UDC 004.75
DOI https://doi.org/10.32782/2663-5941/2025.2.1/11

Bobyk Yu. V.
Institute of Information and Communication
Technologies and Electronic Engineering

Shpur O. M.
Institute of Information and Communication
Technologies and Electronic Engineering

DESIGNING THE COMPLEX MONITORING IN DISTRIBUTED INFORMATION AND COMMUNICATION SYSTEMS

This paper explores the development and implementation of a comprehensive monitoring and management solution designed to ensure high Quality of Service (QoS) in Distributed Information and Communication Systems (DICS). It focuses on the prerequisites and technological foundations necessary for the early detection of anomalies in network performance and the automatic reallocation of resources across multiple layers of infrastructure, including network, computational, and service levels. As modern DICS operate in increasingly complex and dynamic environments, maintaining stability and service quality requires adaptive, intelligent, and scalable solutions.

The proposed architecture is based on the integration of distributed telemetry agents, centralized telemetry storage systems, and hybrid data processing methodologies. These tools work together to analyze performance indicators like latency, jitter, packet loss, CPU load, and bandwidth usage in real time, enabling proactive response to performance degradation or resource overloads.

A key aspect of the system is its decision-making and automation capability, achieved through integration with modern orchestration and network management environments. These environments support near real-time adaptation of infrastructure based on analytical insights provided by the monitoring system, thus enabling self-healing, load balancing, and failover mechanisms without human intervention.

The designed solution is modular and interoperable, making it suitable for seamless integration into existing network and service management platforms. It enhances the reliability, fault tolerance, and scalability of distributed architectures, particularly in scenarios involving high user demand, geographic dispersion, heterogeneous infrastructure (including cloud and edge computing), or stringent SLA requirements. By enabling intelligent monitoring and automatic adaptation, the system ensures sustained service quality, operational efficiency, and resilience even under conditions of unpredictable load spikes or security threats.

Key words: *distributed ICS (DICS), monitoring, quality of service (QoS) management, adaptive algorithms, anomalies, machine learning, scaling.*

Formulation of the problem. The current stage of development of information and communication technologies (ICT) is characterized by rapid growth of data volumes and expansion of the range of services provided through distributed information and communication systems (DICS). Advances in cloud computing, virtualization, and containerization (Kubernetes, Docker, etc.), as well as the growing popularity of microservice architecture, have led to a more complex infrastructure structure and management. On the one hand, users need a wide range of available services 24/7 with guaranteed quality of service (QoS), and on the other hand, system administrators and telecom operators are forced to look for more flexible approaches to ensure reliability, performance, and scalability in the face of high load and dynamic changes in network topology.

This situation is caused by two key trends. First, the number of devices connected to the network is constantly increasing, which is being fueled by the proliferation of the Internet of Things (IoT) and smart sensor systems. This creates both a growing load on the network infrastructure and the need for constant monitoring and analysis of relevant data. Secondly, business processes that serve large networks increasingly require guaranteed QoS levels from ICT systems to maintain competitiveness and meet the strict requirements of Service Level Agreements (SLAs). At the same time, managing distributed infrastructure becomes more complicated, as resources and services are often located in different geographical areas that may belong to different operators or cloud platforms (AWS, Azure, Google Cloud, etc.). Unpredictable transit delays, various routing mechanisms, variable bandwidth, and the possibility of local overloads or failures of individual components should be taken into account. Therefore, there is a need to improve methods and algorithms for monitoring and managing QoS to ensure stable operation of services under any network and computing load.

Analysis of recent research and publications. The issue of ensuring proper quality of service (QoS) in distributed information and communication systems has long been in the focus of attention of the scientific community and the telecommunications industry. Traditionally, the approaches recommended by ITU-T (in particular, E.800 [1]) have been used to assess and maintain QoS, which offer basic methods for measuring key indicators (delay, jitter, throughput, packet loss, etc.). However, with the proliferation of cloud computing, virtualization, and the widespread adoption of the Internet of Things (IoT), such traditional systems are increasingly proving insufficient for monitoring large, distributed, and dynamically changing environments. However, as the topology became more complex and the load on network nodes increased, it became clear that a shift to a proactive monitoring and management paradigm was needed to ensure a high level of QoS in distributed systems. At the same time, there is a growing interest in machine learning (ML) algorithms and artificial intelligence systems capable of predicting workload. These tools allow to identify patterns (seasonality, daily cycles, activity spikes) based on historical data, allocating additional resources (e.g., computing nodes, bandwidth) in advance. This approach is mainly used in cloud and virtualized environments, where resource allocation or release can be performed in an almost automated manner [3, 6]. The papers [4, 7] addresses this problem by monitoring SDN flows and service logs, which is a very important feature of a monitoring system that can reduce the risk of DoS and keep the service component available to users. Recent studies emphasize the growing role of highly reliable real-time monitoring of cloud services and networks. In particular, in [5], the authors consider traffic engineering in service-oriented software-defined networks, paying special attention to the operational monitoring of network flow parameters to implement QoS-oriented routing and ensure the required level of QoE for end users. However, the monitoring in this study focuses mainly on the network aspects, without taking into account data on services or computing resources. This conclusion prompted us to develop a comprehensive system capable of providing a high level of quality of service (QoS) in the face of dynamic changes in network infrastructure and diverse loads.

Task statement. The main purpose of the article is to investigate the effectiveness of the interaction between information technologies and neural networks for automated text content generation and to determine the optimal approaches to the use of these technologies in real industries such as writing, marketing, and business. In addition, the paper examines the impact of modern neural network architectures on the quality of text generation, and explores the features of using basic neural network models for text generation. Criteria for a comprehensive assessment of the quality of the generated content are proposed, and prospects for the development of synergy between information technology and neural networks are identified. Forecasts are given on the trends of the industry development, including increasing the adaptability of texts to the cultural or linguistic context.

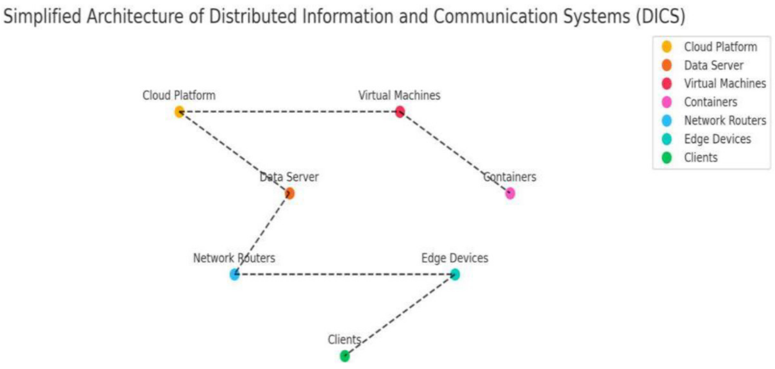

Fig. 1. DICS architecture diagram

Outline of the main material of the study. With the rapidly increasing complexity of modern distributed information and communication systems (DICS), there is a need for a comprehensive approach to monitoring and managing the quality of information services (QoS).

The enhanced architecture of Distributed Information and Communication Systems (DICS) consists of an expanded network of interconnected components that ensure data storage, processing, and transmission between users and cloud resources. The central element is the cloud platform, which provides computing power and is connected to data servers and virtual machines. Data servers process requests, interact with databases, and facilitate data transmission through network routers.

To meet user needs and strict SLA requirements, QoS monitoring and management systems must not only diagnose the current state, but also proactively prevent potential failures or dramatic deterioration in performance. Several key factors complicate this task:

Dynamic changes in infrastructure. (DICS) consist of interconnected subsystems (network routers, data servers, virtual machines, containers, etc.), the configuration of which can change at any time due to load balancing, automatic autoscaling, or software updates.

In multiservice environments, services with varying degrees of criticality are provided simultaneously.

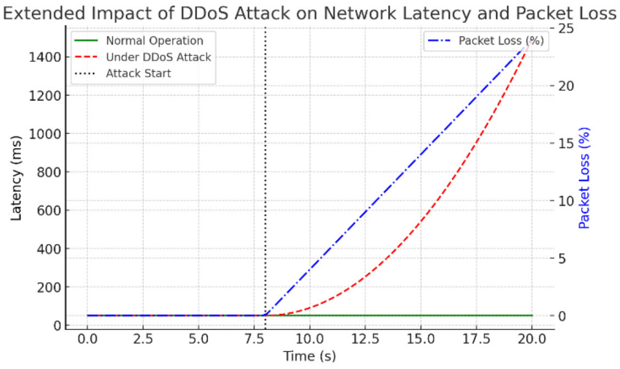

Fig. 2. Impact of DDoS attacks on latency

Table 1

Comparison of QoS parameters and service types

Service Type	Critical Metrics	Tolerated Packet Loss (%)	Required Bandwidth (Mbps)
Video Streaming	Latency, Jitter	1	5
Voice Communication	Latency, Jitter	1	0.1
Backups	Bandwidth	5	100

QoS degradation can arise from several interconnected factors:

– Excessive user traffic may result in the overloading of network channels, application servers, or databases, disrupting normal operations.

– Insufficient computing resources often lead to suboptimal performance of service components, directly affecting their ability to handle requests efficiently.

– Inefficient network routing that fails to account for user traffic patterns or the geographic locations of users and service components can exacerbate delays and packet losses.

Solving the problem of proactive monitoring and adaptive management of the quality of information services in distributed ICS requires an integrated approach that covers all levels of the system: from physical and channel interaction (telemetry collection, low-level monitoring) to high-level service orchestration (dynamic scaling in the cloud, reconfiguring routes in SDN, traffic prioritization).

Each node or group of nodes in the DICS is equipped with agents that measure key indicators: bandwidth, latency, jitter, packet loss, CPU utilization, memory usage, virtual machine status, etc. Data collection technologies. To minimize the delay in data transmission, agents can perform primary processing (aggregation, hashing) locally and send the compressed information to central monitoring nodes.

Alert system. In case of significant deviations from normal indicators or critical events, notifications are sent (via e-mail, SMS, push channels) and/or external scripts are automatically called to trigger control mechanisms.

Linear and polynomial regression. They are used as basic approaches to identify trends (e.g., slow growth of delay) and extrapolate short-term load. ARIMA, SARIMA, and other time-based models. Used for more accurate modeling of time series with seasonal fluctuations (daily/weekly cyclicality). Machine learning methods (neural networks,

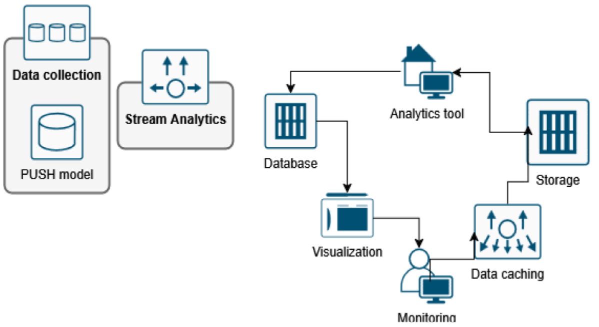

Fig. 3. Multi-level monitoring system

Random Forest, XGBoost). They allow taking into account nonlinear dependencies between parameters and predicting unusual situations in advance. For each indicator, statistical thresholds (mean, standard deviation) are calculated, when exceeded, the system generates a signal of a possible deviation. Clustering models (K-means, DBSCAN). Metrics belonging to clusters with low density or that do not correspond to "typical" centroids are treated as anomalous. Distance estimation (Mahalanobis distance, Isolation Forest). Allows you to automatically detect points or entire subsets of data that have atypical characteristics compared to the majority. If possible, the central components of the monitoring system should be duplicated in geographically distant data centers.

Effective proactive monitoring and adaptive management of information service quality in DICS rely on continuous improvement and extension of the monitoring infrastructure. As networks grow in scale and complexity, new technological solutions and architectural models become relevant to handle emerging challenges.

By placing data preprocessing and partial analytics (e.g., anomaly detection) at edge or fog nodes, the system can reduce the load on central servers and minimize latency.

Deploy monitoring agents across multiple public or private cloud providers, enabling unified visibility into distributed workloads. Harmonize telemetry formats (e.g., OpenTelemetry) to collect data consistently regardless of the cloud platform. Use federated learning or distributed AI techniques to train and improve anomaly detection models across different cloud environments without transferring raw data.

Incorporate deeper neural network architectures (LSTM, GRU, Transformers) for more accurate forecasting of network load and resource utilization. Apply reinforcement learning for dynamic adaptation strategies, where the monitoring system optimizes its own decision-making policies based on real-time feedback. Improves trust and transparency for operators managing critical infrastructure.

Extend the monitoring system to collect and analyze security-related telemetry (intrusion attempts, unexpected port scans, lateral movement in the network). Correlate security metrics with performance data to detect malicious traffic patterns that also affect QoS (e.g., DDoS attacks). Combine anomaly detection with network policy enforcement tools (firewalls, intrusion prevention systems) to isolate compromised nodes or throttle suspicious traffic. Implement runbooks or playbooks that trigger automated mitigation steps based on predefined security thresholds.

Adopt tools like Terraform or Ansible to define and manage monitoring environments, enabling repeatable and version-controlled deployments. Automate scaling of monitoring agents or central servers in response to usage spikes or newly deployed services. By extending the proposed monitoring system with edge/fog processing, advanced AI techniques, and multi-cloud orchestration, organizations can achieve even higher levels of agility, resilience, and efficiency in managing distributed ICS. Incorporating enhanced security metrics, self-healing mechanisms, and robust disaster recovery strategies will further solidify the system's reliability and responsiveness.

The IMS platform, operating at the core network level, is a key architecture enabling Voice over LTE (VoLTE) and other IP-based multimedia services. It consists of critical components responsible for session control, subscriber authentication, and media handling. These components function at various sublevels within the core network:

1. Session control is managed by the Call Session Control Function (CSCF), which operates at the application signaling level.

2. Subscriber authentication is handled by the Home Subscriber Server (HSS), functioning at the database level.

3. Media handling is performed by the Media Resource Function (MRF), which operates at the media processing level.

Given the critical role IMS plays in delivering VoLTE and multimedia services, it is essential to implement robust firewalls to safeguard the network against unauthorized access, cyberattacks, and service disruptions. Firewalls, deployed at the network level, particularly at the perimeter and between network segments, are crucial for protecting the IMS platform's core infrastructure from external threats. They filter incoming and outgoing traffic, ensuring that only legitimate traffic is allowed while blocking potentially malicious activity. Firewalls also provide essential protection for sensitive subscriber data and critical IMS components like the HSS and MRF, maintaining both privacy and service reliability.

In addition to firewalls, a notification system, operating at the application level, plays a vital role in network management by providing real-time alerts in the event of significant deviations from normal operating conditions or critical system failures. When key QoS parameters or network events exceed predefined thresholds, the system sends notifications via various channels such as email, SMS, or push alerts. This allows network operators to be immediately informed of potential issues, enabling quick intervention and minimizing service disruptions. Furthermore, external scripts can be automatically triggered in response to these alerts, activating predefined mechanisms to control or mitigate the impact of the issues. For example, if a surge in packet loss or latency is detected, scripts may be executed to reroute traffic, adjust resources, or activate backup systems, ensuring the network continues to perform optimally even during periods of stress.

To complement this security layer, Vodafone employs a sophisticated notification system, functioning at the application level, to continuously monitor its network. In the event of deviations from expected QoS parameters (e.g., high latency, packet loss, or jitter spikes), the system triggers immediate alerts via multiple channels such as email, SMS, and push notifications to the operations team.

For example, in the case of a major mobile operator, parameters such as latency, jitter, packet loss, and throughput are continuously monitored to assess network performance. These metrics are measured at the transport level of the network. Operators often use regression models like linear and polynomial regression to identify trends, such as gradual increases in latency, allowing them to anticipate potential issues and optimize network resources.

Time series models such as ARIMA and SARIMA are employed to account for seasonal variations, such as daily or weekly traffic cycles. These models help telecom operators refine their predictions, making them more accurate for specific time frames. Machine learning techniques, including neural networks, Random Forest, and XGBoost, are increasingly used to capture complex, non-linear relationships between network parameters. They offer an advantage in predicting unexpected situations, such as sudden spikes in traffic or network congestion, which would otherwise be difficult to foresee using traditional methods.

Additionally, statistical thresholds are set for each QoS parameter (e.g., mean, standard deviation), and the system is programmed to trigger alerts whenever these limits are exceeded, signaling potential issues that could affect service quality. Clustering methods like K-means and DBSCAN are used to detect outliers, with any metrics that deviate significantly from typical patterns flagged as anomalies. These anomalies can indicate a network fault or congestion event, enabling operators to take preemptive action. For more precise anomaly detection, distance-based methods like Mahalanobis distance and Isolation Forest can be employed to identify data points or subsets that exhibit atypical behavior.

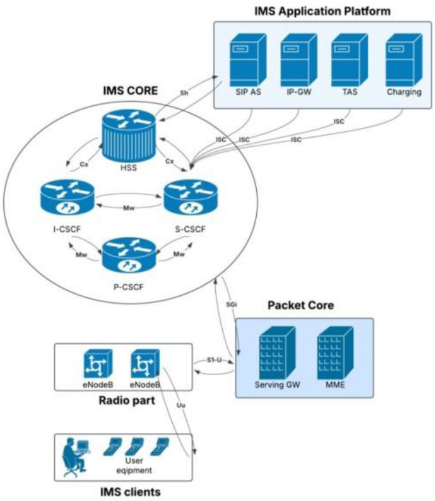

Fig. 4. The typical scheme of IMS

In a live operator environment, such as telecommunications networks, redundancy and fault tolerance play a key role in ensuring high availability, reliability, and performance. To achieve this, monitoring systems are duplicated across data centers located in different geographic regions. A telecom operator may have data centers, for example, in New York, Los Angeles, and Frankfurt, where identical instances of the monitoring system operate, including components for data collection, processing, and notification delivery. This setup ensures that if one data center fails – due to a power outage, network disruption, or natural disaster – the monitoring system automatically switches to another data center. Load balancers, such as HAProxy or Google Cloud Load Balancing, distribute incoming monitoring traffic across these data centers, taking into account latency, health checks, and available capacity, reducing the risk of a single point of failure and ensuring continuous network monitoring.

Fault tolerance is further enhanced by automatically launching backup instances for critical components. Monitoring systems utilize modular containerized components, such as data collectors, analytics engines, and alerting modules, which are managed through orchestration tools like Kubernetes. This tool continuously monitors the state of containers using liveness and readiness probes. For instance, if the virtual machine running the analytics engine for processing latency data fails, Kubernetes detects the issue and restarts the container, minimizing downtime and ensuring uninterrupted user service.

Proactive network management is also a key advantage of monitoring systems, as they continuously track key performance indicators such as latency, jitter, packet loss, and bandwidth. Monitoring agents installed on network devices – routers, switches, and base stations – send real-time metrics to the monitoring system using protocols like SNMP or streaming telemetry, such as gRPC and OpenTelemetry. This data is stored in time-series databases like InfluxDB or Prometheus, allowing efficient querying and visualization through tools such as Grafana. Alerting rules are configured to send notifications when predefined thresholds are exceeded – for example, if latency surpasses 100 ms for five minutes, the on-call team receives an alert via PagerDuty. This continuous monitoring helps detect early signs of network degradation before they affect users. If, for instance, latency on a particular network path begins to rise, the monitoring system triggers an alert, allowing operators to reroute traffic to less congested paths and prevent customer complaints about dropped connections or slow internet speeds.

Additionally, monitoring systems provide real-time insights to ensure stable and high-quality service. Machine learning models integrated into monitoring pipelines predict traffic spikes or anomalies. Automation tools like Ansible or Terraform execute predefined scripts based on this data – if, for instance, tower bandwidth usage exceeds 80 %, additional resources are allocated automatically. This proactive approach allows telecom operators to maintain stable and high-quality service even during peak load periods while adhering to service level agreements (SLAs).

In the case of Vodafone, ensuring optimal QoS is essential for maintaining the reliability of their voice and multimedia services, especially in a highly competitive market. The operator consistently monitors key QoS parameters like latency, jitter, packet loss, and throughput to ensure a seamless experience for its users.

Vodafone also leverages time series models such as ARIMA and SARIMA to account for daily and weekly traffic cycles, which are critical for managing network load during peak times. In addition to these traditional methods, Vodafone has incorporated advanced machine learning techniques, such as neural networks and XGBoost, to better handle non-linear dependencies in network traffic.

To detect performance anomalies, Vodafone employs clustering techniques like K-means and DBSCAN, identifying any metrics that deviate significantly from typical patterns. This enables the company to spot potential issues early, such as network outages or sudden drops in service quality. Advanced anomaly detection methods, including Mahalanobis distance and Isolation Forest, are used to pinpoint specific instances where network behavior falls outside expected norms, allowing for faster issue resolution.

Vodafone also emphasizes redundancy and fault tolerance in its monitoring systems. To ensure uninterrupted service, they replicate critical components across geographically diverse data centers.

1. Real-Time Traffic Rerouting. Vodafone's monitoring systems continuously analyze network congestion levels. If a particular network path experiences excessive latency or packet loss, traffic is dynamically rerouted through alternative, less congested routes.

2. Proactive Network Maintenance. By integrating predictive analytics, Vodafone can anticipate hardware failures in critical infrastructure such as base stations and fiber optic links. For example, if a base station starts showing a gradual increase in error rates or unusual temperature spikes, preemptive maintenance can be scheduled to prevent potential outages.

3. Optimized Video Streaming Performance. Using real-time telemetry data, Vodafone adjusts video streaming bitrates based on network conditions. If the system detects high congestion in a region, it dynamically reduces the resolution of video streams to prevent buffering, ensuring a smooth user experience.

4. Load Balancing in Cloud Infrastructure. Vodafone's cloud-based services leverage load balancers like HAProxy and Google Cloud Load Balancing to distribute traffic among multiple servers. If one server cluster experiences high CPU or memory usage, new sessions are redirected to underutilized servers to maintain consistent performance.

5. Emergency Response Management. In the event of natural disasters or large-scale network failures, Vodafone's monitoring system prioritizes emergency communications by allocating additional network resources to first responders. This ensures that critical services remain operational even under extreme conditions.

6. Customer Experience Enhancement through AI-Driven Support. AI-driven monitoring tools analyze customer complaints related to network quality and correlate them with real-time performance data. If multiple complaints arise from a specific area, Vodafone's system automatically triggers an investigation, allowing for faster resolution of service issues.

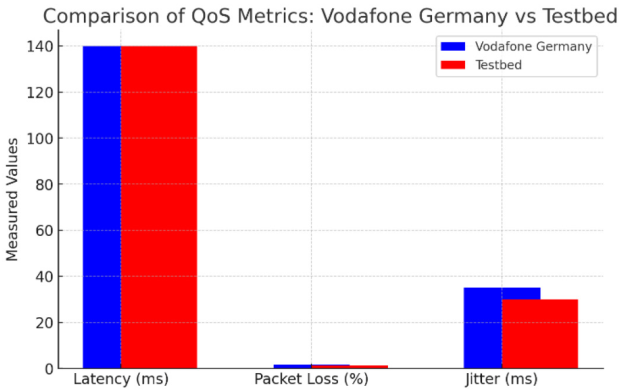

Fig. 5. Comparison of QoS Metrics

By employing a combination of predictive analytics, machine learning, and robust infrastructure, Vodafone ensures a consistently high level of QoS for its users while proactively addressing network challenges in real time.

To evaluate the QoS of the IMS platform, multiple test scenarios were executed under controlled conditions. End-to-end testing was performed by initiating VoLTE calls between test devices while monitoring key performance indicators such as call setup time, voice clarity, and connection stability. Load testing involved simulating thousands of concurrent calls and data sessions to observe system behavior under peak traffic. Packet-level analysis was conducted using Wireshark, capturing real-time traffic to measure latency, jitter, and packet loss.

To illustrate real-world QoS challenges, we analyzed Vodafone VoLTE network performance. During peak hours, call setup time increased by 3 %, reaching 310 ms, slightly exceeding the 300 ms threshold. Packet loss under heavy load rose to 1.5 %, affecting voice clarity. Network logs showed that congestion primarily occurred at eNodeB backhaul links. Using the formula for Packet Loss Rate (PLR):

$$PLR = \left(\frac{LP}{T}\right) \cdot 100, \qquad (1)$$

where *LP* – Lost Packets; *T*– Total Packets sent

For a stress test with 10 million packets sent and 150,000 lost packets, the calculated PLR was 1.5 %. Comparing our testbed results with Vodafone real-world data:

1. Latency remained stable in both cases, averaging 140 ms.

2. Packet loss exceeded thresholds (1.5 % vs. 1.2 %), suggesting bottlenecks in high-load scenarios.

3. Jitter spikes (Vodafone: 35 ms, Lab: 30 ms) were noticeable but tolerable.

To assess the impact on call quality, Hammer Call Analyzer measured parameters like MOS (Mean Opinion Score) and call drop rates during peak load periods. Advanced machine learning models, specifically Long Short-Term Memory (LSTM) networks, were trained on historical network data to predict congestion events and optimize resource allocation dynamically. These AI-driven insights allowed for real-time adjustments in the network configuration, improving QoS by proactively managing capacity and mitigating performance degradation, ensuring a seamless VoLTE experience for Vodafone's users.

The data from the stress test with 100,000 concurrent calls reveals several important insights into the performance of the network under heavy load. Below is a more detailed analysis based on the metrics provided:

1. The CSSR is slightly below the expected value, indicating a small number of failed call setups under stress. Although 98.5 % is a high success rate, this small degradation may result in some users experiencing issues when trying to initiate calls during peak times. This metric is critical for user experience, and while it is still acceptable in most cases, attention should be given to optimizing network resource allocation to reduce call setup failures during high demand.

2. Under normal conditions, the packet loss rate is within acceptable limits, but during the stress test, packet loss increased to 1.2 %, slightly exceeding the expected threshold. This suggests that the network is experiencing congestion under heavy load, leading to packet loss. Although this is marginally above the threshold, it indicates a potential area for optimization. Packet loss above 1 % can have a significant impact on service quality, especially for VoLTE calls, leading to audio dropouts or poor call quality.

3. The average call setup time is within the acceptable range, even under load. A 2 % increase in call setup time under stress is well within operational limits, suggesting that the network is managing to

Table 2

Performance Metrics

Metric	Call Setup Success Rate (CSSR)	Packet Loss Rate	Average Call Setup Time	Jitter	Latency	System Throughput
Expected Value	>99 %	<1 %	<300 ms	<30 ms	<150 ms	>1 Gbps
Measured Value	98.5 %	0.8 %	280 ms	25 ms	140 ms	1.2 Gbps

handle the load efficiently in terms of call initiation. However, it is important to continue monitoring this parameter as increased traffic may eventually lead to higher delays.

4. Jitter remains within acceptable limits during normal operation. However, during the stress test, occasional spikes in jitter beyond 30ms were observed. While jitter in itself is not an immediate concern, these spikes can lead to noticeable issues in voice quality during calls. VoLTE traffic is particularly sensitive to jitter, and periodic fluctuations can degrade user experience by causing choppy audio or dropped calls. This suggests a need for further optimization to mitigate jitter during peak periods.

5. Latency remains stable and within the acceptable limits even under stress. The network has shown resilience in handling the increased traffic without experiencing excessive delays in packet transmission. While latency is well within the threshold, periodic monitoring of the network infrastructure is necessary to ensure it remains stable during prolonged periods of high traffic.

6. In the case of Vodafone, ensuring optimal QoS is essential for maintaining the reliability of their voice and multimedia services, especially in a highly competitive market. The operator consistently monitors key QoS parameters like latency, jitter, packet loss, and throughput to ensure a seamless experience for its users. For instance, Vodafone uses linear and polynomial regression models to track trends in latency and identify gradual increases that could indicate network stress. By analyzing these trends, Vodafone can predict potential bottlenecks and take corrective action before they impact customers.

Even under load, the network maintained throughput above 1 Gbps, ensuring that data-intensive applications can function without significant degradation. To improve QoS during high traffic periods, implementing traffic prioritization mechanisms such as DiffServ or MPLS can help manage network resources more efficiently. These protocols enable better differentiation of traffic types, ensuring that critical services like VoLTE receive higher priority and are less likely to be affected by congestion. Addressing packet loss requires further capacity planning, particularly during peak periods, which may involve upgrading hardware such as routers and switches or allocating additional bandwidth to prevent congestion. Proactive bandwidth monitoring tools should be employed to detect potential congestion points before they impact performance.

Introducing dynamic and adaptive QoS policies based on real-time network load can optimize resource allocation. By leveraging real-time data on network conditions such as traffic volume, load distribution, and QoS parameters, the network can adjust its policies dynamically to ensure optimal service quality. For example, during periods of high load, the system could automatically allocate more resources to maintain call quality, while during low-load periods, resources could be reallocated to other services. While jitter remains within acceptable limits in most cases, occasional spikes suggest the need for jitter mitigation strategies. Techniques such as buffer management, prioritization of VoLTE traffic, and improving network resilience can help reduce jitter during peak periods. Additionally, investing in network infrastructure that reduces congestion and improves packet delivery consistency can help keep jitter levels within desired thresholds.

Continuous monitoring should be implemented for all key QoS parameters, especially under heavy traffic conditions. This could include re-routing traffic, adjusting network configurations, or alerting the network operations team to potential problems. While the network performs well under most conditions, critical areas such as packet loss, jitter, and dynamic traffic handling require optimization to maintain a consistently high-quality user experience, particularly during high-demand periods.

Conclusions. This paper presents the development of a multi-level monitoring system for distributed information and communication systems (DICS), which includes telemetry agents, centralized data storage, and real-time analysis tools. By integrating technologies such as machine learning, edge/fog computing, and automated orchestration, the system ensures high QoS even under dynamic network conditions. The integration of advanced features like anomaly detection and adaptive resource management highlights the system's ability to maintain a high level of Quality of Service (QoS) while reducing operational costs.

By detecting malicious activities such as DDoS attacks and integrating with firewalls and threat detection modules, the system ensures that security incidents are identified and mitigated in real-time. This proactive defense not only protects the network but also minimizes disruptions, ensuring continuous service availability.

This enables the detection of potential issues early, such as network outages or sudden drops in service quality. Advanced anomaly detection methods, including Mahalanobis distance and Isolation Forest, are used to pinpoint specific instances where network behavior falls outside expected norms, allowing for faster issue resolution.

The analysis of the IMS platform in the context of a telecom system has provided valuable insights into the performance, security, and reliability of VoLTE services. The study examined key aspects such as Quality of Service (QoS) parameters, security mechanisms, and automated notification systems to ensure a seamless user experience. The findings highlight the importance of continuous monitoring, predictive analysis, and proactive network management in maintaining high service quality.

The implementation of these security mechanisms ensures the integrity of critical components like the Home Subscriber Server (HSS) and Media Resource Function (MRF). Key QoS parameters, including latency, jitter, packet loss, and throughput, were analyzed using statistical and machine learning models. Regression models, time series forecasting, and clustering methods help identify performance trends and detect anomalies. These techniques enhance the ability to optimize network performance and anticipate congestion before it affects end-users.

The study included end-to-end VoLTE call testing, load testing, and packet-level analysis using tools like Wireshark. Performance degradation was observed during peak traffic periods, particularly in packet loss and jitter. Stress testing confirmed that under heavy loads, network congestion primarily occurs at the eNodeB backhaul links. The system met most KPIs but showed slight degradation under peak conditions. The call setup success rate was slightly below the expected threshold. Packet loss exceeded the 1 % limit under heavy load. Jitter occasionally spiked beyond the 30ms threshold, while latency remained within acceptable limits. System throughput exceeded expectations, ensuring sufficient capacity for handling network traffic. IMS-based VoLTE networks meet most QoS standards, though peak traffic can cause slight degradation. Proactive monitoring and dynamic resource management are essential for sustaining high service quality, especially in the context of 5G development.

Bibliography:

1. ITU-T Recommendation E.800 (Rev. 09/2008). Definitions of terms related to quality of service. International Telecommunication Union, 2008.

2. NetFlow services and applications white paper. Cisco, 2004.

3. Kumar B., Krishnamurhty A., Mohan R.M. Machine learning based presaging technique for multi-user utility pattern rooted cloud service negotiation for providing efficient service. *2020 2nd international conference on innovative mechanisms for industry applications (ICIMIA)*, Bangalore, India, 5–7 March 2020. 2020. URL: https://doi.org/10.1109/icimia48430.2020.9074895

4. Peleh N., Shpur O., Klymash M. Intelligent detection of ddos attacks in SDN networks. *Lecture notes in electrical engineering*. Cham, 2021. P. 210–222. URL: https://doi.org/10.1007/978-3-030-92435-5_12

5. Traffic engineering and QoS/QoE supporting techniques for emerging service-oriented software-defined network / M. Beshley et al. *Journal of Communications and Networks*. 2024. Vol. 26, no. 1. P. 99–114. URL: https://doi.org/10.23919/jcn.2023.000065

6. Abeykoon V.L., Fox G.C., Kim M. Performance Optimization on Model Synchronization in Parallel Stochastic Gradient Descent Based SVM. *2019 19th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID)*, Larnaca, Cyprus, 14–17 May 2019. 2019. URL: https://doi.org/10.1109/ccgrid.2019.00065.

7. Concept of intelligent detection of ddos attacks in SDN networks using machine learning / M. Klymash et al. *2020 IEEE international conference on problems of infocommunications. science and technology (PIC S&T)*, Kharkiv, Ukraine, 6–9 October 2020. 2020. URL: https://doi.org/10.1109/picst51311.2020.9467963

Бобик Ю. В., Шпур О. М. РОЗРОБКА КОМПЛЕКСНОЇ СИСТЕМИ МОНІТОРИНГУ В РОЗПОДІЛЕНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

У цій статті розглядаються питання розробки та впровадження комплексного рішення для моніторингу та управління, спрямованого на забезпечення високої якості обслуговування (QoS) у розподілених інформаційно-комунікаційних системах (РІКС). Основна увага приділяється передумовам і технологічним основам, необхідним для раннього виявлення аномалій у роботі мережі та автоматичного перерозподілу ресурсів на різних рівнях інфраструктури – мережевому, обчислювальному та сервісному. Оскільки сучасні РІКС функціонують у дедалі складніших і динамічніших середовищах, підтримка стабільності та якості обслуговування вимагає адаптивних, інтелектуальних і масштабованих рішень.

Запропонована архітектура базується на інтеграції розподілених агентів збору телеметрії, централізованих систем зберігання телеметричних даних та гібридних методів обробки інформації. Ці інструменти працюють разом для аналізу показників продуктивності, таких як затримка, джиттер, *втрата пакетів, завантаження процесора та використання пропускної здатності в режимі реального часу, що дозволяє проактивно реагувати на погіршення продуктивності або перевантаження ресурсів.*

Ключовим аспектом системи є її здатність до прийняття рішень і автоматизації, яка досягається завдяки інтеграції з сучасними середовищами оркестрації та управління мережею. Ці середовища забезпечують адаптацію інфраструктури майже в реальному часі на основі аналітичних даних, які надає система моніторингу, що дозволяє реалізовувати механізми самовідновлення, балансування навантаження та аварійного перемикання без участі людини.

Розроблене рішення має модульну структуру та забезпечує сумісність, що дозволяє легко інтегрувати його у вже наявні платформи управління мережею та сервісами. Воно підвищує надійність, відмовостійкість і масштабованість розподілених архітектур, особливо в умовах високого користувацького навантаження, географічної розподіленості, гетерогенного середовища (включаючи хмарні й периферійні обчислення) або жорстких вимог щодо рівня обслуговування (SLA). Завдяки інтелектуальному моніторингу та автоматичній адаптації система забезпечує стабільну якість обслуговування, ефективність роботи та стійкість навіть у разі непередбачуваних пікових навантажень чи кіберзагроз.

Ключові слова: *розподілені ІКС (РІКС), моніторинг, управління якістю обслуговування (QoS), адаптивні алгоритми, аномалії, машинне навчання, масштабування.*