# ENGINEER

international scientific journal

ISSUE 3, 2025 Vol. 3
E-ISSN
3030-3893
ISSN
3060-5172

SLIB.UZ
Scientific library of Uzbekistan

A bridge between science and innovation

TOSHKENT DAVLAT TRANSPORT UNIVERSITETI
Tashkent state transport university

# ENGINEER

A bridge between science and innovation

**E-ISSN: 3030-3893**

**ISSN: 3060-5172**

**VOLUME 3, ISSUE 3**

**SEPTEMBER, 2025**

**engineer.tstu.uz**

# TASHKENT STATE TRANSPORT UNIVERSITY

# ENGINEER

INTERNATIONAL SCIENTIFIC JOURNAL
VOLUME 3, ISSUE 3 SEPTEMBER, 2025




---


Founder of the international scientific journal "Engineer" – Tashkent State Transport University, 100167, Republic of Uzbekistan, Tashkent, Temiryo'lchilar str., 1, office: 465, e-mail: publication@tstu.uz.


The "Engineer" publishes the most significant results of scientific and applied research carried out in universities of transport profile, as well as other higher educational institutions, research institutes, and centers of the Republic of Uzbekistan and foreign countries.

The journal is published 4 times a year and contains publications in the following main areas:

- Engineering;
- General Engineering;
- Aerospace Engineering;
- Automotive Engineering;
- Civil and Structural Engineering;
- Computational Mechanics;
- Control and Systems Engineering;
- Electrical and Electronic Engineering;
- Industrial and Manufacturing Engineering;
- Mechanical Engineering;
- Mechanics of Materials;
- Safety, Risk, Reliability and Quality;
- Media Technology;
- Building and Construction;
- Architecture.

---


Tashkent State Transport University had the opportunity to publish the international scientific journal "Engineer" based on the **Certificate No. 1183** of the Information and Mass Communications Agency under the Administration of the President of the Republic of Uzbekistan. **E-ISSN: 3030-3893, ISSN: 3060-5172.** Articles in the journal are published in English language.

# Security issues in IP-based communication networks

**A.Sh. Khurramov**[1][a]
[1]Tashkent state transport university, Tashkent, Uzbekistan

Abstract: This article examines the structural reliability and cyber resilience of IP-based rapid technological communication networks in railway sections, particularly using train dispatcher communication systems as an example. A logical-functional model was developed for multiple stations, demonstrating that the overall reliability of the rapid technological communication network directly depends on the coordinated operation of all its elements. Simulation experiments conducted in the MATLAB environment revealed that DoS (Denial of Service) attacks can significantly reduce network performance, increasing packet loss threefold and latency fivefold. To address these issues, scientific and technical solutions such as traffic encryption, strengthening QoS mechanisms, implementing real-time monitoring systems, optimizing resources, and using firewalls were proposed. Practical implementation of these measures improved the readiness coefficient of the rapid technological communication network, ensured compliance with international information security standards, and strengthened both the safety and stability of train traffic in railway sections.

Keywords: IP communication networks; rapid technological communication (RTC); railway communication; structural reliability; cyber resilience; DoS attacks; network security; availability coefficient; firewalls; train dispatcher systems

## 1. Introduction

The IP communication network technology must become a ready-made solution and be able to provide full functional services; however, there are many technical and legal issues and problems. These aspects can be roughly divided into three groups [1]:

- development of technology and equipment;
- legal aspects of management;
- ensuring security.

Improving the equipment of information exchange systems is carried out in different directions. First of all, this involves the development of the concept of Session Border Controllers (SBCs). These are software and hardware tools that solve the problems of logical separation of networks and ensuring their functionality. Mechanisms for connecting IP communication networks are being developed, the set of interfaces and parameters is being standardized, and configuration and usage procedures are being simplified. Models developed in the field of IP communication networks mainly describe Quality of Service (QoS) mechanisms. This allows for the standardization and characterization of all parameters and norms of the quality of services offered by IP communication network technology [2].

Security is one of the main issues in the functioning of any information exchange system. IP communication networks and local IP computer network technologies are closely related, incorporating not only advantages but also certain disadvantages. In general, the set of potential threats to the communication network and influencing factors can be divided into two groups according to their origin: natural and artificial.

The elements of Rapid Technological Communication (RTC) networks [3] may be damaged or disabled as a result of the impact of natural or artificial factors.

Natural threats – threats to RTC networks and their elements arising from physical processes or natural disasters (earthquakes, thunderstorms, etc.) beyond human control.

Artificial threats – threats arising from human activity, which can be divided into:

- unintentional (accidental) threats caused by errors in design, software failures, or operator mistakes;
- intentional threats related to hacker activities and malicious actions.

Natural factors are difficult to predict in advance, as well as the damage caused by them. Artificial factors may include, for example, railway communication networks, powerful radio stations, high-voltage power lines, mechanical influences, and, most importantly, modern cyberattacks [4].

The degree of destructive influence of each factor on RTC network elements determines their level of inoperability and depends on the type, strength, scale, and accuracy of the impact. In IP-based communication network infrastructures, information security threats arise when a channel is formed between the threat source and the information source, creating conditions for security violations. The severity of such threats depends on the type of threat source, the vulnerability of the information source, and the characteristics of the signal transmission environment.

According to the type of source, threats to information security can be divided into the following:

- threats related to organizations with high potential, equipment, and motivation, acting in accordance with political, economic, or other goals of the railway company;
- threats related to organizations motivated by economic or informational interests;
- threats related to the activities of individuals (criminal elements).

Methods of influencing RTC networks [4] depend on the capabilities of the threat source. A source that gains or

[a] https://orcid.org/0000-0002-8443-9250

attempts to gain unauthorized access is considered a violator of information security. Such violators may act accidentally or intentionally in their own interests, causing breaches of information security in the network.

Violators are divided into two types:

- External violators – those without authorized access to the network (foreign intelligence representatives, members of criminal organizations, economically motivated individuals).
- Internal violators – those with authorized access (communication operators, developers, or suppliers of technical components).

One of the main problems of RTC networks is equipment failure. This can occur due to various reasons, including channel interruptions, interception of conversations, service theft, or spam attacks. Although no cases of IP communication network violations have been recorded in Uzbekistan so far, in other countries such cyberattacks have led to significant economic losses and disruption of technological processes [5].

## 2. Research methodology

Ensuring the cyber resilience of the communication network involves identifying the main types of cyberattacks and the methods of protection against them. The analysis of the results described in these studies shows that, for railway sections, the most effective approach for use in train dispatcher communication networks is the implementation of measures aimed at protecting network elements from cyberattacks [6], i.e., threats posed by network intruders (NI) (Fig 1).

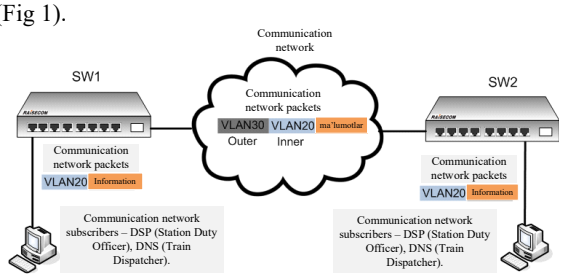


**Fig. 1. Rules for network configuration**

Specialized software and hardware. Although attacks can be carried out at any level of the ISO/OSI model, the most common ones occur at levels 3–4 and 7. Nowadays, many software and hardware manufacturers offer ready-made solutions to protect against network intruder (NI) threats. Such software and hardware may resemble a small server that allows protection against weak and medium-scale DDoS attacks as well as other types of NI threats. In practice, the following equipment is often used to neutralize intruders [7]:

- Firewalls with dynamic packet inspection;
- Dynamic SYN-proxy mechanisms;
- Limiting the number of SYN requests per IP address per second;
- Limiting the number of SYN requests per remote IP address per second;
- Installing ICMP flood filters on the firewall;
- Installing UDP flood filters on the firewall;
- Limiting the speed of routers connected to the firewall and the network.

Filtering and blocking traffic from attacking machines allows us to mitigate or completely neutralize the attack. When this method is applied, incoming traffic is filtered according to specific rules defined during the configuration of filters.

Network firewalling [8] is considered a highly effective method of protection against cyberattacks. A network firewall is a set of hardware or software tools that control and filter network packets passing through it in accordance with predefined rules.

Fig 2 shows the scheme of organizing the data transmission network of a railway station communication node using a firewall.

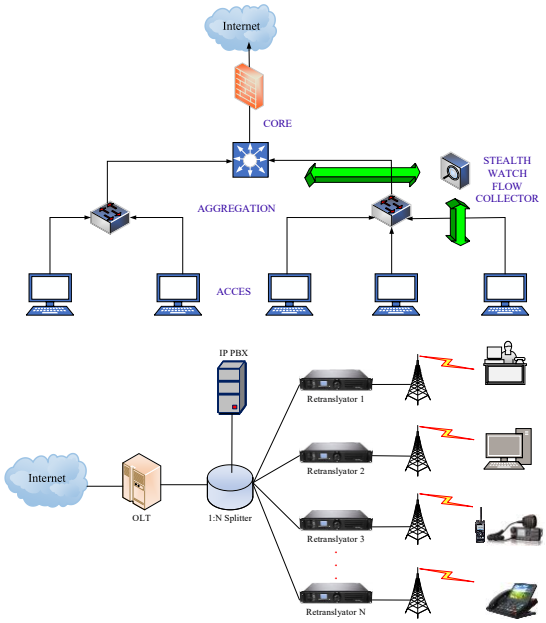


**Fig. 2. Communication center of the railway station**

The main function of network firewalling (firewall) is to protect computer networks or individual nodes from unauthorized access. In addition, firewalls are often referred to as filters, since their primary task is to block packets that do not meet the criteria specified in the configuration (i.e., filtering).

When a firewall is connected to a data transmission network (DTN), most modern firewalls perform the following functions [9]:

- attack detection;
- antivirus scanning to search for known virus signatures in traffic;
- tools for monitoring the integrity of files on a personal computer;
- tools for routing and proxying traffic (proxy servers).

The principle of operation of a firewall is to protect a network or computer from threats originating from the Internet. Each computer in a network has its own IP address, and data is transmitted through the network in IP packets. When data is transmitted, each IP packet contains the IP addresses of the sender and receiver. Accordingly, packets are delivered to recipients based on IP addresses.

However, typically, several applications run on a computer, and most of them require network access. In order for applications to interact in a network according to standards, they use special protocols [9]. For example, e-mail requires SMTP (Simple Mail Transfer Protocol), a web

browser requires HTTP (Hyper Text Transfer Protocol), and so on. Each protocol uses specific network ports, and their numbers are defined in standards. Thus, for SMTP the port is 25, and for HTTP it is 80.

Malware such as worms and trojan horses, as well as other malicious programs, can also use network ports and protocols to gain access to victims' devices, spread to other devices in the network, and transmit confidential computer data to hackers. Therefore, all ports and protocols that are not used in the direct operation of the computer should be "closed" using a firewall.

Modeling DoS Attacks in IP Communication Networks: Theory, Impact, and Mitigation [10].

The purpose of Denial of Service (DoS) attacks is to disrupt the normal operation of a network or server, which is usually carried out by overloading resources through excessive requests. In IP communication networks, such attacks cause packet loss and increased latency, mainly due to unencrypted traffic and limited resources. For Rapid Technological Communication (TTA) networks, particularly train dispatcher communication systems used in railway sections, this poses a serious threat to security and train traffic safety [10].

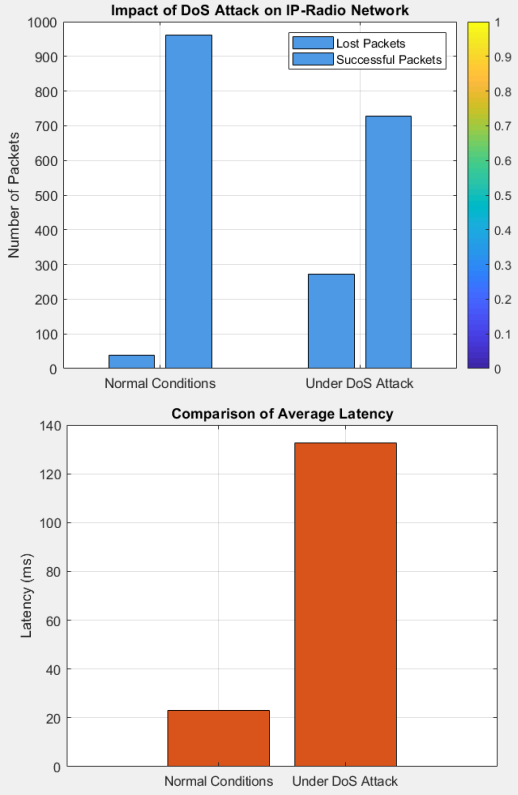


**Fig. 3. DoS attack**

A simulation was conducted in the MATLAB environment using 1000 packets under normal and DoS conditions:

- Normal conditions: packet loss 5%, average latency ~20 ms.
- DoS conditions: packet loss 30%, average latency ~100 ms. Random probabilities and noise were introduced to approximate real network conditions.
- Simulation results:
  - In normal conditions: approximately 50 packets were lost (5%), 950 packets successfully delivered, with an average latency of ~20 ms.
  - In DoS conditions: approximately 300 packets were lost (30%), 700 packets successfully delivered, with an average latency of ~100 ms.

These results indicate that during a DoS attack, packet loss increases threefold and latency increases fivefold.

Recommended Mitigation Measures

- Traffic Encryption – Encrypting IP communication network traffic to reduce the risk of data theft by attackers.
- Strengthening QoS Mechanisms – Developing specialized tools (e.g., SBC) to manage network load and ensure service quality.
- Real-Time Monitoring – Implementing dedicated monitoring systems to detect DoS attacks.
- Optimizing Network Resources – Enhancing server and network capacity to withstand DoS attacks.

The results of the conducted simulation demonstrate that DoS attacks have a significant negative impact on IP communication networks—leading to increased packet loss and latency, which jeopardizes the safety of railway communications. The practical implementation of these mitigation measures is crucial for protecting RTC networks from cyber threats and ensuring stable communication in railway sections.

Reliability Model of the TTA Network for $N$ Stations. For the reliable operation of the Rapid Technological Communication (TTA) network in a railway section, all station elements along the section must function correctly. This condition can be represented mathematically as follows. Logical condition for the correct operation of the TTA network sections of the railway segment (1).

$$K_{i.element}(t_f) = f_{\text{railway section}}(t_f) = f_{\text{element.st.A}}(t_f) \wedge f_{\text{element..st.B}}(t_f) \wedge \ldots \wedge f_{\text{element..st.N}}(t_f) \quad (1)$$

$f_{\text{element..st}}$ – denotes the reliability function of the $n$-th station element at time $t_f$;

$\wedge$ – represents the logical AND operation, meaning that the overall system works correctly only if all station elements operate reliably;

$K_{i.element}(t_f)$ – the overall reliability condition of the TTA network in the railway section.

Thus, the overall reliability of the TTA network in a railway section with $N$ stations is determined by the product of the reliabilities of each individual station. If any single station element fails, the overall reliability of the section's TTA network decreases significantly.

Based on formula (1), the dynamic change of reliability of the TTA network in the railway section is obtained (Fig 4).

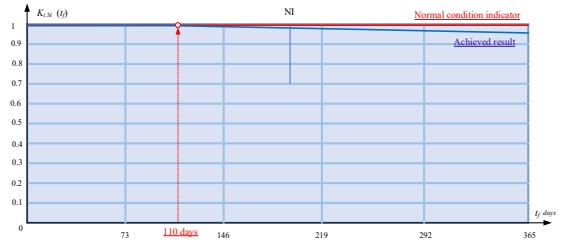


**Fig. 4. Variation of the readiness coefficient of the RTC network in the railway section**


https://doi.org/10.56143/3030-3893-2025-3-55-58 A bridge between science and innovation

As can be seen from Figure 4, after 110 days of operation (on an annual scale), the availability coefficient of the RTC network in the railway section did not meet the required level of reliability. This, in turn, necessitated additional maintenance and recovery measures, as well as the development of scientific and technical solutions aimed at improving the readiness coefficient of the RTC network in the selected area [11].

By applying the developed scientific and technical solutions to enhance the reliability of the communication network in the railway section, significant improvements can be achieved. These results are calculated based on formula (1).

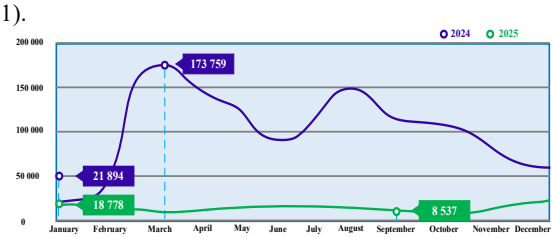


**Fig. 5. Variation of the readiness level of the communication network under DDoS attacks by months during the implementation of scientific and technical solutions developed for the railway section**

The analysis of the obtained results shows that the practical implementation of the proposed scientific and technical solutions significantly improves the reliability level of the RTC network in the railway section, while also taking into account potential cyber impacts on network elements. The achieved results meet the requirements of information security system standards, ensuring that, on an annual scale, the average number and duration of failures or malfunctions in dispatcher-level networks do not exceed 10 minutes [12].

## 3. Conclusion

Based on the conducted research, scientific approaches for assessing the reliability and ensuring the cyber resilience of IP-based RTC networks in railway sections have been developed. Simulation results identified the risks of DoS attacks and evaluated their impact on packet loss and latency.

As a result of the analysis, technical solutions such as traffic encryption, strengthening QoS mechanisms [12], real-time monitoring, and the use of firewalls were proposed for train dispatcher communication systems.

The practical implementation of these solutions improved the readiness coefficient of RTC networks, ensured compliance with international information security standards, and contributed to enhancing overall transport safety.

## References

[1] Smith, A., & Garcia, M. (2020). Enhancing data security in IP-based railway communication systems. International Journal of Transportation Safety. DOI: 10.1016/j.ijts.2020.05.001

[2] ITU. (2016). Introduction to railway communication systems. ITU Report. Retrieved from https://www.itu.int.

[3] Jablonski, M. (2022). Digital transformation in rail transport—key challenges and barriers. Springer Proceedings on Intelligent Transportation Systems. DOI: 10.1007/978-3-030-96133-6_5.

[4] European Parliament. (2019). Digitalization in railway transport. European Parliamentary Research Service. Retrieved from https://www.europarl.europa.eu.

[5] Nikitin, A., Manakov, A., & Knyazev, A. (2020). On the issue of using digital radio communications of the DMR standard to control the train traffic on Russian railways. Retrieved from.

[6] Li, P., Xue, R., Shao, S., Zhu, Y., & Liu, Y. (2023). Current state and predicted technological trends in global railway intelligent digital transformation. Railway Sciences. DOI: 10.1108/rs-10-2023-0036.

[7] Khalikov Abdulxak, Khurramov Asliddin, Urokov Olim, Rizakulov Sherzod. A mathematical model of the operation process of a radio communication network based on IP technologies in the conditions of information impact during the transmission of a non-repetitive data stream / E3S Web of Conferences 420, 03022 (2023).

[8] Xurramov A.Sh., O‘roqov O.X., Xolboyev Sh.F. Temir yo‘l uchastkalarida poyezd radioaloqasini tashkil qilishda raqamli mobil tizimlarini joriy qilish. Muhammad al-Xorazmiy avlodlari, № 1 (27), mart 2024. ISSN-2181-9211. TATU. 140-143b.

[9] Хуррамов А.Ш., Уроков О.Х., Ирагашев Н.Н. Анализ и оценка факторов, влияющих на сеть оперативной технологической радиосвязи на основе IP-радиотерминалов. Транспорт: наука, техника, управление. Научный информационный сборник. – 2024. – № 5. – С. 26-29. – DOI 10.36535/0236-1914-2024-05-4. – EDN KKOZTJ.

[10] Recommendation ITU – T Y.110. Global Information Infrastructure principles and framework architecture.

[11] Khalikov Abdulxak, Khurramov Asliddin, Urokov Olim, Rizakulov Sherzod. A mathematical model of the operation process of a radio communication network based on IP technologies in the conditions of information impact during the transmission of a non-repetitive data stream / E3S Web of Conferences 420, 03022 (2023).

[12] Xalikov A.A., O‘rokov O.X., Xurramov A.Sh. IP-tarmoq asosidagi tezkor texnologik radio aloqa tarmog‘i ishonchliligini hisoblash metodikasi. Muxammad Al-Xorazmiy avlodlari № 1(23)/2023. ISSN-2181-9211. TATU. 125-132 b.

## Information about the author

**Asliddin Khurramov**
Tashkent State Transport University, Associate professor of Department of Radioelectronic Devices and Systems, Ph.D.
E-mail: asliddinxurramov703@gmail.com
Tel.: +998909077300
https://orcid.org/0000-0002-8443-9250

# CONTEXT / MUNDARIJA