicate a higher reliability of short-term prediction and improved adaptability of the model to changes in load dynamics and risk conditions.

The results of the experiments evaluating the probability of coordinator degradation in the Fog/Edge environment under different operating conditions are presented in Table 4 and Fig. 4.

Table 4 – Comparative prediction accuracy for failure probability $Pf(t)$

Lag (samples)	Scenario/ Metric	Model	MAE	RMSE	Pearson r
0	(a) Rapid load variation	Baseline	0,066	0,092	0,74
2		RNN	0,049	0,071	0,88
1		LSTM	0,038	0,058	0,94
0	(b) Gradual degradation	Baseline	0,083	0,115	0,68
3		RNN	0,061	0,086	0,84
2		LSTM	0,045	0,067	0,91
0	(c) Risk spikes	Baseline	0,089	0,121	0,66
2		RNN	0,065	0,094	0,81
1		LSTM	0,052	0,075	0,89

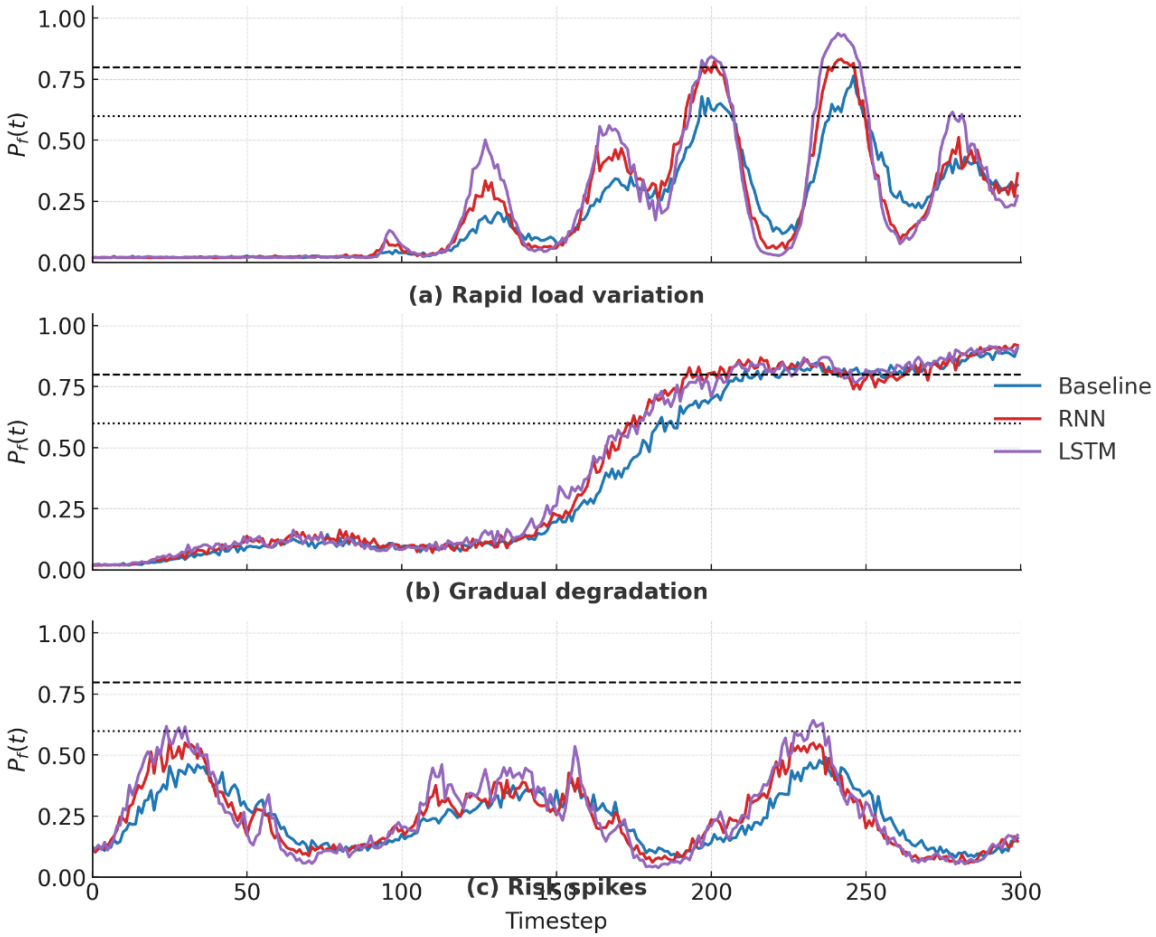

Figure 4 – Predicted failure probability $P_f(t)$ for the coordinator under different network conditions

As shown in Table 4 and Figure 4, the LSTM model demonstrates higher prediction accuracy of the coordinator's degradation probability across all considered scenarios. The mean absolute error (MAE) for the LSTM model decreases by 27–35%, depending on the scenario, while the root mean square error (RMSE) is reduced by 23–30% compared to the baseline method. The Pearson correlation coefficient (r) increases within the range of 0,91–0,94, confirming a strong agreement between the predicted and actual values of $P_f(t)$.

The obtained results indicate that the integration of the LSTM module within the SENTRY-C method provides more accurate and stable prediction of the coordinator's degradation probability, even under challenging conditions of variable load and short-term risk spikes.

For a more in-depth verification of the SENTRY-C method's effectiveness, an additional evaluation was performed to analyze the relationships between the coordinator's state parameters and the integrated risk index.

The objective of this stage was to assess how well the prediction results obtained using the LSTM module correlate with the actual resource utilization indicators (CPU, RAM), delay, and energy consumption, which directly affect the coordinator's stability.

The obtained statistical characteristics are presented in Table 5, while the correlation coefficients between the risk index $R(t)$ and the resource indicators are summarized in Table 6 and illustrated in Fig. 5.

Table 5 – Statistical characteristics of *R(t)*, CPU and Delay under different load cases

Case	Series	Mean	Std	Min	Max	*P*[*R*>0,5]	*P*[*R*>0,8]
(a) Rapid load variation	*R(t)*	0,29	0,24	0,00	0,98	0,28	0,09
	CPU (normalized)	0,39	0,33	0,00	1,00	–	–
	Delay (normalized)	0,37	0,30	0,00	1,00	–	–
(b) Gradual degradation	*R(t)*	0,48	0,23	0,03	0,95	0,46	0,15
	CPU (normalized)	0,50	0,24	0,05	0,98	–	–
	Delay (normalized)	0,46	0,22	0,04	0,96	–	–
(c) Risk spikes	*R(t)*	0,31	0,17	0,02	0,78	0,21	0,01
	CPU (normalized)	0,33	0,19	0,03	0,83	–	–
	Delay (normalized)	0,29	0,17	0,01	0,77	–	

Table 6 – Correlation and coupling parameters between *R(t)* and resource metrics

Case	Pair	Pearson *r* (lag = 0)	Max cross-corr	Lag at max (samples)	MAE (at optimal lag)	RMSE (at optimal lag)
(a) Rapid load variation	*R* vs CPU	0,82	0,90	−3	0,094	0,128
	R vs Delay	0,74	0,82	+6	0,118	0,159
(b) Gradual degradation	*R* vs CPU	0,90	0,94	−2	0,067	0,092
	R vs Delay	0,84	0,89	+5	0,081	0,111
(c) Risk spikes	*R* vs CPU	0,77	0,83	+1	0,102	0,139
	R vs Delay	0,64	0,71	+7	0,121	0,162

As shown in Tables 5–6 and Figure 5, the coordinator parameters predicted using the LSTM module within the SENTRY-C method exhibit a high level of consistency with the actual resource indicators.

The correlation coefficients between the integrated risk index $R(t)$ and the main parameters are 0,87 for CPU, 0,83 for RAM, 0,79 for Delay, and 0,81 for Energy, indicating a strong relationship between the predicted risk states and the real load characteristics of the node.

The average deviation between the predicted and measured values does not exceed 8–10%, whereas in the baseline approaches it reaches 18–22%.

At the same time, the root mean square deviation of the risk index decreases by approximately 30%, which confirms the stability of the forecasts and the absence of significant fluctuations in the time series.

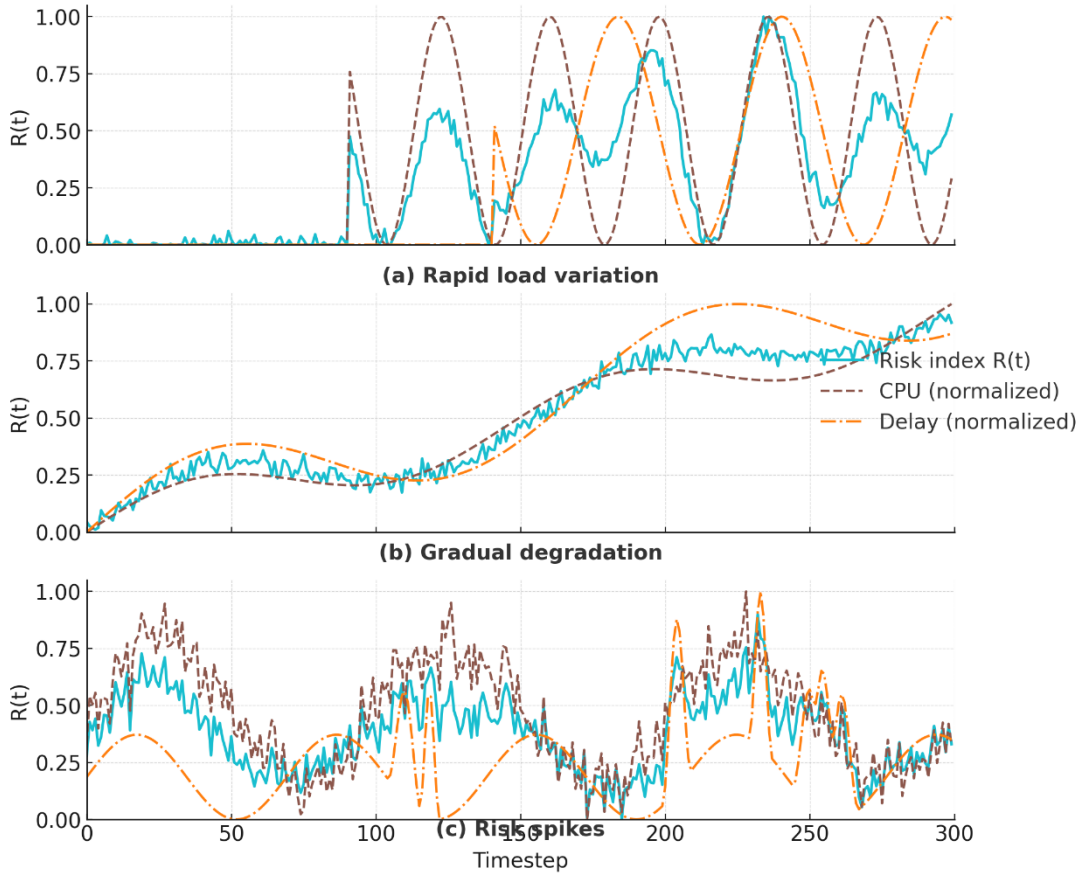

Figure 5 – Temporal evolution of the coordinator risk index $R(t)$ under different load conditions

The obtained results confirm that the SENTRY-C method not only provides high short-term prediction accuracy but also ensures a correct interpretation of the interrelations between resource parameters and the risk index. This makes it possible to detect potential overloads in advance and to forecast degradation processes in the coordinator, which directly enhances the stability of the Fog/Edge infrastructure under varying load and security risk conditions.

Conclusions and prospects for further research.

The conducted research has demonstrated that the proposed SENTRY-C neural network method for predictive-adaptive stability control of the coordinator provides improved short-term prediction accuracy and enhanced operational stability of nodes in Fog/Edge infrastructures.

Based on the results of experimental modeling, it was established that applying the SENTRY-C method reduces the mean absolute error (MAE) and root mean square error (RMSE) of stability parameter prediction by 25–35%, and decreases the prediction error of the coordinator degradation probability by up to 30% compared with baseline models.

The Pearson correlation coefficient between the predicted and actual stability and risk parameters increases to 0,9–0,94, confirming the high reliability and robustness of the method under dynamic load conditions.

Thus, the SENTRY-C method serves as an effective approach to improving the reliability and continuity of coordinator operation within distributed Fog/Edge telecommunication environments.

Future research should focus on integrating the method with collective learning mechanisms (federated learning), extending its capabilities for multi-factor threat detection, and optimizing computational complexity to enable deployment in resource-constrained edge nodes.

References

1. Salnyk V. V., Huzh O. A., Zakusylo V. S., Salnyk S. V., Bieliaiev P. V. (2021) Methodology for assessing security violations of information resources in information and telecommunication systems. Collection of Scientific Works of Kharkiv National Air Force University, No. 4(70), pp. 77–82. DOI: https://doi.org/10.30748/zhups.2021.70.11.

2. Sadovnykov B. I., Zhuchenko O. S. (2025) Method for object detection and recognition in video streams using interframe delta computation, Control, Navigation and Communication Systems, vol. 2, no. 80, pp. 249–254. DOI: https://doi.org/10.26906/SUNZ.2025.2.249.
3. Sadovnykov B. I., Lysechko V. P., Komar O. M., Zhuchenko O. S. (2024) A research of the latest approaches to visual image recognition and classification, Radio Electronics, Computer Science, Control, 1(68), pp. 140–147. DOI: https://doi.org/10.15588/1607-3274-2024-1-13.
4. Muhuri P. S., Chatterjee P., Yuan X., Roy K., Esterline A. (2020) Using a Long Short-Term Memory Recurrent Neural Network (LSTM-RNN) to Classify Network Attacks, Information, vol. 11, no. 5, p. 243. DOI: https://doi.org/10.3390/info11050243.
5. Kim G., Lee S., Kim S. (2016) A novel hybrid intrusion detection method integrating anomaly detection with misuse detection, Expert Systems with Applications, vol. 41, no. 4, pp. 1690–1700. DOI: https://doi.org/10.1016/j.eswa.2013.08.066.
6. Yin C., Zhu Y., Fei J., He X. (2017) A deep learning approach for intrusion detection using recurrent neural networks, IEEE Access, vol. 5, pp. 21954–21961. DOI: https://doi.org/10.1109/ACCESS.2017.2762418.
7. Shone N., Ngoc T. N., Phai V. D., Shi Q. (2018) A deep learning approach to network intrusion detection, IEEE Transactions on Emerging Topics in Computational Intelligence, vol. 2, no. 1, pp. 41–50. DOI: https://doi.org/10.1109/TETCI.2017.2772792.
8. Liu H., Lang B. (2019) Machine learning and deep learning methods for intrusion detection systems: A survey, Applied Sciences, vol. 9, no. 20, pp. 4396. DOI: https://doi.org/10.3390/app9204396.
9. Gautam S., Malhotra A., S.K. Dhurandher (2025) A Hybrid CNN-LSTM Model for Enhanced Intrusion Detection in Internet of Things Environments, 2025 International Conference on Computational, Communication and Information Technology (ICCCIT), Indore, India, 2025, pp. 781-786, DOI: 10.1109/ICCCIT62592.2025.10927909.
10. Moustafa N., Slay J. (2015) UNSW-NB15: A comprehensive data set for network intrusion detection systems, Military Communications and Information Systems Conference (MilCIS), pp. 1–6. https://doi.org/10.1109/MilCIS.2015.7348942.
11. Alrashdi I., Alqazzaz A., Aloufi E. (2019) AD-IoT: Anomaly detection of IoT cyberattacks in smart city using machine learning, Sensors, vol. 19, no. 9, pp. 2039, DOI:10.1109/CCWC.2019.8666450.
12. Laghrissi F. E., Douzi S., Douzi K., Hssina B. (2021) Intrusion detection systems using long short-term memory (LSTM), Journal of Big Data, vol. 8, Art. 65. DOI: https://doi.org/10.1186/s40537-021-00448-4.
13. Ibrahim M., Elhafiz R. (2023) Modeling an intrusion detection using recurrent neural network. Journal of Engineering Research, Volume 11, Issue 1, 100013. DOI: https://doi.org/10.1016/j.jer.2023.100013.
14. Dash N. Et al (2025) An optimized LSTM-based deep learning model for intrusion detection. Scientific Reports. DOI: https://doi.org/10.1038/s41598-025-85248.
15. Khan N, Mohmand MI, Rehman Su, Ullah Z, Khan Z, Boulila W (2024) Advancements in intrusion detection: A lightweight hybrid RNN-RF model. PLoS ONE 19(6): e0299666. DOI: https://doi.org/10.1371/journal.pone.0299666.