https://doi.org/10.31891/2219-9365-2026-86-12
UDC 004.056:530.145:004.032.26

FESENKO Tatiana
National University «Yuri Kondratyuk Poltava Polytechnic»
https://orcid.org/0009-0006-1698-3795
e-mail: tanifesenko@gmail.com
MAGALETSKA Vladyslava
Limited Liability Company Private Higher Education Institution «University of Modern Technologies»
https://orcid.org/0009-0000-5562-699X
e-mail: vlarut@gmail.com
RUBIN Eduard
Limited Liability Company Private Higher Education Institution «University of Modern Technologies»
https://orcid.org/0009-0005-4447-4413
e-mail: edw.rubin@gmail.com

PROTECTION AND RESILIENCE MODEL FOR QUANTUM REPEATERS

Modern quantum networks necessitate high levels of reliability and data security. Quantum repeaters are pivotal for enabling network scalability and maintaining quantum state coherence over significant distances. Simultaneously, repeaters represent critical network nodes that may be vulnerable to physical noise, technical malfunctions, and node-level cyberattacks. Consequently, there is an urgent need to develop systemic models capable of assessing the resilience of repeaters and ensuring their protection within scalable quantum network architectures.

This paper proposes a mathematical-cybernetic model for the protection and resilience of quantum repeaters. The model incorporates physical processes, noise effects, and potential cyber threats, integrating static approaches for vulnerability assessment with dynamic-adaptive mechanisms for automated response to external influences. Furthermore, it is highlighted that contemporary hybrid models synergize quantum algorithms with classical security protocols. This integration enables a systematic evaluation of the trade-off between computational fidelity, resource efficiency, and attack resilience.

The analyzed objective functions facilitate the quantitative assessment of protection mechanism effectiveness and quantum repeater resilience across various operational scenarios, including active interference and infrastructure scaling. The study introduces systemic criteria for evaluating node reliability and cybersecurity, representing a critical component for the integration and operation of quantum communication technologies.

The findings establish a methodological framework for enhancing cyber defense strategies in quantum networks, with a primary focus on bolstering the resilience of critical infrastructure components. The proposed model optimizes repeater protection mechanisms within scalable network topologies and provides an analytical foundation for investigating adaptive control algorithms. This ensures reliable transmission and the seamless integration of quantum communications into next-generation systems.

Keywords: quantum repeaters, resilience, cybersecurity, adaptive models, scalable quantum networks, secure communications.

ФЕСЕНКО Тетяна
Національний університет «Полтавська політехніка імені Юрія Кондратюка»
МАГАЛЕЦЬКА Владислава, РУБІН Едуард
ТОВ ПВНЗ «Університет сучасних технологій»

МОДЕЛЬ ЗАХИСТУ ТА СТІЙКОСТІ КВАНТОВИХ ПОВТОРЮВАЧІВ

Сучасні квантові мережі потребують високого рівня надійності та захисту передавання інформації. Квантові повторювачі виконують ключову роль у забезпеченні масштабованості мереж та підтримці когерентності квантових станів на великих відстанях. Водночас повторювачі є критичною точкою мережі і можуть бути вразливими до фізичних шумових впливів, технічних несправностей і кібератак на вузловому рівні. Це створює потребу у розробці системних моделей, здатних оцінювати стійкість повторювачів та забезпечувати їх захист у масштабованих квантових мережах.

У статті запропоновано математично-кібернетичну модель захисту і стійкості квантових повторювачів. Модель враховує фізичні процеси, шумові впливи та можливі кіберзагрози. Вона включає статичні підходи для оцінки вразливостей та динамічно-адаптивні для автоматичного реагування на зовнішні впливи. Зазначається, що сучасні гібридні моделі поєднують квантові алгоритми з класичними протоколами безпеки. Саме поєднання таких підходів забезпечує систематичну оцінку компромісу між точністю обчислень, ефективністю використання ресурсів та стійкістю до атак.

Розглянуті цільові функції дозволяють кількісно оцінювати ефективність механізмів захисту та стійкість квантових повторювачів у різних сценаріях експлуатації, включаючи активні втручання та масштабування мережевої інфраструктури. У статті запропоновано системні критерії оцінки надійності та кібербезпеки вузлів, що є визначальною складовою для інтеграції та функціонування технологій квантового зв'язку.

Отримані результати формують методологічну основу для вдосконалення стратегій кіберзахисту квантових мереж із фокусом на підвищення стійкості критичних компонентів інфраструктури. Запропонована модель забезпечує оптимізацію механізмів захисту повторювачів у масштабованих мережевих топологіях та створює аналітичне підґрунтя для дослідження адаптивних алгоритмів керування, що гарантує надійну передачу та інтеграцію квантових комунікацій у системах наступного покоління

Ключові слова: квантові повторювачі, стійкість, кібербезпека, адаптивні моделі, масштабовані квантові мережі, захищені комунікації.

ISSN 2219-9365

Стаття надійшла до редакції / Received 30.03.2026
Прийнята до друку / Accepted 28.04.2026
Опубліковано / Published 31.05.2026

PROBLEM STATEMENT

Despite significant efforts in the development, experimental implementation, and standardization of quantum technologies including Quantum Key Distribution (QKD) protocols and other information security mechanisms – next-generation quantum networks remain far from fully secure practical operation.

Quantum repeaters, which are essential for overcoming channel distance limitations and supporting long-range quantum communication, remain largely experimental or only partially implemented, facing numerous technological constraints. Laboratory and simulation studies demonstrate that the security of repeaters and network topologies in real-world conditions is significantly more complex than predicted by classical theoretical models. Specifically, an adversary's control over even a fraction of the nodes can substantially degrade the resilience and reliability of the entire network, even in the presence of secure segments [1].

In practical quantum communication implementations, modified QKD protocols and other security strategies are applied, which depend heavily on physical implementation and hardware architecture. This creates additional points of vulnerability due to hardware defects, physical interventions, and implementation errors that can diminish quantum state coherence and repeater resilience. Recent reviews confirm that threats to networks arise not only from the cryptographic strength of protocols but also from physical, hardware, and software aspects of quantum device implementation, including repeaters, photonic detectors, and control software [2].

The scientific and applied problem lies in the fact that existing protection and resilience assessment models fail to comprehensively account for the multidimensional factors of real-world environments. These factors include partial and temporal interventions at individual nodes, noise processes, hardware defects, and adaptive attacks on control protocols. There is a lack of harmonized mathematical and cybernetic approaches for the quantitative assessment of risks during the scaling of quantum networks and the transition from laboratory prototypes to practical infrastructures.

Addressing this problem is a fundamental task for enhancing the resilience and cybersecurity of quantum communications. In this context, the development of models that integrate the physical implementation of repeaters, dynamic threats, and adaptive control allows for risk assessment, prediction of system behavior during attacks, and the ensuring of reliable operation for scalable topologies.

Consequently, within the scope of this study, three key scientific questions have been identified:

1. Critical attack types for nodes and repeaters, including physical interventions, hardware defects, instability of quantum state sources, and modifications to control software.
2. Modeling of adaptive and resilient protection strategies, accounting for non-linear quantum dynamics, dissipative effects, feedback loops, and the application of variational quantum algorithms and quantum neural networks.
3. Efficiency and reliability criteria, such as quantum state fidelity, success probability of transmission, resistance to physical and cyber interventions, and resource efficiency.

Resolving these questions forms the methodological basis for developing adaptive strategies that ensure the resilient, reliable, and cyber-secure operation of next-generation scalable quantum networks.

ANALYSIS OF THE LATEST RESEARCH

Analysis of recent scientific publications indicates an active development of both theoretical and practical aspects of quantum network security and quantum repeaters as key components for scalable systems. Specifically, in 2024-2025, several works were published focusing on vulnerability analysis and methods for enhancing network resilience. One such study provides a detailed security analysis of partially compromised repeater networks, considering a scenario where an adversary controls only a subset of nodes while part of the topology at the initial subscriber level remains relatively secure. Practical simulation results suggest that under conditions of partial compromise and controlled noise, it is possible to achieve improved performance and noise tolerance, whereas full compromise scenarios are characterized by significant degradation of network operational parameters [1].

Another example is research analyzing the resilience of quantum networks to targeted attacks. The authors proposed two heuristic routing strategies aimed at reducing fidelity loss. The first strategy is based on optimal route selection, while the second involves the application of entanglement purification procedures. Simulation results showed that the combination of re-routing and local fidelity enhancement mitigates the negative impact of attacks on network performance. At the same time, trade-offs were identified between reliability indicators, resource costs, and the efficiency of quantum resource utilization in real-world network topologies [3].

Alongside resilience models, contemporary scientific works propose adaptive approaches to optimizing quantum network performance, such as using deep neural networks to achieve an optimal balance between latency and throughput. Such hybrid approaches are becoming vital for the practical implementation of high-performance quantum communication systems, as classical routing methods are insufficiently effective for networks with high state variability and noise influences [4].

Reviews in the field of quantum cryptography also note a trend toward strengthening the role of quantum repeaters as critical security nodes and identify open challenges regarding effective security proofs and practical operational models in large-scale networks. One such review highlights the need to improve QKD security models, enhance repeater support, and integrate with post-quantum cryptographic schemes, which resonates with the issues of developing resilient protocols for real-world networks [5].

Furthermore, research project initiatives aimed at transitioning from laboratory testing to outdoor testbeds open opportunities for assessing quantum repeater behavior under real operational conditions. This direction of development confirms the importance of interdisciplinary approaches that combine theoretical models, simulations, and practical experiments when scaling quantum networks for commercial or critical infrastructure scenarios [6].

Thus, the analysis of recent research and publications shows a transition from classical theoretical security models to practically oriented approaches involving cyberattacks on topologies, adaptive routing, machine learning, and comprehensive risk assessment. However, a number of issues related to comprehensive resilience assessment, security guarantees, and the practical implementation of adaptive protocols in scalable networks with repeaters remains open.

FORMULATION OF THE GOALS OF THE ARTICLE

The aim of this article is to analyze critical types of attacks on nodes and quantum repeaters, to develop mathematical models of adaptive and resilient protection strategies that account for non-linear quantum dynamics, and to establish a system of criteria for the quantitative assessment of efficiency, reliability, and resource efficiency in the functioning of scalable quantum networks.

PRESENTING THE MAIN MATERIAL

By systematizing the existing categories of threats that significantly impact the functioning of nodes and quantum repeaters in scalable quantum networks, it should be noted that the analysis is based on contemporary reviews, experimental studies, and technical recommendations from leading international research organizations. These include the National Institute of Standards and Technology (NIST) and the UK's Quantum Communications Hub. These institutions place particular emphasis on the practical challenges of implementing quantum channels and repeaters, including the physical, hardware, and software aspects that form the foundation for developing effective resilience and cyber defense models for quantum networks in real-world environments [7].

Based on this analysis, the primary types of attacks posing critical threats to nodes and repeaters can be identified. These include physical interventions, hardware defects, the instability of quantum state sources, and modifications to control software. Further examination of these categories enables the systematization of risks, the assessment of their impact on network resilience, and the establishment of a methodological framework for developing adaptive and resilient protection strategies.

First – **physical attacks and interventions.** Physical manipulations of hardware and transmission channels pose direct threats to the integrity of quantum states. Known instances of attacks on practical quantum communication systems include the use of fake signals or high-intensity light pulses, which can lead to incorrect measurements or channel eavesdropping. Such attacks have been experimentally demonstrated in classical BB84 QKD systems, where detector vulnerabilities allowed for the modeling of external states and the degradation of security [8].

Second – **hardware defects and technical flaws.** The hardware implementation of photon sources, photon detectors, and quantum memory represents one of the primary points of vulnerability. The instability of quantum state sources or low detector efficiency significantly impacts the probability of successful transmission and overall network reliability. Analysis in review [2] indicates that such defects are often overlooked in existing theoretical models, yet they exert a substantial influence on real-world network topologies.

Third – **software and control attacks.** Attacks at the software level involve the modification of control protocols for nodes and repeaters. Proper configuration of adaptive algorithms and routing parameters is critical for maintaining network resilience [9]; their compromise can lead to disruptions in the sequence of quantum state transmission or an inadequate response to fluctuations in load and emerging threats.

Fourth – **combined threats and network attack vectors.** The most sophisticated attack scenarios involve the simultaneous exploitation of physical, hardware, and software vectors, necessitating comprehensive threat models and risk assessments. Contemporary reviews emphasize the need to consider such multi-factor attacks, as they can significantly diminish the effectiveness of existing protection mechanisms and require highly flexible adaptive protocols [7].

Table 1 below provides a comparative-analytical summary of critical attack types for nodes and quantum repeaters in scalable networks.

Analysis of the table reveals that physical and hardware attacks exert the most significant impact on network resilience, while software threats amplify their consequences, creating combined risks. Consequently, the presented systematization allows for the identification of protection priorities and underscores the necessity of implementing adaptive strategies capable of predicting system behavior and responding to multi-level threats in scalable quantum networks.

Another aspect of the study focuses on the mathematical modeling of adaptive protection strategies that ensure the effective operation of quantum repeaters in scalable networks. The foundation of such modeling is a generalized mathematical model that accounts for the non-linear dynamics of the repeater's state, control feedback loops, and the integration of resilience to external perturbations and attacks. Non-linear dynamics allow for considering the dependence of state evolution on previous measurements and internal interactions [10], while feedback ensures the automatic adjustment of repeater parameters in response to changing operational conditions and potential threats.

Table 1

Comparative analysis of critical attack types on quantum nodes and repeaters

Attack type	Impact mechanism	Impact on the node	Impact on the repeater	Criticality level
Physical	Unauthorized access to optical lines, manipulation of the transmission medium	Disruption of quantum state stability and degradation of local protocol performance	Degradation of coherence and repeater efficiency	High
Hardware	Photon detector instability, source parameter fluctuations	Escalating error probabilities, degradation of state processing	Erratic repeater operation, throughput degradation	High
Software	Modification of routing and error correction algorithms, disruption of state processing	Improper node management, reduced transmission reliability	Synchronization disruption, entanglement recovery failures	Medium
Combined	Integration of physical, hardware, and software factors	Cumulative reduction in node stability and reliability	Severe repeater impairment, systemic network degradation	High

Within this approach, three main types of models are distinguished:

1. Static models. Static models allow for the assessment of vulnerabilities and risks without considering changes in the repeater's state over time. Formally, the state of a node or repeater can be represented by a density operator $\rho_0 \in \mathrm{H}$, where H is the Hilbert space of the system. Vulnerabilities and risks are modeled through static quality functionals:

$$\mathrm{F}_s = f(\rho_0, E_{phys}, E_{soft}, \mathrm{C}_{crit}), \tag{1}$$

which enables the identification of the most vulnerable nodes and network segments.

Main Parameters [11]:

- Repeater state $\rho_0 \in \mathrm{H}$, which describes the initial quantum state.
- Hardware defects E_{phys}, accounting for the instability of quantum state sources and various noise factors.
- Software vulnerabilities E_{soft}, reflecting potential errors and flaws in the control software.
- Critical components C_{crit}, upon which the overall network operability and performance depend.

Thus, given the identified constraints, the transition to dynamic models is logically well-founded. These models facilitate the accounting of temporal state changes in quantum repeaters under the influence of external attacks – dynamics that cannot be adequately captured through static assessments alone.

2. Dynamic adaptive models. Dynamic models account for the temporal evolution of the repeater's state and enable parameter adaptation in response to attacks and external perturbations. The state evolution is described by the generalized Lindblad equation:

$$\frac{d\rho(\mathrm{t})}{dt} = -i\left[H_0 + H_c(t,\rho), \rho(t)\right] + \sum_k \mathrm{D}_k[\rho(t)], \tag{2}$$

where H_0 is the system's base Hamiltonian, $H_c(t,\rho)$ is the adaptive control Hamiltonian derived from intermediate measurements and risk assessment, and D_k denotes the dissipative superoperators that model the influence of external attacks and noise.

The feedback loop is defined as:

$$H_c(t,\rho) = \mathcal{G}(\rho(t),\ R\ (t)), \tag{3}$$

where $R\ (t)$ represents the risk indicators derived from intermediate measurements. The primary evaluation criteria include state coherence, successful transmission probability, resilience to attacks, and recovery time following interventions [12].

In this context, the expediency of employing hybrid models is driven by the need to integrate quantum algorithms with classical protocols to ensure enhanced resilience and efficiency across complex network topologies.

3. Hybrid Models. Hybrid models integrate quantum algorithms with classical security protocols. The repeater's state is parameterized by a vector of variational parameters $\theta(t)$, which governs quantum neural networks

and variational algorithms:

$$\rho(t) = U(\boldsymbol{\theta}(t))\rho_0 U^{\dagger}(\boldsymbol{\theta}(t)), \tag{4}$$

where $U(\boldsymbol{\theta}(t))$ is the unitary adaptive control operator. Simultaneously, classical protocols provide local state purification and rerouting to minimize coherence loss.

The performance metrics include coherence, the probability of successful transmission, resource utilization efficiency, and resilience to complex physical and cyber attacks [13]. In summary, it can be noted that through the integration of quantum and classical mechanisms, **hybrid models** provide the highest level of adaptive resilience in scalable networks.

Table 2 presents the results of a comparative analysis of the three protection and resilience models for quantum repeaters.

Table 2

Comparative analysis of potection and resilience models for quantum repeaters

Model	Parameters	Criteria	Attacks	Adaptation / Advantages
Static	fixed parameters	coherence	physical, hardware, software	None / simple implementation, quick analysis
Dynamic-adaptive	feedback, dissipative processes	coherence	physical, software, adaptive	Yes / coherence support, reacts to attacks
Hybrid	integration of quantum algorithms and classical protocols	coherence	complex: physical, hardware, software	Yes / high resilience, resource optimization, comprehensive risk assessment

Consequently, modeling based on non-linear quantum dynamics, dissipative processes, and adaptive control via variational quantum algorithms and quantum neural networks forms the foundation for developing resilient and efficient security protocols. These protocols are capable of ensuring the reliable operation of next-generation scalable quantum networks.

The adaptive control model for a quantum repeater in a scalable network is appropriately formalized as a multi-level block architecture (Figure 1).

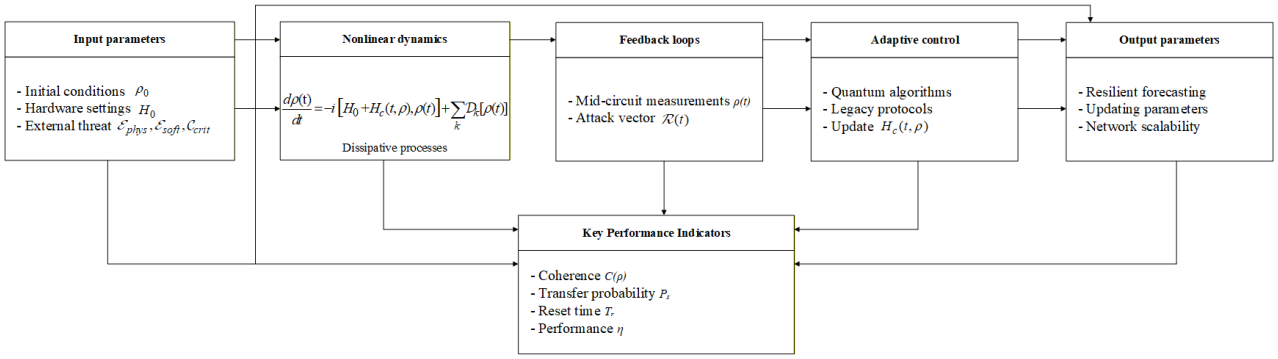

Fig. 1. Adaptive control of a quantum repeater

This architecture ensures coordinated interaction between the processes of measurement, state estimation, control decision-making, and parameter adaptation in the presence of dynamic perturbations and targeted attacks. In this formulation, each repeater is considered a controlled dynamical system, the state of which is described by a density matrix

$$\rho_i(t) \in \mathrm{S}(\mathrm{H}_i), \tag{5}$$

and its evolution is governed by a non-linear controlled Lindblad-type quantum equation

$$\frac{d\rho_i(\mathrm{t})}{dt} = -i\,[H_i(u_i(t)), \rho_i(t)] + \sum_k \mathrm{L}_{i,k}(\rho_i) + \sum_{j \in \mathrm{N}_i} \mathrm{C}_{ij}(\rho_i, \rho_j), \tag{6}$$

where $u_i(t)$ is the control input vector, and the terms C_{ij} represent the interaction with adjacent network repeaters.

Thus, the model input receives the measured parameters of the quantum states, which are formulated as an observation vector

$$y_i(t) = \left[\mathrm{C}(\rho_i), \mathrm{F}_i, N_i, \tau_i, \{\mathrm{F}_{ij}\}_{j \in \mathrm{N}_i}\right], \tag{7}$$

where $\mathrm{C}(\rho_i)$ is the coherence metric, F_i and F_{ij} represent local and inter-node fidelity, N_i is the noise level,

and τ_i denotes time delays. These signals form the primary information base for evaluating the repeater's dynamics, reflecting both internal quantum processes as well as external network operating conditions.

The state estimation module implements the reconstruction of the repeater's current operational mode based on quantum filtering and statistical reconstruction, formulated as an estimation operator

$$\hat{\rho}_i(t) = \mathrm{F}_i\left(y_i(t)\right), \tag{8}$$

followed by the calculation of entropic and information-theoretic characteristics

$$S(\rho_i) = -\mathrm{Tr}(\rho_i \log \rho_i), \quad \Delta\rho_i = \left\|\hat{\rho}_i - \rho_i^{\mathrm{ref}}\right\|. \tag{9}$$

The obtained estimates determine the deviations from the target parameters and serve as input data for the control loops.

The core element of the model is the adaptive control loop, within which control actions are formulated based on feedback according to the control law:

$$u_i(t) = \pi_i\left(\hat{\rho}_i(t), \hat{\theta}_i(t), R_i(t)\right), \tag{10}$$

where $\hat{\theta}_i(t)$ is the estimate of perturbation and attack parameters, and $R_i(t)$ represents the generalized risk metric. Adaptation is implemented through the dynamic tuning of the Hamiltonian

$$H_i(u_i) = H_i^{(0)} + \sum_m u_{i,m} H_{i,m} \tag{11}$$

of variational quantum algorithm parameters and the weight coefficients of quantum neural networks, which are optimized to minimize the quality functional

$$J_i = \int_0^T \left(\alpha_1 S(\rho_i) + \alpha_2 R_i + \alpha_3 \| u_i \|^2\right) dt. \tag{12}$$

The risk prediction module is focused on evaluating the probability of successful attacks and the impact of external perturbations. The risk dynamics analysis for each repeater is described by the equation:

$$\dot{R}_i = f_i\left(\hat{\theta}_i(t), \rho_i(t), \{R_j(t)\}_{j\in \mathrm{N}_i}\right), \tag{13}$$

which allows for accounting for both local and network-wide degradation effects and the generation of scenarios for potential loss of coherence or entanglement.

Based on the state estimation and risk prediction results, the parameter adaptation module performs real-time updates of the repeater configuration according to the rule:

$$\Theta_i(t+1) = \Theta_i(t) + \Lambda_i \frac{\partial J_i}{\partial \Theta_i}, \tag{14}$$

where Θ_i encompasses parameters for routing, local entanglement processing, and fidelity recovery procedures. Such an approach ensures the coordinated adaptation of both local and network-level operational mechanisms.

Consequently, under the given conditions, the model's output signals include adjusted control parameters $u_i(t)$, updated system state estimates $\rho_i(t)$, and recommendations for the operation of network protocols. Collectively, they ensure the fulfillment of the resilience criterion for the scalable network.

$$\max_i \left(S(\rho_i), R_i\right) \le \varepsilon, \quad \mathrm{F} \ge \mathrm{F}, \tag{15}$$

thereby guaranteeing the stable operation of nodes, the maintenance of quantum state coherence, and the enhancement of the overall resilience of the quantum network in the face of dynamic threats and perturbations.

In describing the interaction logic between the model's elements, it should be emphasized that it is implemented as a consecutive and closed-loop circuit for information processing and decision-making. The starting point for the implementation of the proposed development is the results of quantum state measurements, which serve as the information foundation for the operation of the estimation modules. At this stage, an analysis of the repeater's current characteristics is performed, and a representation of its dynamic operational mode is formed. Subsequently, based on the obtained estimates, a risk analysis is conducted to quantify the impact of external perturbations and potential attacks, followed by the synthesis of updated control actions incorporating adaptive strategies. The cycle concludes with an efficiency forecasting stage, the results of which are fed back into the measurement loop, closing the process and ensuring continuous control.

Overall, the integration of non-linear dynamics into the model provides a foundation for a coordinated and physically grounded description of quantum state evolution under real-world operating conditions. This approach allows for tracking how external perturbations and targeted attacks are consistently integrated into the system's dynamics, ensuring the alignment of theoretical models with the practical operational modes of quantum repeaters within a network.

At the same time, feedback loops act as the key mechanism providing the system with adaptive properties. They ensure the prompt adjustment of parameters in response to state changes or the partial compromise of individual

nodes, allowing for the maintenance of quantum state coherence and sustaining network resilience even in the presence of local attacks and degradation processes.

In turn, the performance and reliability evaluation criteria serve as formalized indicators of the system's operational quality. Their application ensures the quantitative verification of quantum repeater resilience in scalable networks and establishes a unified methodological framework for comparing various control and protection modes. To quantitatively assess the efficiency and reliability of quantum repeaters in scalable networks, a set of interrelated indicators has been defined [14]. These indicators evaluate quantum state coherence, resilience to physical and cyber interventions, successful transmission probability, and resource utilization efficiency.

Within the framework of the adaptive control model for a quantum repeater, the assessment of system efficiency and reliability is conducted based on four key criteria: quantum state coherence $C(t)$, fidelity $F(t)$ and successful transmission probability $P_{\text{success}}(t)$, resilience to physical and cyber interventions $R(t)$, and resource utilization efficiency E_{res}.

1. Quantum state coherence. Quantum state coherence $C(t)$ reflects the system's capacity to preserve the phase information of quantum states over a duration t. It is defined as the ratio of the coherent part of the density matrix $\rho(t)$ to the initial state ρ_0:

$$C(t) = \text{Tr}[\rho_{\text{coh}}(t) \cdot \rho_0] / \text{Tr}[\rho_0^2], \tag{16}$$

where $\rho_{\text{coh}}(t)$ is the coherent component of the density matrix at time t, ρ_0 is the initial density operator of the quantum state, and $\text{Tr}[\cdot]$ denotes the matrix trace, ensuring normalization.

Assuming the initial state ρ_0 is a pure state, then $\text{Tr}[\rho_0^2] = 1$. After $1\,\mu$s, the coherent component is measured:

$$\text{Tr}[\rho_{\text{coh}}(1\,\mu\text{s}) \cdot \rho_0] = 0.92.$$

The coherence after $1\,\mu$s is then calculated as:

$$C(1\,\mu\text{s}) = \frac{0.92}{1} = 0.92.$$

This indicates that the system has retained 92% of its initial coherence, demonstrating a high level of stability for the quantum repeater over the specified time interval.

2. Fidelity and successful transmission probability. Fidelity $F(t)$ characterizes the accuracy of reproducing a target quantum state ρ_{target} after its transmission or processing through a repeater. It serves as the primary metric for assessing the reliability of information transfer and entanglement recovery (distillation).

$$F(t) = \left[\text{Tr}\sqrt{\sqrt{\rho_{\text{target}}}\,\rho(t)\sqrt{\rho_{\text{target}}}} \right]^2, \tag{17}$$

where $\rho(t)$ is the density matrix after transmission, and ρ_{target} is the target density operator.

Let ρ_{target} be a pure state. After passing through the repeater, the state $\rho(t)$ is obtained, for which:

$$\left[\text{Tr}\sqrt{\sqrt{\rho_{\text{target}}}\,\rho(t)\sqrt{\rho_{\text{target}}}} \right]^2 = 0.95. \tag{18}$$

Then:

$$F(t) = 0.95.$$

Thus, state recovery was achieved with 95% fidelity, demonstrating the effectiveness of the adaptive control.

3. Successful transmission probability. Successful transmission probability $P_{\text{success}}(t)$ determines the fraction of quantum states transmitted across the network without losses or errors:

$$P_{\text{success}} = \frac{N_{\text{success}}}{N_{\text{total}}}, \tag{19}$$

where N_{success} is the number of successfully transmitted states, and N_{total} is the total number of transmitted states.

For example, if 9,200 out of 10,000 states are successfully transmitted:

$$P_{\text{success}} = \frac{9200}{10000} = 0.92.$$

The obtained result corresponds to a 92% transmission success rate.

4. Resilience to physical and cyber interventions. Resilience $R(t)$ formalizes the repeater's capacity to

maintain its operational characteristics under the influence of adversarial attacks and environmental noise:

$$R = 1 - \frac{\Delta C + \Delta F + \Delta P}{3}, \tag{20}$$

where $\Delta C = 1 - C(t)$ is the loss of coherence, $\Delta F = 1 - F(t)$ is the loss of fidelity, and $\Delta P = 1 - P_{\text{success}}(t)$ is the probabilistic transmission loss.

Based on the previous calculations, we obtain:

$$\Delta C = 1 - 0.92 = 0.08, \quad \Delta F = 1 - 0.95 = 0.05, \quad \Delta P = 1 - 0.92 = 0.08.$$

Then

$$R = 1 - \frac{0.08 + 0.05 + 0.08}{3} = 1 - 0.07 = 0.93.$$

Thus, the resilience of the repeater to disturbances and attacks is 93 %.

5. Resource utilization efficiency. The efficiency E_{res} characterizes the ratio of effectively used resources to the total resources of the system:

$$E_{\text{res}} = \frac{R_{\text{useful}}}{R_{\text{total}}}, \tag{21}$$

where: R_{useful} – resources that ensured successful transmission and coherence maintenance; R_{total} – total resources of the repeater.

Therefore, if 88 out of 100 resource units are used effectively, then:

$$E_{\text{res}} = \frac{88}{100} = 0.88.$$

Thus, the resource utilization efficiency is 88%.

Collectively, the metrics defined above are formalized through the integral resilience indicator S_{total}, which serves as a quantitative basis for comparing different repeater configurations and adaptive strategies:

$$S_{\text{total}} = \alpha C(t) + \beta F(t) + \gamma R(t) + \delta E_{\text{res}} \tag{22}$$

where α, β, γ, δ – weighting coefficients (sum = 1) for each criterion, which allows adapting the evaluation to the specific characteristics of the network.

With equal weighting coefficients α, β, γ, δ = 0.2, we have:

$$S_{\text{total}} = 0.2(0.92 + 0.95 + 0.92 + 0.93 + 0.88) = 0.2 \cdot 4.6 = 0.92.$$

The integral resilience of the repeater stands at 92%, attesting to a high level of reliability and efficiency within a scalable network.

Overall, the obtained results confirm the viability of a systemic and formalized approach to analyzing the resilience of quantum repeaters in scalable quantum networks. The proposed model allows for the integration of physical, hardware, and software aspects of repeater operation into a unified mathematical framework, providing a consistent description of their dynamics under perturbations and targeted attacks.

The examined mathematical apparatus for adaptive control provides a quantitative assessment of quantum state degradation and enables the generation of real-time corrective control actions. Scaling the model to a network of $n repeaters represented as a graph structure confirms the possibility of coordinated management of both local and global network parameters [15].

The implemented system of evaluation criteria forms a unified quantitative foundation for analyzing the reliability and efficiency of various repeater configurations and adaptive protection strategies. The computational results demonstrate that the integral resilience metric allows for the comparison of alternative control modes and the making of informed decisions regarding network optimization.

In general, these findings establish a methodological foundation for developing adaptive and resilient quantum network architectures designed to operate under dynamic perturbations and partial compromises. Furthermore, the presented mathematical apparatus and quantitative evaluation criteria define future research directions in the field of scalable quantum communications and cyber-resilient quantum information systems.

CONCLUSIONS AND PROSPECTS FOR FURTHER RESEARCH

This research addresses an urgent scientific and practical challenge: enhancing the resilience and reliability of quantum repeaters in scalable quantum networks under dynamic physical and cyber threats. The findings carry both theoretical and practical significance, offering a foundation for designing next-generation quantum communication infrastructures.

It has been established that physical interventions, hardware defects, instability of quantum state sources, and the compromise of control software lead to the non-linear degradation of quantum state coherence C and fidelity

F. The study demonstrates that even partial adversarial control over a subset of nodes significantly reduces the overall network resilience, justifying the transition from local to systemic protection models.

The paper develops a mathematical model for adaptive quantum repeater control, formalizing it as a controlled non-linear quantum dynamic system with feedback. The model integrates measurement processes, state estimation, risk forecasting, and control parameter correction into a single closed-loop circuit. This approach is generalized to a network of n repeaters represented as a graph topology, allowing for the analysis of coordinated dynamics across local and global processes of quantum state degradation and recovery.

A system of quantitative criteria has been implemented to evaluate the efficiency and reliability of quantum repeaters. An integral resilience indicator is proposed, combining quantum state coherence, fidelity, successful transmission probability, resistance to physical and cyberattacks, and resource utilization efficiency. Numerical simulations confirm the suitability of these criteria for the comparative analysis of various control modes and network configurations.

The results confirm the viability of adaptive control protocols for ensuring the stable operation of quantum repeaters in real-world conditions and provide a methodological basis for designing scalable, cyber-resilient quantum networks.

Future research directions include adapting the developed model to heterogeneous quantum networks with diverse physical repeater realizations and conducting an in-depth analysis of the impact of combined physical and cyberattacks. Special emphasis will be placed on automating control processes through Machine Learning (ML) integration, enabling the synthesis of real-time adaptive strategies to enhance the operational efficiency of large-scale quantum networks.

References

1. Harkness, Adrian, Krawec, Walter O, & Wang, Bing. *Security of partially corrupted quantum repeater networks*. *Quantum Science and Technology*, *10* (1). URL: https://par.nsf.gov/biblio/10572623. https://doi.org/10.1088/2058-9565/ad7882.
2. A review of quantum communication and information networks with advanced cryptographic applications using machine learning, deep learning techniques / R. Ramya, P. Kumar, D. Dhanasekaran et al. *Franklin Open*. 2025. Vol. 10. Art. 100223. DOI: https://doi.org/10.1016/j.fraope.2025.100223
3. Resilience analysis of quantum network against targeted attacks: Recovery via rerouting and purification / H. S. D. Tunc, A. A. Bayleyegn, J. Notcker et al. *Optical Switching and Networking*. 2025. Vol. 57. Art. 100810. DOI: https://doi.org/10.1016/j.osn.2025.100810
4. Ni G., Ho L., & Claussen, H. Adaptive Optimization of Latency and Throughput with Fidelity Constraints in Quantum Networks Using Deep Neural Networks. 2025. *arXiv preprint arXiv:2505.12459*.
5. Akter M.S., Rodriguez-Cardenas J., Shahriar H., Cuzzocrea A., & Wu F. (2023, December). Quantum cryptography for enhanced network security: a comprehensive survey of research, developments, and future directions. In *2023 IEEE International Conference on Big Data (BigData)*. P. 5408-5417
6. Universität des Saarlandes. (2025, February 11). *Neues Verbundvorhaben forscht an Quantenrepeatern für sichere Quantennetzwerke der Zukunft* [Press release]. EurekAlert! URL: https://www.eurekalert.org/news-releases/1073217?language=german
7. National Institute of Standards and Technology. (n.d.). *Quantum communications and networks*. U.S. Department of Commerce. URL: https://www.nist.gov/programs-projects/quantum-communications-and-networks
8. Polyakov M. (2025, July 2). *Quantum encryption in orbit: How close are we to 100% hack protection?* Max Polyakov. URL: https://maxpolyakov.com/quantum-encryption-in-orbit-how-close-are-we-to-100-hack-protection/
9. Shyshatskyi, A. (Ed.). The development of management methods based on bio-inspired algorithms Information and control systems: modelling and optimizations: collective monograph. – Kharkiv: *TECHNOLOGY CENTER PC*. 2024. P. 35-69. DOI: http://doi.org/10.15587/978-617-8360-04-7
10. Zhyvylo, Y., & Kuchma, Y. Mathematical modeling of intellectual and cryptographic protection of authentication keys. *Collection "Information Technology and Security"*. 2025. Vol. 13(2), P. 162–177. DOI: https://doi.org/10.20535/2411-1031.2025.13.2.344591
11. Fesenko, T., & Kalashnikova, Y. Mathematical aspects of the combined application of the AES algorithm and steganographic methods in authentication key protection. *Collection "Information Technology and Security"*. 2025. Vol. 13(2), P. 178–191. DOI: https://doi.org/10.20535/2411-1031.2025.13.2.344592
12. Zhyvylo, Y., & Kuchma, Y. DEEP LEARNING MODEL FOR PREDICTING COMPROMISED ACCOUNTS IN SECURITY EVENT MANAGEMENT SYSTEMS. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique»*. 2025. Vol. 3(31), P. 589–601. DOI: https://doi.org/10.28925/2663-4023.2025.31.1050
13. Kashkevich S., Kashkevych I., Kuvshynov O., Kuzavkov V., Zhyvylo Y., Dmytriieva O., Lebedynskyi A., Pysarenko A., Zudikhin Y., Shyshatskyi A. Development of a method for assessing the state of dynamic objects using a population algorithm. *Eastern-European Journal of Enterprise Technologies*. 2024. Vol. 4 (3 (130)), P. 29–36. DOI: https://doi.org/10.15587/1729- 4061.2024.308389
14. Koval M., Sova O., Shyshatskyi A., Orlov O., Artabaiev Yu., Shknai O., Veretnov A., Koshlan O., Zhyvylo Ye., Zhyvylo I. Improvement of complex resource management of special-purpose communication systems. *Eastern-European Journal of Enterprise Technologies*. 2022. Vol. 5, no. 9 (119), P. 34−44. DOI: https://doi: https://doi.org/10.15587/1729-4061.2022.266009
15. Yanko A., Krasnobayev V., Hlushko A., & Myziura M. Implementation of cryptographic transformations for digital security using the Residue Number System. *13th International Scientific and Practical Conference "Information Control Systems & Technologies" (ICST-2025)*. CEUR Workshop Proceedings, 4048, 55–67. URL: https://ceur-ws.org/Vol-4048/paper05.pdf.