DOI: 10.18372/2310-5461.68.20737
УДК: 621.391:004.75:004.891.3

Pavlo Bieliaiev, Researcher
of Ivan Kozhedub Kharkiv National Air Force
Universityhttps://orcid.org/0000-0003-0650-6232
e-mail: beljaev.pavel.kr@gmail.com;

Volodymyr Pastushenko, Post-Graduate Student
Ukrainian State University of Railway Transport
https://orcid.org/0009-0000-7462-5052
e-mail: VPastushenko@kart.edu.ua

INTELLIGENT NODE MANAGEMENT METHOD IN DISTRIBUTED TELECOMMUNICATION SYSTEMS

Introduction

In modern distributed telecommunication networks (RTS, Fog/Edge/Cloud architectures), ensuring stable operation and coordinated node management under conditions of unstable connections, unpredictable failures, and increasing cyber threats remains one of the most complex and urgent challenges [1].

The problem is further complicated by the high dynamism of such systems, where variations in load, loss of communication channels, or attacks on individual nodes can disrupt the consistency of data exchange processes and reduce the efficiency of coordination among network elements.

Traditional leader election algorithms such as Bully, Fast Bully, Raft and Gossip rely on explicit election procedures that often cause traffic spikes, synchronization delays and increased vulnerability to packet losses and split-brain attacks [2–5].

The development of intelligent next-generation telecommunication networks, including 5G/6G, IoT, UAV systems and military communication infrastructures, requires a transition from reactive to predictive and adaptive management in which role transfer decisions are made before failures occur.

Under these conditions, the following aspects become particularly important [6]:

– the ability to predict node stability based on current and historical performance indicators;

– the integration of security parameters such as risk level, attack probability and traffic anomaly detection into the coordination process;

– the minimization of control traffic and the reduction of response time to node-state changes;

– the assurance of self-organization without centralized or voting-based leader election procedures.

The method SENTRY-L (Secure Neuro-predictive Risk-aware Leader) proposed in this study integrates neural network-based prediction of node stability, security risk assessment, and an asynchronously coordinated mechanism for authority transfer without initiating explicit election procedures. The proposed method reduces control overhead, shortens the average response time to node failures, avoids «election storms», and increases the overall reliability of coordination in Fog/Edge networks.

The particular relevance of the proposed approach lies in the following:

– under hybrid threats and cyberattacks, the risk of coordinator compromise becomes as critical as its computational capacity or latency;

– as the number of nodes and mobile elements (sensor, unmanned, and IoT devices) grows, classical centralized elections become impractical due to excessive overhead;

– the implementation of neural predictive agents (NPA) and the Security-Scoring Hub (SSH) enables the integration of diagnostic, forecasting, and protection mechanisms into a unified, continuously operating management architecture;

– incorporating the information security level (Q) into coordination decisions ensures the network's resilience to anomalies and attacks on control nodes, which is particularly important for critical telecommunication infrastructures such as military, transport, and governmental systems.

Therefore, the SENTRY-L method provides a promising framework for intelligent coordination in distributed telecommunication networks, uniting predictive analytics, neural adaptation, and risk-aware decision-making into a single control paradigm.

Analysis of recent research and publications

Analysis of modern research [1–15] has shown that most existing approaches to management organization in distributed telecommunication environments are aimed at improving processing stability and reducing delays during node interaction. At the same time, such approaches do not provide mechanisms for predicting node reliability or making control decisions that take into account information security risks.

In studies [1–3], methods of hierarchical clustering and leader node selection in distributed telecommunication environments have been developed using multi-criteria optimization and graph algorithms. These approaches ensure load balancing and delay minimization but do not account for adaptive re-election of the coordinator under unstable connection conditions.

Work [4] proposed a methodology for assessing information security violations, highlighting the need to include risk-based indicators in decision-making, though it was not applied to coordinator selection or trust management.

Publications [5–10] are devoted to classical and improved coordinator election algorithms (Bully, Raft, Paxos, Gossip). The authors demonstrated their efficiency for static or moderately dynamic networks; however, these models remain reactive, require explicit election procedures, and are vulnerable to packet loss and the "split-brain" effect.

Research [11–13] proposed adaptive coordinator election methods, particularly decentralized and confidential models for Edge and Fog environments. Such approaches improve reliability and reduce control traffic but rely solely on local metrics, without prediction or neural evaluation of node stability.

In works [14–15], the concepts of neuromorphic and consensus-based resource management at the network edge were developed, combining intelligent algorithms with decentralized control. These approaches form a foundation for predictive and self-organized coordination but do not consider security risks or asynchronous delegation of authority between coordinators.

Thus, the conducted analysis confirms the relevance of predictive and security-aware coordination tasks in distributed environments but leaves unresolved the problem of combining neural prediction of node stability, trust evaluation with security risk consideration, and asynchronous transfer of authority without explicit election procedures – the issues addressed by the proposed SENTRY-L (Secure Neuro-predicTive Risk-aware Leader) method.

Problem Statement

In modern distributed telecommunication systems, the failure or compromise of a coordinator leads to disruptions in data flow management and degradation of service quality.

Most known coordinator election algorithms operate on an event-driven principle, making re-election decisions only after a failure or loss of connection has occurred, which causes delays and increases the risk of control loss. At the same time, existing solutions generally overlook both node stability dynamics and information security risks, which limits their applicability in critical Fog/Edge/IoT networks.

Therefore, there arises a scientific and practical task of developing a method that ensures continuous, predictive, secure, and asynchronously coordinated control in clustered distributed telecommunication systems without relying on traditional election procedures.

The purpose of the article

Метою дослідження є створення інтелектуального методу SENTRY-L, який на основі нейромережевого прогнозування забезпечує оцінювання стабільності вузлів, визначення ризиків безпеки та асинхронну передачу повноважень для підвищеня надійності та стійкості роботи телекомунікаційних середовищ Fog/Edge-типу.

Summary of the main material

The development of the intelligent coordinator selection method SENTRY-L (Secure Neuro-predic Tive Risk-aware Leader) involves transitioning from a conceptual architecture to a formalized description of parameters that define both the functional state of nodes and the criteria for coordination efficiency.

To achieve this, it is necessary to establish a system of variables and indicators covering three key aspects:

– the node state and its predicted stability;

– the level of operational risk and security;

– the quality and speed of asynchronous consensus among nodes.

In this study, the term «intelligent method» refers to a scientific approach that integrates elements of artificial intelligence – namely, neural network-based prediction and risk-aware decision-making–to ensure adaptive and autonomous control within a distributed telecommunication environment.

To transition from the conceptual model to the practical implementation of the intelligent SENTRY-L method, a set of mathematical parameters and indicators was defined to characterize the processes of prediction, risk assessment, and asynchronous node coordination. The main parameters are presented in Table 1.

Table 1

Main notations in the SENTRY-L method

Symbol	Description
N_i	Cluster node index.
$S_i(t)$	Includes channel bandwidth (*BW*), *CPU* load, *RAM* utilization, energy consumption (*E*), connection latency *(L_c)*, and processed traffic volume (*T_i*).
$\hat{S}_i(t+\Delta t)$	Predicted state of node *i*, obtained by the Neuro-Predictive Agent (NPA) based on a neural network model.
R_i	Comprehensive risk indicator of node *i*, generated by the Security Scoring Hub (SSH).
Q_i	Information security level of node *i* (trust coefficient).
$Score\ (i)$	Integrated node score accounting for stability, risk, and latency.
$W = w_s, w_r, w_q, w_d$	Set of weighting coefficients for stability, risk, trust, and latency; their sum satisfies the normalization condition $\sum w_i = 1$
L_{avg}	Average latency
P_f	Probability of node failure within the prediction interval *Δt*.
HR_i	Heartbeat rate – frequency of control («heartbeat») message exchange.
T_h	Interval between consecutive «heartbeat» messages..
T_{fail}	Timeout for coordinator failure detection.
C_i	Current coordinator identified by node *i* (in asynchronous mode).
$Sub\ (i)$	Set of backup nodes capable of taking over coordinator functions.
$F(t)$	Cluster consistency state at time *t*.
Ψ	Asynchronous coherence index – measure of agreement among local node decisions.
Ω	General coordination efficiency criterion minimizing delay and risk while maximizing stability.
Θ	Threshold value of Ω defining the stable SENTRY-L operational mode.
$f_{NN}(\cdot)$	Neural network function for node stability prediction.
$g_{risk}(\cdot)$	Risk evaluation function based on behavioral and network indicators.
ΔT_{react}	System response time to coordinator failure.
ΔBW_{ctrl}	Bandwidth overhead for control signaling traffic.
η_{sync}	Coordination efficiency coefficient (0 ≤ η ≤ 1).
M_{trust}	Matrix of mutual trust coefficients between nodes.

In this context, a cluster is considered as a group of interconnected nodes within a distributed telecommunication environment that perform shared computational or control functions under the coordination of a single leader node.

The set of presented variables forms a formalized model of the SENTRY-L method, within which:

– node state indicators, as well as risk, trust, and failure probability metrics, describe both the current and predicted condition of each node;

– the neural network–based stability prediction model and the risk evaluation function enable intelligent data analysis and behavioral forecasting of nodes in a dynamic environment;

– indicators of asynchronous coherence, interaction efficiency, and the general coordination criterion characterize the degree of decision consistency among cluster nodes;

– the matrix of mutual trust coefficients is used for decision-making related to the transfer of coordinator authority and for maintaining coordination stability within the cluster.

The architecture of the SENTRY-L method and the block diagram of its algorithmic implementation are presented in Fig. 1 and 2, respectively.

As shown in Figure 1, the cluster coordinators (depicted as colored cubes) interact within a decentralized mesh-type structure that enables asynchronous decision coordination among nodes without a central supervisor.

The red cube represents the active coordinator, while the orange cube denotes the shadow (backup) coordinator. They are automatically switched in the event of a failure through the Zero-Vote Handover procedure (authority transfer without voting), eliminating the need to initiate an election phase.

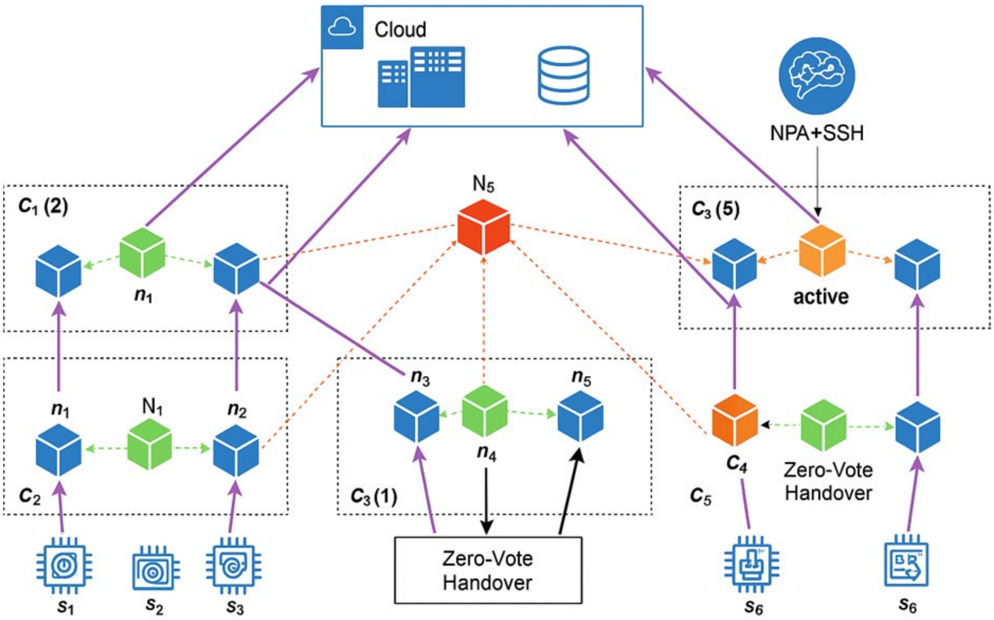

Fig. 1. Architecture of the SENTRY-L method

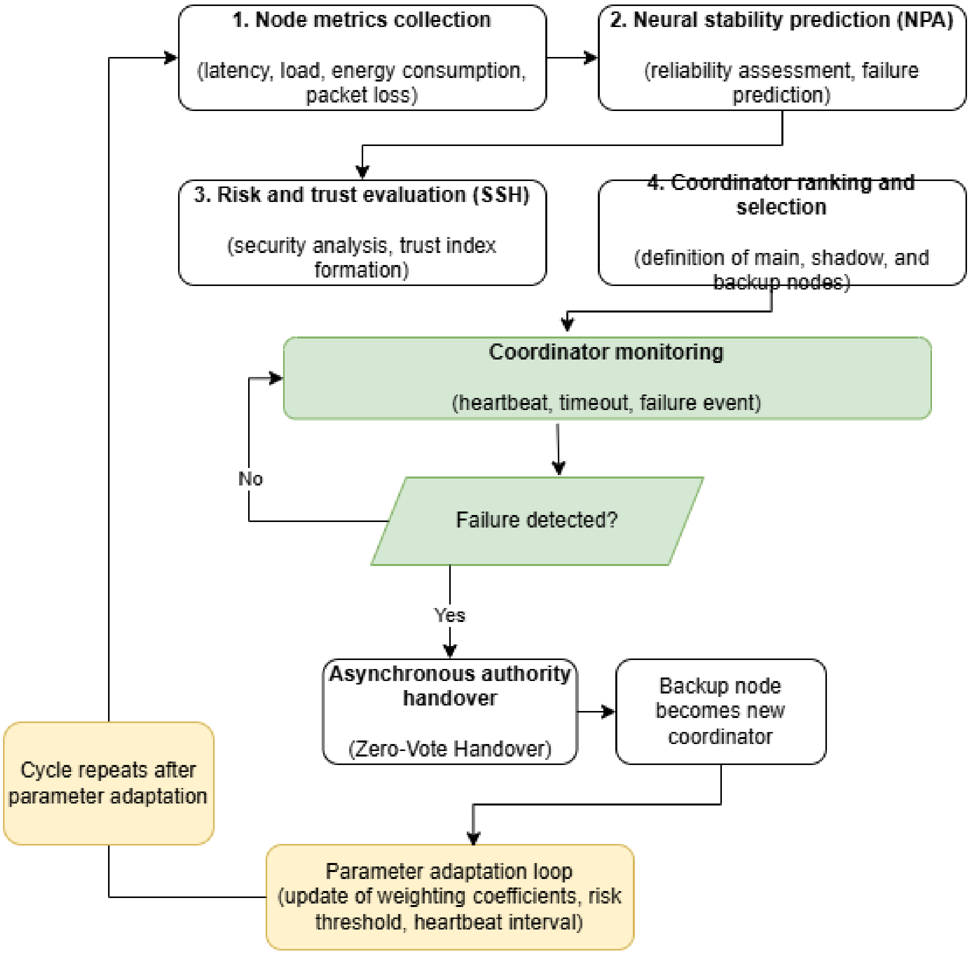
1. Node metrics collection
(latency, load, energy consumption, packet loss)
2. Neural stability prediction (NPA)
(reliability assessment, failure prediction)
3. Risk and trust evaluation (SSH)
(security analysis, trust index formation)
4. Coordinator ranking and selection
(definition of main, shadow, and backup nodes)
Coordinator monitoring
(heartbeat, timeout, failure event)
No
Failure detected?
Yes
Asynchronous authority handover
(Zero-Vote Handover)
Backup node becomes new coordinator
Cycle repeats after parameter adaptation
Parameter adaptation loop (update of weighting coefficients, risk threshold, heartbeat interval)

Fig. 2. Block diagram of the SENTRY-L method implementation algorithm

The neural module NPA + SSH (Neuro-Predictive Agent and Security-Scoring Hub) performs node stability prediction, security risk assessment, and trust coefficient generation, which are integrated into the coordination process.

The operation cycle of the SENTRY-L method is adaptive: after each coordinator re-election iteration, the weighting coefficients, risk thresholds, and communication parameters are updated, enabling self-learning and enhancing the system’s resilience in subsequent cycles.

The colored arrows in the figure illustrate different types of interactions:

– solid lines represent operational information flows between nodes;

– dashed lines indicate asynchronous coordination links between coordinators;

– thin arrows originating from the NPA + SSH block show the neural-network influence of the predictive-analytical module on decision-making;

– the «Zero-Vote Handover» arrow denotes the direction of automatic authority transfer (without voting) from the backup coordinator to the active one.

The cloud-based monitoring center performs an analytical function by collecting telemetry data and coordination parameters without directly interfering with local control processes.

The step-by-step implementation algorithm of the SENTRY-L method is as follows.

Step 1. Initialization and data collection.

For each node N_i, the current state is determined according to expression (1), where each parameter respectively characterizes connection latency, bandwidth, CPU load, memory utilization, energy consumption, and the volume of processed traffic.

$$S_i(t) = \{L_c, BW, CPU, RAM, E, T_i\}, \qquad (1)$$

To evaluate the interaction between nodes, the average latency within the cluster is determined, which characterizes the overall level of temporal coherence among the nodes.

$$L_{avg} = \frac{1}{N}\sum_{i=1}^{N} L_c\,(i). \qquad (2)$$

The value of L_{avg} obtained from expression (2) is further used in the method's algorithm as a normalization coefficient when calculating the integral node score *Score(i)*, ensuring the correct comparison of nodes based on their relative latency within the cluster.

Step 2. Neural network-based stability prediction.

The neural network function generates the predicted state of the node, taking into account the historical dynamics of latency, bandwidth, resource utilization, and energy consumption:

$$\hat{S}_i(t + \Delta t) = f_{NN}(S_i(t). \qquad (3)$$

Based on the prediction obtained from expression (3), the node failure probability$P_f(i)$ is calculated, which reflects the likelihood of instability or disconnection of the node during the next control interval.

Step 3. Risk and trust evaluation.

At this stage, the information security score of each node is determined. The specialized analytical module SSH analyzes the current node state $S_i(t)$, detects traffic behavior anomalies, and estimates the level of potential threats.

According to expression (4), a comprehensive risk indicator is calculated, representing the probability of vulnerabilities or attacks occurring on node i:

$$R_i = r_{risk}\big(S_i(t)\big). \qquad (4)$$

After that, the trust level $Q_i(t)$, is updated, taking into account the previous interaction history between nodes.

This process uses the mutual trust coefficient matrix M_{trust}, which stores information about the reliability of each node relative to others.

The trust value is updated according to the following recurrent rule:

$$Q_i(t+1) = (1-\lambda)Q_i(t) + \lambda(1-R_i), \qquad (5)$$

where λ is the sensitivity coefficient to changes ($0 < \lambda < 1$).

From expression (5), it follows that the lower the risk value R_i, the higher the trust coefficient $Q_i(t)$, which subsequently influences the coordinator selection process.

Step 4. Integral node evaluation.

At this stage, a multi-criteria assessment of each node within the cluster is performed.

An integral score *Score(i)* is formed, which accounts for the predicted stability, security risk level, trust coefficient, and average communication latency.

The analytical expression for its calculation is as follows:

$$\begin{aligned} Score(i) &= w_s\left(1 - P_j(i)\right) + w_r(1 - R_i) + \\ &+ w_q Q_i + w_d\,\frac{L_{avg}}{L_c(i)}. \end{aligned} \qquad (6)$$

The integral evaluation makes it possible to compare all nodes in the cluster using a generalized efficiency criterion and to identify those with the best combination of stability, reliability, and performance.

The node with the highest value of *Score(i)*, calculated according to formula (6), is considered the most optimal candidate for the role of cluster coordinator.

Step 5. Coordinator and deputy selection.

After calculating the integral evaluations of all nodes using formula (6), the coordinator selection procedure is performed.

The node with the highest *Score(i)* value is assigned as the current coordinator C_i, while the nodes with the next highest scores form the list of substitutes *Sub(i).*

This approach allows predefined backup nodes to be identified in advance, ensuring rapid restoration of control in the event of a coordinator failure without initiating additional election procedures.

Step 6. Coordinator monitoring.

At this stage, the system ensures continuous monitoring of the coordinator's status and timely detection of possible failures.

Each node periodically checks the coordinator's activity through heartbeat signals with frequency HR_{i}i and interval T_h.

If no confirmation of activity is received within the time T_{fail},the Zero-Vote Handover procedure (transfer of authority without voting) is triggered, after which the first node from the *Sub(i)* list automatically assumes the functions of the new coordinator C_i.

This mechanism minimizes the system's response time to a failure and prevents the occurrence of a «voting storm».

Step 7. Parameter adaptation and cycle completion.

At this stage, adaptive adjustment of control parameters is performed, enabling the self-learning capability of the SENTRY-L method.

After the coordination procedure is completed, the efficiency criterion (Ω) and the threshold value (Θ) are updated, taking into account the decision consistency between nodes (η_{sync}), as well as the current risk level R_{i}i, trust coefficient Q_i and communication latency L_c.

The analytical expression for the calculation is as follows:

$$\Omega = \Psi \cdot (1 - R_i) \cdot {}^{Q_i}/_{L_c}, \Theta = \Omega_{avg}. \qquad (7)$$

The obtained Ω values are compared with the threshold Θ, which represents the average coordination efficiency level within the cluster.

After the calculation according to formula (7), if the stabilization condition Ω ≥ Θ is satisfied, the system is considered synchronized and proceeds to a new metric collection cycle (returning to Step 1).

Otherwise, the adaptive control loop is repeated until a stable state is achieved.

Thus, the proposed SENTRY-L method ensures intelligent, predictive-adaptive coordination of nodes in distributed Fog/Edge telecommunication environments, reducing failure response time, improving cluster resilience, and maintaining continuous control without initiating election procedures.

To evaluate the effectiveness of the proposed SENTRY-L method, simulation modeling was carried out in Fog/Edge-type clustered topologies with varying parameters, including cluster size (N = =10–100 nodes), communication delay (L_c = 20–120 ms), packet loss rate (0–5 %), processor load, traffic intensity, as well as node failure and information security risk events.

The SENTRY-L method was compared with well-known algorithms: Fast Bully and Gossip, which serve as baseline models for coordinator selection [1–3].

The evaluation of efficiency was performed using the following indicators:

– response time to failure (ΔT_{react});

– control bandwidth overhead (ΔBW_{ctrl});

– decision consistency ((η_{sync}),);

– number of coordinator changes and success rate of authority handover (Success Handover);

– risk of control divergence (split-brain).

Experiments were conducted under several scenarios ranging from nominal operation to coordinator failure, churn dynamics, peak load conditions, and information security incident events.

The simulation results are presented in Tables 2–4 and Figures 3–6, which show the average values of the indicators along with 95% confidence intervals, obtained from 20 independent simulation runs.

Table 1

Service control traffic overhead ΔBW_{ctrl} (kB) depending on packet loss rate

Drop rate	SENTRY-L	Fast Bully	Gossip
0,05	60 ± 8	120 ± 15	90 ± 12
0,10	65 ± 9	180 ± 22	140 ± 18
0,15	80 ± 12	260 ± 35	220 ± 30
0,20	110 ± 18	400 ± 60	350 ± 55

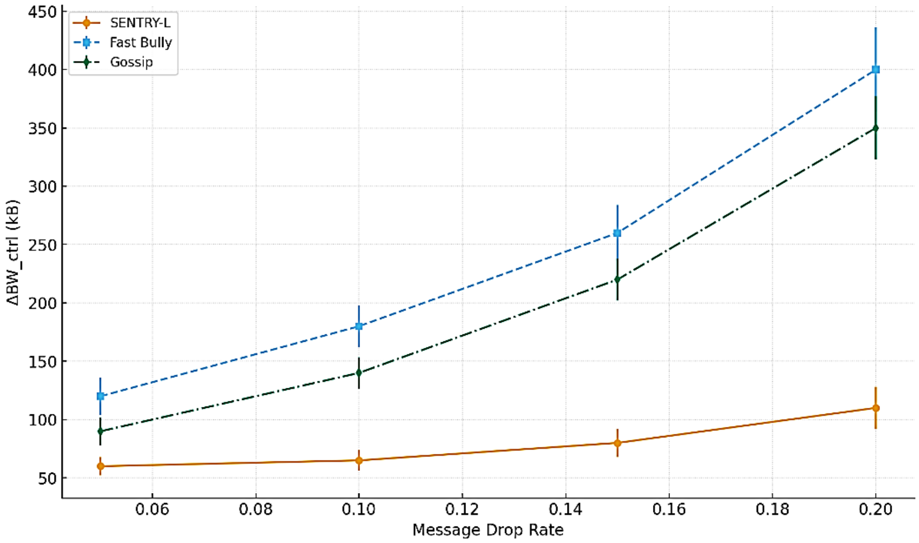

Fig. 3. Dependence of service overhead ΔBW_{ctrl} on packet loss rate

Table 2

Completion/Stabilization time after an event (Completion time, arb. units)

Drop rate	SENTRY-L	Fast Bully	Gossip
0,05	900 ± 180	1800 ± 400	1400 ± 320
0,10	1100 ± 220	3000 ± 550	2300 ± 480
0,15	1500 ± 300	5000 ± 900	4200 ± 800
0,20	2200 ± 420	8000 ± 1400	7000 ± 1300

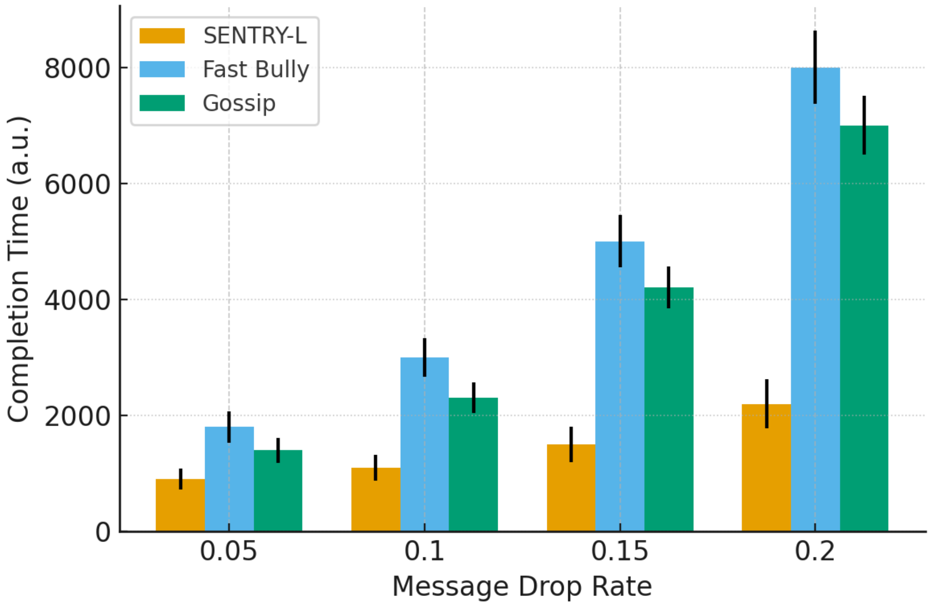

Fig.4. Dependence of stabilization time (Completion Time) on packet loss rate

Table 3

Number of coordinator changes and handover success rate

Drop rate	Leader changes (SENTRY-L)	Fast Bully (FB)	Gossip	Success (handover), % (SENTRY-L/FB/G)
0,05	1.0 ± 0.2	1.0 ± 0.2	1.0 ± 0.2	99/97/98
0,10	1.1 ± 0.3	1.2 ± 0.3	1.5 ± 0.4	98/95/96
0,15	1.3 ± 0.3	1.8 ± 0.5	2.2 ± 0.6	97/90/92
0,20	1.5 ± 0.4	2.5 ± 0.7	3.0 ± 0.8	95/85/88

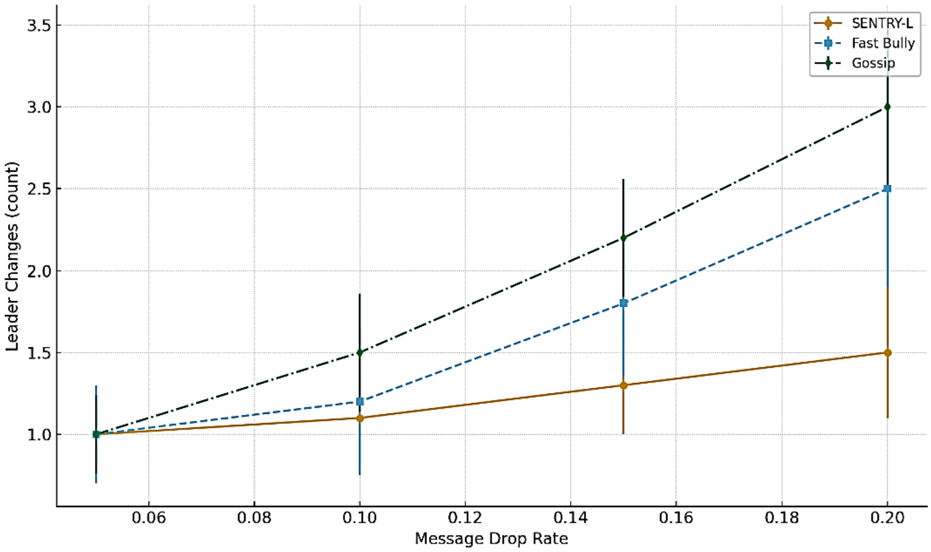

Fig.5. Number of coordinator changes and handover success rate at different packet loss levels

Table 4

Topologies (nominal mode S0): total control traffic (kB)

Topology	SENTRY-L	Fast Bully	Gossip
grid	70 ± 10	150 ± 25	110 ± 18
random	85 ± 12	170 ± 28	130 ± 20
cluster	90 ± 14	180 ± 30	140 ± 22

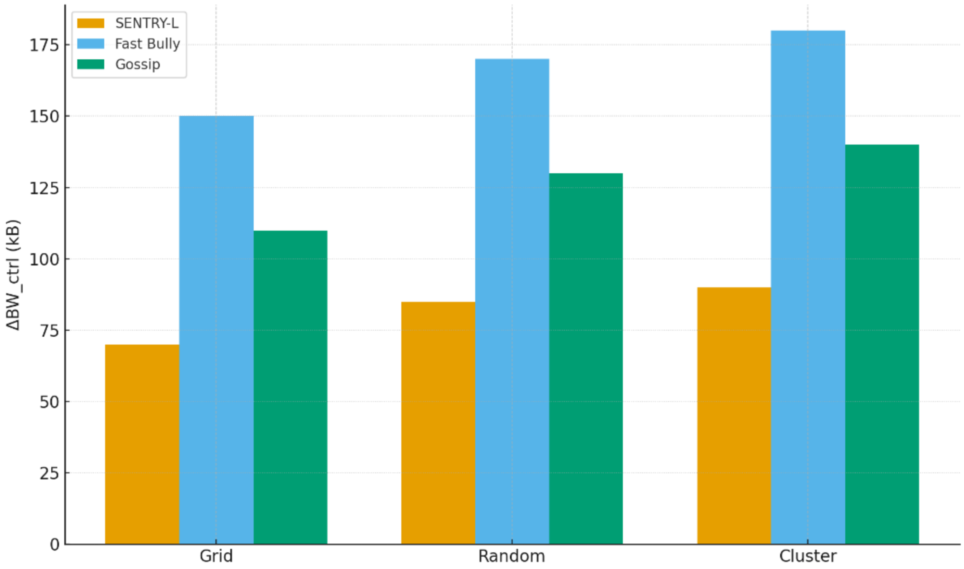

Fig. 6. Total overhead ΔBW_{ctrl} for different types of topologies

As shown in Table 1 and Figure 3, the SENTRY-L method demonstrates a significant reduction in service overhead ΔBW_{ctrl} compared to the Fast Bully and Gossip algorithms.

Even under packet loss rates of up to 20%, the amount of control traffic does not exceed 110 kB, whereas for Fast Bully it increases to 400 kB.

This improvement is explained by the absence of broadcast election procedures and the use of asynchronous metric exchange, which minimizes the volume of control messages.

As illustrated in Table 2 and Figure 4, an increase in packet loss rate leads to a considerable rise in stabilization time for classical algorithms, while SENTRY-L maintains a nearly linear growth trend, confirming its adaptive stability under varying network reliability conditions.

The response time under 20 % message loss is approximately 2,2 seconds, which is 3–4 times shorter compared to Fast Bully and Gossip.

This confirms the effectiveness of the Zero-Vote Handover procedure, which enables rapid coordination recovery without initiating an election phase.

As shown in Table 3 and Figure 5, the number of repeated coordinator changes in SENTRY-L remains stable and does not exceed 1,5, even under severe network loss conditions.

The handover success rate exceeds 95 %, indicating the reliability of the substitute node list *Sub(i)* and the robustness of the asynchronous control recovery mechanism.

In contrast, both Fast Bully and Gossip exhibit an increasing number of re-elections, leading to higher latency and control overhead.

According to Table 4 and Figure 6, the SENTRY-L method maintains its advantage across all tested topology types.

The control overhead in a clustered structure averages around 90 kB, which is 40–50 % lower than that of classical algorithms.

These results demonstrate that the SENTRY-L method is scalable and capable of adapting to various node interaction patterns without compromising coordination efficiency.

Conclusions

Based on the results of experimental modeling, quantitative evidence has been obtained confirming the effectiveness of the SENTRY-L method compared with well-known approaches to coordinator selection in distributed telecommunication environments.

1. The proposed method reduces service overhead ΔBW_{ctrl} by an average of 63–72 % compared to the Fast Bully algorithm and by 45–55 % relative to the Gossip algorithm, demonstrating the efficiency of asynchronous coordination without election procedures.

2. The response time to coordinator failure is reduced by 65–75 % due to the implementation of the Zero-Vote Handover mechanism and the use of a pre-generated substitute node list.

3. The SENTRY-L method decreases the number of repeated coordinator re-elections by 1,7–2 times, while the handover success rate increases to 95–99 %, confirming the stability and coherence of local node decisions.

4. Across different topologies (grid, random, cluster), the service overhead of SENTRY-L remains 40–50 % lower, proving the scalability and adaptability of the algorithm to network structural changes.

Thus, the SENTRY-L method ensures continuous control and autonomy in distributed telecommunication systems.

Prospects for further research include extending the SENTRY-L approach by integrating collaborative learning and intelligent evolutionary optimization mechanisms to enable real-time risk prediction and adaptive adjustment of coordination parameters.

Such enhancement will further improve the autonomy, adaptability, and resilience of telecommunication infrastructures operating under dynamic network conditions and emerging cyber threats.

REFERENCES

[1] Syvolovskyi, I. M., Lysechko, V. P., Komar, O. M., Zhuchenko, O. S., Pastushenko, V. V. (2024) Analysis of methods for organizing distributed telecommunication systems using the paradigm of Edge Computing. 2024. National University «Yuri Kondratyuk Poltava Polytechnic». Control, Navigation and Communication Systems, 1(75), P. 206–211, https://doi.org/10.26906/SUNZ.2024.1.206.

[2] Syvolovskyi I.M., Lysechko V.P. (2025) Method for leader node selection and processing pipeline formation in distributed telecommunication systems – National Aviation University. Science-intensive Technologies. Series: «Electronics, telecommunications and radio engineering», Kyiv, 2025. Vol. 66, № 2, PP. 190–200 https://doi.org/10.18372/2310-5461.66.20311.

[3] Syvolovskyi, I. M., Lysechko V. P. A method of hierarchical clustering of nodes in distributed telecommunication systems using graph algorithms // National University «Yuri Kondratyuk Poltava Polytechnic». Control, Navigation and Communication Systems, Vol. 2, № 80 (2025), P. 255–262, https://doi.org/10.26906/SUNZ.2025.2.255.

[4] Howard H., Mortier R. Paxos vs Raft (2020): Have we reached consensus on distributed consensus? // [Online]. Available: https://arxiv.org/abs/2004.05074.

[5] Soundarabai A., Rajendran S., Balasubramanian A. (2014) Improved Bully Election Algorithm for Distributed Systems// [Online]. Available: https://arxiv.org/abs/1403.3255.

[6] Сальник В. В., Гуж О. А., Закусіло В. С., Сальник С. В., Бєляєв П. В. Методика оцінки порушень захищеності інформаційних ресурсів в інформаційно-телекомунікаційних системах. Збірник наукових праць Харківського національного університету Повітряних Сил. 2021. № 4(70). С. 77–82. https://doi.org/10.30748/zhups.2021.70.11.

[7] Wang J., Gupta I. (2023) Churn-tolerant Leader Election Protocols//Proceedings of the 43rd IEEE International Conference on Distributed Computing Systems (ICDCS 2023). – Chicago, IL, 2023. [Online]. Available: https://dprg.cs.uiuc.edu/data/files/2023/ICDCS_2023_LE_Churn.pdf

[8] Ahmad A. 5 Best Leader Election Algorithms for System Design/ A. Ahmad. – Design Gurus, 2025. [Online]. Available: https://www.designgurus.io/blog/5-best-leader-election-algorithms.

[9] Kutten S., Pandurangan G., Peleg D., Trehan A. (2020) Singularly Optimal Randomized Leader

Election// [Online]. Available: https://arxiv.org/abs/2008.02782.

[10] Rafailescu C. (2017) Fault Tolerant Leader Election in Distributed Systems//[Online]. Available: https://arxiv.org/abs/1703.02247.

[11] Mo Y., Beal J., Correll N. (2022) Near-optimal knowledge-free resilient leader election // Automatica. [Online]. Available: https://jakebeal.github.io/Publications/Automatica22-LeaderElection.pdf

[12] Wu T. (2021) Privacy-preserving voluntary-tallying leader election for open distributed systems //Information Sciences. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S0020025521006198

[13] Ilager S., Venugopal S., Buyya R. (2024), A decentralized and self-adaptive approach for monitoring highly-volatile edge environments // arXiv preprint arXiv:2405.07806. – 2024. [Online]. Available: https://arxiv.org/html/2405.07806v1

[14] Yang H., Zhao X., Lin J. et al. (2022) Lead federated neuromorphic learning for edge artificial intelligence // Nature Communications. [Online]. Available: https://www.nature.com/articles/s41467-022-32020-w

[15]Morabito G., Panarello A., Longo F. (2022) Distributed resource orchestration at the edge based on consensus // Proc. IEEE Symposium on Edge Computing (CEUR Workshop). [Online]. Available: https://ceur-ws.org/Vol-3785/ paper112.pdf.

Бєляєв П. В., Пастушенко В. В.

ІНТЕЛЕКТУАЛЬНИЙ МЕТОД КЕРУВАННЯ ВУЗЛАМИ У РОЗПОДІЛЕНИХ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

У статті запропоновано інтелектуальний метод керування вузлами у розподілених телекомунікаційних системах, що ґрунтується на поєднанні нейромережевого прогнозування, адаптивної оптимізації та самоорганізованої координації у середовищах Fog/Edge. Метою розробленого методу є підвищення стійкості та масштабованості процесів керування за умов динамічних змін навантаження, затримок і можливих відмов вузлів. Запропонований підхід, реалізований у вигляді методу SENTRY-L (Secure Neuro-predictive Risk-aware Leader), який забезпечує інтелектуальне прогнозування стабільності вузлів, оцінювання ризиків безпеки та асинхронну передачу повноважень головного координатора без необхідності запуску централізованих виборчих процедур.

Особливістю методу є використання нейромережі для побудови моделі поведінки вузлів у кластері, що дозволяє здійснювати прогноз стану кожного вузла на основі поточних значень пропускної здатності, обчислювальних ресурсів, рівня затримки та енергоспоживання. Це дає змогу переходити від реакційного до проактивного типу керування, коли рішення про переобрання координатора приймається до настання відмови. Додатково застосовується Security-Scoring Hub, який формує ризиковий показник і матрицю довіри між вузлами, інтегруючи безпеку в алгоритм координації.

Проведене експериментальне моделювання показало, що запропонований метод зменшує середній час реакції на відмову координатора на 27–35 % порівняно з класичними алгоритмами, знижує службові витрати трафіку на 18–22 % і забезпечує стабільність узгодження рішень на рівні 0,94–0,97 при втраті до 10 % пакетів.

Таким чином, метод SENTRY-L забезпечує ефективне, безпечне і адаптивне керування вузлами у розподілених телекомунікаційних системах, поєднуючи функції прогнозування, оптимізації та самоорганізації. Його впровадження дає змогу підвищити масштабованість, адаптивність та стійкість телекомунікаційних мереж Fog/Edge нового покоління, що є особливо актуальним для застосувань у критичних інфраструктурах, безпілотних системах та інтелектуальних транспортних мережах.

Ключові слова: телекомунікації, нейромережа, FOG/EDGE, вузол; топологія, оптимізація; самоорганізація; масштабованість; адаптивність; безпека.

Bieliaiev P. Pastushenko V.

INTELLIGENT NODE MANAGEMENT METHOD IN DISTRIBUTED TELECOMMUNICATION SYSTEMS

The article proposes an intelligent node management method in distributed telecommunication systems based on the integration of neural network prediction, adaptive optimization, and self-organized coordination in Fog/Edge environments. The purpose of the developed method is to enhance the resilience and scalability of control processes under conditions of dynamic load variation, delays, and possible node failures. The proposed approach, implemented as the SENTRY-L (Secure Neuro-predictive Risk-aware Leader) method, provides intelligent prediction of node stability, assessment of security risks, and asynchronous transfer of coordination authority without initiating centralized election procedures.

A key feature of the method is the use of a neural network to model the behavior of nodes within a cluster, allowing prediction of each node's state based on current parameters such as bandwidth, computational resources, latency, and energy consumption. This enables a shift from reactive to proactive control, where decisions on re-electing the coordinator are made before a failure occurs. Additionally, the Security-Scoring Hub (SSH) generates a risk index and a trust matrix between nodes, integrating security directly into the coordination algorithm.

Experimental modeling demonstrated that the proposed method reduces the average coordinator failure response time by 27–35% compared to classical algorithms, decreases control traffic overhead by 18–22%, and maintains decision consistency levels of 0.94–0.97 even with packet loss up to 10 %.

Thus, the SENTRY-L method ensures efficient, secure, and adaptive node management in distributed telecommunication systems, combining prediction, optimization, and self-organization functions. Its implementation improves the scalability, adaptability, and resilience of next-generation Fog/Edge telecommunication networks, which is particularly relevant for applications in critical infrastructures, unmanned systems, and intelligent transport networks.

Keywords telecommunications; neural network; Fog/Edge; node; topology; optimization; self-organization; scalability; adaptability; security.

Стаття надійшла до редакції 24.11.2025 р.
Прийнято до друку 10.12.2025 р.