CONTENT

Vol. 12. No. 2-2026

Published bi-monthly since 2015

ISSN 2664-0678 (Online)
ISSN 2664-066X (Print)

Publisher
Institute of Radio and Information Systems (IRIS), Vienna, Austria

Address:
1010 Wien, Austria, Ebendorferstrasse 10/6b
media-publisher.eu/synchroinfo-journal

SYNCHROINFO JOURNAL

www.media-publisher.eu/synchroinfo-journal

DETECTING AND COUNTERING MODERN ATTACKS

Dovletaly N. Nuryagdyyev [1], Vitaly B. Kreindelin [2]

[1] The Institute of Telecommunications and Informatics of Turkmenistan, Ashgabat, Turkmenistan;
97dowlet97@gmail.com

[2] Moscow Technical University of Communications and Informatics, Moscow, Russia;
vitkrend@gmail.com

ABSTRACT

The IT community's top priority has become the implementation of monitoring and active defense tools, including IDS, IPS, and integrated IDS platforms. This paper provides a detailed analysis of existing threats, with a particular emphasis on the destructive impact of zero-day attacks, which have become a critical problem for US cybersecurity. It examines the paradigm of network infrastructure protection using IDS/IPS (Intrusion Detection System/Intrusion Prevention System) tools against the backdrop of a qualitative change in cyberthreats. Analyzing modern challenges – from fileless infection methods to targeted APT (Advanced Persistent Threat) campaigns – the authors point to the exhaustion of the potential of standard signature analysis. The paper aims to find ways to improve the effectiveness of network traffic monitoring in the face of constantly evolving attacker tools.

DOI: 10.36724/2664-066X-2026-12-2-2-7

Received: 07.02.2026
Accepted: 10.04.2026

Citation: D.N. Nuryagdyyev, V.B. Kreindelin, "Detecting and countering modern attacks," *Synchroinfo Journal* **2026**, vol. 12, no. 2, pp. 2-7.

KEYWORDS: *Information security, IDS/IPS solutions, machine learning, network packet analysis, data security, intrusion prevention, cyber threats, behavioral analysis, network resiliency*.

Introduction

Current cybercrime statistics demonstrate a sharp increase in the number of large-scale breaches of confidential information, affecting thousands of organizations worldwide. Such incidents cause reputational and economic damage to a wide range of individuals, from ordinary consumers to major investors. Under these circumstances, the IT community has prioritized the implementation of monitoring and proactive defense tools, including IDS, IPS, and integrated IDS platforms. This paper provides a detailed analysis of existing threats, with a particular emphasis on the destructive impact of zero-day attacks, which have become a critical issue for US cybersecurity [1].

Logging and auditing functionality in the designed IPS system

The effectiveness of incident identification and subsequent analysis mechanisms in intrusion prevention systems (IPS) directly depends on the quality of the generated log files. Although various technological solutions (WIPS, NIPS, HIPS) (from English: Wireless Intrusion Prevention System, from English: Network Intrusion Prevention System, from English: Host Intrusion Prevention System) have their own specific data sets, there is a basic layer of information attributes common to most systems.

Within the proposed IPS model, key attention is paid to the following groups of parameters:

• Temporal determination: The use of precise timestamps allows for the construction of a strict chronology of the attack, which is necessary for the correct reconstruction of events.

• Session identification: Each network interaction (for example, within the TCP protocol) (from English: Transmission Control Protocol) is assigned a unique session ID. This simplifies the aggregation of disparate packets into a single data stream.

• Criticality Metrics: Differentiating incidents by threat and confidence (Impact/Confidence Scoring) allows automated systems to prioritize responses to the most dangerous anomalies.

• Network Attributes: Data collection includes identifying protocols used at different layers of the OSI (Open Systems Interconnection) model (transport, application, network), as well as recording the physical (MAC) and logical (IP) addresses of the sender and recipient. MAC address analysis can also serve as an additional tool for identifying the vendor of the attacked or attacking device.

• Byte-by-byte analysis (Deep Inspection): To ensure maximum transparency, IPS monitors the entire volume of transmitted content, analyzing every byte within the established connection.

The final element of the system's functionality is protective measures logging – recording active actions taken to block threats. This information is critical for assessing the quality of the chosen security strategy.

Centralization and storage of information

The solution implements a centralized data aggregation model. All incidents identified as confirmed threats (True Positive) are transferred to a single repository. This approach provides:

• Cross-platform correlation: the ability to correlate suspicious activity recorded simultaneously at the network (NIPS), wireless (WIPS), and host (HIPS) levels.

• Fault tolerance: the central database supports redundancy mechanisms, including cloud backup and the creation of identical mirror copies (cloning).

Data lifecycle and retention policies

The duration of data storage is directly related to the system's analytical potential and operating costs. The proposed architecture utilizes a two-stage approach:

1. Local storage: primary sensors and collection points retain information "onboard" for seven days.

2. Long-term archiving: after a week, the data migrates to a central storage facility, where it is accumulated for up to 12 months.

This extended planning horizon enables in-depth historical analysis (retrospective analysis) and the generation of high-quality security reporting over long periods.

Neighborhood Analysis-Based Anomaly Detection Methods

Within the proposed solution, anomaly identification is based on a geometric representation of the data. The primary implementation tool is a method used to process samples containing both normal and malicious traffic [2].

Method Rationale and Mechanics.

The choice of outlier detection is based on its ability to recognize threats not present in the training data. The algorithm operates according to the following principle:

1. Standard Determination: Clusters representing typical ("normal") network behavior are formed.

2. Distance Calculation: For each new event, the mathematical distance to the centroid of the corresponding cluster is calculated.

3. Threshold Filtering: If the obtained value exceeds the set limit, the object is marked as an anomaly.

Benefits for IDS Systems

The integration of this mathematical framework into the system's analytical core aims to reduce the rate of false positives. The main advantages of the method are:

• High performance: A small number of iterative calculations makes the approach ideal for analyzing data streams in real time.

• Adaptability: Resistance to minor fluctuations in network patterns and ease of software implementation.

• Detection flexibility: Unlike signature-based methods, this approach allows for the identification of previously unknown attack types (zero-day) without requiring their descriptions to be entered into a knowledge base [3].

Pattern Matching Method

In addition to anomaly detection algorithms, the IPS being developed includes a deterministic analysis module based on signature matching. This component operates by continuously verifying incoming packets for specific characteristics corresponding to known cyberthreats [4].

Operating principle

The algorithm accesses a structured repository containing pre-defined patterns of malicious activity. These patterns can range from single compromise markers to complex behavioral chains. If an identical pattern is detected in the current information flow, the system immediately generates an alert and activates attack blocking protocols.

Justification for the choice of method

The integration of a signature-based approach into the system's analytics stack is driven by three key factors:

1. High classification accuracy: This method minimizes the likelihood of type I and type II errors (False Positives/False Negatives). This avoids false alarms, eliminating the unnecessary consumption of computing power on processing non-existent incidents.

2. Performance: Using an optimized set of decision rules, the algorithm demonstrates high data processing speed, preventing network bottlenecks.

3. Informative reports: Thanks to detailed descriptions in the signature database, the security administrator receives comprehensive information about the type and vector of the current attack, significantly simplifying the response process [5].

Application of expert rules in the analytical core

The IPS mechanism is based on the (rule-based detection) continuous recording of system events and the subsequent generation of decision algorithms. These instructions serve as criteria for classifying network activity as legitimate or malicious. In modern practice, it is common to distinguish two main concepts: anomaly detection and intrusion

attempt identification. These two concepts, despite their differences, can complement each other within a single platform.

Specifics of rule-based anomaly detection

This method overlaps significantly with statistical analysis, but its distinctive feature is the formation of specific logical conditions ("rules") describing the normal state of the system. The implementation process includes the following steps:

• Analysis of historical data: Based on audit archives, consistent patterns of resource use by users, software systems, and network nodes are identified.

• Formalization of behavioral models: The identified patterns are converted into a set of rules describing standard work cycles.

• Comparative monitoring: The current activity of subjects is compared with accumulated historical patterns. Any significant deviation from the recorded "norm" is interpreted as a potential incident.

The effectiveness of such systems directly correlates with the size and quality of the rule base: the more detailed the behavioral profiles are described, the higher the accuracy of threat recognition.

Key features of the approach

• Contextual flexibility: The system is capable of identifying suspicious activity even when it formally fits within established use patterns. This is achieved by flagging specific system calls as potentially dangerous.

• Platform adaptation: Decision rules are designed taking into account the architectural features of specific nodes and the specific operating systems used, minimizing the likelihood of errors.

• Development methodology: The most effective way to build a rule base is through proactive analysis of exploits, hacking tools, and malicious scripts available in open and specialized sources. This allows the system to "know" the attacker's logic before an attack occurs.

Antivirus

Antivirus protection tools are a fundamental tool for identifying, blocking, and eliminating destructive software. Operating in the background, these solutions provide continuous monitoring of the operating environment, protecting not only user data but also the system's hardware resources. Modern products also include advanced functionality, such as web filtering and configurable firewalls [6].

Mechanics of interaction within the proposed IPS

In the designed intrusion prevention system, the antivirus component is installed directly on host computers. Its operation is based on the following principles:

• Signature verification: Software code is scanned for matches against global databases of known threats. Automated signature updates ensure up-to-date protection against the latest malware modifications.

• Reactive incident management: Upon receiving a signal from the IDS module about a detected intrusion, the antivirus software localizes the compromised objects. The system can automatically quarantine a suspicious file, restrict access to it, or completely delete it.

• Notification and auditing: Upon detection of virus activity, an instant notification is generated for the security administrator, allowing for prompt adjustment of the security policy.

The Importance of Maintenance

A key factor in the effectiveness of an antivirus module is the regularity of its intelligent database updates. Our model features a hybrid update scheme (manual and automatic), which is critical for maintaining a high level of security in the ever-changing cyberthreat landscape.

Advanced antivirus

Traditional antivirus solutions that rely on signature databases remain effective in blocking known threats, but they are ineffective against modern polymorphic attacks. Advances in endpoint protection are driven by the implementation of behavioral analysis, artificial intelligence (AI), and machine learning (ML) technologies. These tools enable the identification of malicious intent, not just searching for matches in file structures.

Intelligent analysis and preventive response

The use of AI (artificial intelligence) and ML algorithms is transforming the threat detection process:

• Behavioral monitoring: Systems detect anomalies in real time, which is critical for blocking zero-day exploits.

• Predictive classification: Predictive analytics methods enable new virus strains to be matched to known families based on common behavioral traits, increasing detection accuracy.

• Automated protection: The use of AI reduces response time through autonomous policy updates and instant suppression of malware activity.

Comparison of EDR, MDR, and XDR architectures

The modern cybersecurity landscape is represented by three key concepts being implemented by leading vendors (Kaspersky, CrowdStrike, FireEye, etc.):

1. EDR (Endpoint Detection and Response): Focuses on continuous event monitoring on specific nodes. In addition to blocking, EDR (Endpoint Detection and Response) provides forensic analysis tools, allowing for detailed reconstruction of the incident chronology.

2. MDR (Managed Detection and Response): This is a service model that combines tools (SIEM (Security Information and Event Management), EDR, and traffic analysis) with the expertise of external specialists. This is the optimal solution for organizations experiencing a shortage of in-house information security resources.

3. XDR (Extended Detection and Response): The highest level of security system evolution. XDR integrates data from various environments – network, clouds, and endpoints – providing intelligent event correlation and automatic suppression of false alarms.

Quarantine

The designed intrusion prevention system is based on a hybrid protection model integrating antivirus modules with object isolation and backdoor countermeasures [2].

The system's operational cycle is structured as follows:

1. Isolation and Initial Containment

If malicious code is identified, the IPS immediately blocks the threat, moving the destructive object to a dedicated secure storage area (quarantine). This measure helps stop the spread of an attack at an early stage and minimize damage to the infrastructure [8, 9].

2. Recursive Scanning

After initial threat containment, the antivirus component initiates a deep inspection of the entire system. The goal of this stage is to find hidden attack vectors or secondary malicious modules that may have been introduced during the incident. If correlated threats are detected, they undergo a similar isolation procedure. If there are no signs of compromise, the system is assigned the status of "verified security."

3. Notification and Feedback

To maintain transparency in security management processes, a notification subsystem has been implemented. The IPS generates detailed reports sent to administrators and users via secure communication channels (email). Notifications contain:

• The type and severity of the recorded incident;

• A history of security events;

• A list of automated measures taken to neutralize the threat.

Conclusion

The study confirms that intrusion detection and blocking systems (IDS/IPS) remain a critical component of a defense-in-depth strategy. However, the dramatic change in the cyber threat landscape and the widespread adoption of cryptographic protocols necessitate a transformation of traditional security paradigms.

Key Findings and Development Prospects

Shift in Technological Focus: Traditional signature-based analysis is losing its effectiveness against dynamic attack vectors. The IDS/IPS development vector is shifting toward intelligent analysis based on machine learning and AI. This enables a shift from reactive searches for known matches to proactive identification of hidden patterns and anomalous behavior.

System Integration and Synergy: Using IPS in isolation is becoming impractical. Modern security architecture requires tight convergence of security tools within unified platforms (XDR, SIEM, SOAR). XDR (Extended Detection and Response)

SIEM (Security Information and Event Management)

SOAR (Security Orchestration, Automation, and Response).

This integration provides end-to-end visibility into the infrastructure and enables threat intelligence mechanisms for the rapid exchange of data on current threats.

Adaptation to encapsulated traffic: Extensive use of TLS/SSL protocols. TLS (Transport Layer Security)

SSL (Secure Sockets Layer) creates significant obstacles to deep packet inspection (DPI). The optimal solution to this contradiction between privacy and security seems to be the transition to the analysis of network session metadata, which allows for the identification of signs of compromise without violating the integrity of encrypted communication channels [7, 10, 11].

REFERENCES

[1] K. Scarfone, Guide to Intrusion Detection and Prevention Systems (IDPS). NIST Special Publication 800-94. Washington: National Institute of Standards and Technology, 2024 (updated). 120 p.

[2] X. Chen, “Intrusion Detection and Prevention Systems: Hybrid Models and Isolation Mechanisms,” *Journal of Cybersecurity and Information Management*, 2018. Vol. 12, no. 4, pp. 45–58.

[3] V. I. Averchenkov, Intrusion Detection Systems: A Textbook for Universities. 3rd ed. Moscow: Flinta, 2022. 145 p.

[4] Yu. S. Vasiliev, “Machine Learning in Information Security Problems: Anomaly Detection Methods,” *Information Technology Security*. 2021. No. 2, pp. 88-101.

[5] E. Tanenbaum, D. Weatherall, Computer Networks. 6th ed. St. Petersburg: Piter, 2023. 992 p.

[6] Kaspersky Lab. Modern Cyber Threat Landscapes: EDR, MDR, and XDR Solutions / Kaspersky Lab: official website. URL: https://www.kaspersky.ru/enterprise-security/endpoint-detection-response (accessed: 27.01.2026).

[7] V. F. Shan'gin, Computer Information Protection. Effective Methods and Tools. Moscow: DMK Press, 2020. 544 p.

[8] V. B. Kreindelin, N. A. Legkov, “Protecting Authentication Data for Websites and WEB Applications,” *Telecommunications and Information Technology*. 2022. Vol. 9, No. 1, pp. 6-10.

[9] V. G. Olifer, N. A. Olifer, Computer Networks. Principles, Technologies, Protocols: Textbook for Universities. St. Petersburg: Piter, 2020. 992 p. (in the context of network infrastructure security).

[10] V. B. Kreindelin, G. A. Vakhromeev, “The Most Effective Machine Learning Algorithms for Risk-Based Authentication Systems,” *Telecommunications and Information Technology*. 2024. Vol. 11, No. 1, pp. 87-92.

[11] M.G. Bakulin, T.B.C. Ben Rejeb, V.B. Kreyndelin, D.Y. Pankratov, A.E. Smirnov, “Code domain NOMA in 3GPP specifications: 5G or 6G?,” *T-Comm*. 2022. vol. 16, no.1, pp. 4-14. DOI: 10.36724/2072-8735-2022-16-1-4-14.

SYNCHROINFO JOURNAL

www.media-publisher.eu/synchroinfo-journal

COMPLEX SIGNAL DETECTION AND VECTOR-MATRIX MULTIPLICATION ALGORITHM

Wu Shi Dao [1]

[1] Vietnam National University, Hanoi, Vietnam

ABSTRACT

The problem of joint detection and estimation of carrier frequency parameters and time delays of a low-power noise-like complex signal (NCS), its several copies mismatched in frequency and time delay, or noise-like signals of different structure, is relevant for a number of radio systems, since its solution can be used for time and frequency synchronization in information transmission channels, positioning in radio navigation systems, summation of signals during their multipath propagation or radiation by spaced repeaters, detection of all ground stations using a satellite constellation for the purpose of frequency resource monitoring, etc. The objective of the work is to improve the efficiency of digital algorithms for detecting low-power noise-like NCS, as well as to analyze the joint operation of the corresponding devices with loop circuits for tracking changes in signal parameters at a given accuracy of their final estimation in a multi-stage parallel-sequential detection and synchronization procedure, as well as to develop a unified synchronization quality criterion for a radio system. The subject of the research is digital algorithms for accelerated vector-matrix multiplication applied to the problem of detecting a set of noise-like signals; a multi-stage parallel-sequential procedure for detecting and synchronizing noise-like signals using digital synchronization devices (PSP) and analog loop circuits.

KEYWORDS: *noise-like signals, vector-matrix multiplication, Rademacher functions, Walsh-Hadamard system, complex signals*.

DOI: 10.36724/2664-066X-2026-12-2-8-25

Received: 30.01.2026
Accepted: 02.04.2026

Citation: Wu Shi Dao, "Complex signal detection and vector-matrix multiplication algorithm," *Synchroinfo Journal* **2026**, vol. 12, no. 2, pp. 8-25.

Licensee IRIS, Vienna, Austria.

Introduction

The problem of joint detection and evaluation of the parameters of carrier frequencies and time delays of a weak-power noise-like complex signal (NLC), several of its copies mismatched in frequency and time delay, or noise-like signals of different structure, is relevant for a number of radio systems, since its solution can be used for synchronization in time and frequency in information transmission channels [1-5], positioning in radio navigation systems [6-9], summation of signals during their multipath propagation or radiation by spaced repeaters [8, 10-13], identification of all ground stations using a satellite constellation for the purpose of monitoring the frequency resource [13, 14], etc.

The detection (search) of weak noise-like signals is usually performed by long-term accumulation of their energy in the receiver [11, 6], since the signal-to-noise ratio by power at its input can be (-10 ... -40) dB, and for unknown frequencies and time delays of the received noise-like signals, its initial accumulation is usually performed using a set of correlators (Cor) or matched filters (MF) [15, 16], at the outputs of which two-dimensional correlation functions (DCF) [13, 15, 17] of the received noise-like signals or their fragments are formed. In what follows, we will consider weak noise-like signals that provide a signal-to-noise ratio by power at the receiver input in the above-mentioned range of values.

However, it should be emphasized that there is a significant limitation on the duration of the accumulation time of the noise-like signals using Cor or MF in case of the need to process the received noise-like signals with large baselines and a significant width of the region of their frequency uncertainty. The main reason for this limitation is the significant technical difficulties in the manufacture of the above-mentioned devices. As a result, the detection time of weak-power SLS can be several tens of seconds or even minutes with sequential restructuring of their detection devices by frequency [6, 10, 11].

In many cases, the Cor or SF are considered only as devices used to improve the reliability of the subsequent post-detector energy detector SLS [18, 19], in which the energy of the required number (up to several tens or even hundreds) of SLS fragments is accumulated [1, 4]. This circumstance leads to a significant decrease in the accuracy of estimating the parameters of these signals in the device for their detection, as well as the efficiency of distinguishing their mismatched copies, which is determined mainly by the size of the projection(s) of the main peak(s) of the SLS DCF onto the frequency-time plane, that is, by the characteristics of the first energy accumulation unit SLS, including a set of Cor or SF.

The subsequent energy accumulator will only ensure the accuracy of estimating the SLS parameters, corresponding to the size of this projection, with the required reliability [12, 20]. The increase in the efficiency of devices for detecting pseudorandom sequences (PRS) is associated with the development of digital algorithms for their processing [2, 3, 21, 22], which are reduced to performing the operation of discrete convolution of the pseudorandom sequence (PRS) on the basis of which it is formed, or, ultimately, the operation of vector-matrix multiplication. The limitation on the length of the PRS, the convolution of which can be performed in such a device, is associated only with the high computational complexity of the corresponding algorithm, since the problem of instability of the PRS clock generators is solved by re-sampling the input PRS with a time shift of half the duration of its elementary pulse [23], and the instability of its carrier frequency and its

Doppler shift lead only to the need for multiple repeated calculations of the discrete convolution of the PRS [14, 24].

A more accurate assessment of the parameters of the signal-to-noise ratio for the operation of a quasi-coherent receiver can be made in devices for tracking changes in these parameters in phase-locked loop (PLL) systems and automatic time control (ATC) devices [10, 20, 22, 25, 26]. That is, detection of the signal-to-noise ratio can be used to bring the devices for tracking the parameters of already detected signals to the working areas of the discriminatory characteristics of these tracking devices [20].

The scientific objective of this paper is a comprehensive examination and optimization of the procedure for jointly detecting and estimating the parameters of sets of low-power noise-like signals based on the criteria of the duration of the correct estimation of their carrier frequencies and time delays with predetermined errors and probabilities.

The problem formulated above includes a set of subproblems, the solution of which constitutes the content of this work. One of these is the justification of the choice of M-like PRS for the formation of SLSs, which are reduced to special orthogonal functions, in systems of which fast vector-matrix multiplication algorithms can be constructed based on the fast Walsh-Hadamard transform.

Previous research in this area

Significant advances in the use of fast spectral transforms in the basis of Vilenkin-Chrestenson functions and, in particular, Walsh-Hadamard in processing discrete signals were achieved in the works of V.V. Losev, V.D. Dvornikov, Y. Be'eny, K. Leung, J. Snyders, P. Li, V.M. Smolyaninov, L.E. Nazarov, and L.M. Finck [9, 7, 15, 16, 27]. In [9], group discrete multiplicative signals were proposed for the first time, their relationship with group codes was revealed, and it was shown that the optimal rule for their recognition is based on spectral analysis, the implementation of which can use fast spectral transforms. In [7, 15, 27, 28], methods for using these transforms in the theory of error-correcting coding were developed. In relation to the problem of decoding p-ary codes of maximum length, the use of fast spectral transformations in the discrete basis of Vilenkin-Chrestenson functions was considered in [12], and directly for synchronization of PRS – in [4, 9]. Also, in [4] the relationship is indicated between the problems of searching (synchronizing) SLCs during their processing in the receiver and decoding block codes constructed on the basis of cyclic shifts of their words.

For fast decoding of a code based on fast spectral transforms, it is necessary to know the method for converting its words to discrete Vilenkin-Chrestenson functions, or, when using binary codes, to Walsh functions [29]. In the case of solving the problem of code synchronization, any of its cyclic shifts must be converted to these functions [7, 9]. However, in [7 ,9, 13], the diversity of options for converting cyclic shifts of the MP to discrete Walsh functions was not identified, caused by both the diversity of multiplicative groups of the extended Galois field and the use of their cyclic shifts in such a reduction. Knowledge of such diversity makes the MP synchronization algorithm more flexible and allows us to reduce its computational complexity in certain situations, which are indicated in this dissertation. In addition, when solving the problem of synchronizing the PSP with large repetition periods, the method of identifying the correspondence between the row numbers of the Walsh-Hadamard matrix and the initial blocks of cyclic shifts of the MP, that is, in the matrix interpretation of this problem – the rows of the circulant matrix of the MP, which can

be constructed in different ways, which is not considered in the works of the above-mentioned authors, becomes important.

The problem of fast synchronization of noise-like SLS, formed on the basis of Gold's PRS [8, 30-34], currently used in many radio systems, including satellite radio navigation, has not been solved. In the works of V.Yu. Mikhailov and R.B. Mazepa, devoted to this problem [33, 34], Gold's PRS, formed using the binary subclass of Gordon-Mills-Welch sequences (GMW-sequences) [7], are considered, which do not exist for N = 2^m-1, where m = 5, 7, 11, 13, 17, …. Taking into account that Gold's PRS for m = 8,12,16 are absent, it can be concluded that the method of synchronization of Gold's PRS, proposed in these works, can be applied to PRS of only four lengths, used in practical applications at present - 511,1023,16283,32567. The main problem of this approach, also used in earlier works [7, 9], but only in relation to GMV sequences, is the increase in the level of the side peaks of the normalized periodic autocorrelation functions (PACF) [4] of short PRS, to which the original longer PRS is transformed, in relation to the central peak of the normalized PACF, which is unchanged in magnitude.

Detection and discrimination of noise-like complex signals

Let the input of the receiver contain P additive copies of the same signal generated by binary phase-shift keying (PSK) of its carrier frequency; this signal over the duration of its repetition period is described as

$$s(t) = \sum_{i=0}^{N-1} d_i S_0(t - iT_e) cos(2\pi f_0 t), \quad (1)$$

where *N* is the repetition period of the binary PRS, $d_i \in \{-1,1\}$ are its elementary symbols, $i = 0,1,\dots,(N-1)$ is the symbol number, $S_0(t)$ is the shape function of the elementary pulse of the SLS with duration T_e, f_0 is its carrier frequency. A rectangular shape of the elementary pulses of the SLS is often considered when

$$S_0(t) = \begin{cases} 1 & if \quad t \le T_e \\ 0 & if \quad t > T_e \end{cases}.$$

In the general case, these copies differ from each other by unknown time delays, the values of the frequencies of their carrier oscillations, and the initial phases of the oscillations of these frequencies. Accordingly, for *P* = 1, the signal-to-noise ratio at the receiver input is described as $s(t - t_1 - \tau_1, f_1 - \Delta f_1, \Delta\varphi_1)$, where τ_1 and Δf_1 are unknown, relatively slow shifts in the time delay and carrier frequency of a given signal-to-noise ratio relative to the constants and known values t_1 and $\Delta\varphi_1$, and Δφ_1 is a random shift in the initial phase of the signal-to-noise ratio's carrier frequency oscillation relative to the conditionally zero shift of this phase.

In accordance with the maximum likelihood criterion, the joint detection and estimation of the parameters of the SLS at *P* =1, that is, the estimation of its time shift $\widehat{\tau_1}$, frequency $\widehat{\Delta f_1}$ and frequency phase $\Delta\varphi_1$ relative to t_1, f_1 and zero phase shift against the background of additive white Gaussian noise corresponds to the algorithm [12]:

$$\widehat{\tau_1}, \widehat{\Delta f_1}, \widehat{\Delta\varphi_1} = \underset{\tau,\Delta f,\Delta\varphi}{arg\max}(Re\left[\dot{Z}(\tau, \Delta f, \Delta\varphi) + \xi\right]), \quad (2)$$

where ξ is the additive noise component at the input of the decision device (DD),

$$\dot{Z}(\tau, \Delta f, \Delta\varphi) = e^{j\,\Delta\varphi}\dot{\chi}(\tau, \Delta f), \quad (3)$$

$$\dot{\chi}(\tau, \Delta f) = \frac{1}{E_{1T_{\text{нак}}}}\int_0^{T_n} \dot{S}(t)\dot{S}^*(t-\tau)e^{j2\pi\Delta f t}dt \; - \quad (4)$$

complex DCF of the SLS [7], $\dot{S}(t)$ is its complex envelope, E_{1T_n} is the value of the SLS energy accumulated over time T_n. Thus,

$$\widehat{\tau_1}, \widehat{\Delta f_1}, \widehat{\Delta\varphi_1} = \underset{\tau,\Delta f,\Delta\varphi}{arg\max}(Re[e^{j\Delta\varphi}\dot{\chi}(\tau, \Delta f, \Delta\varphi)]. \quad (5)$$

It is further taken into account that the estimate of Δφ is uninformative and complicates the process of estimating the frequency and time delay, as a result of which in (2) instead of the real part of the function $\dot{Z}(\tau, \Delta f, \Delta\varphi) + \xi$, its modulus is usually considered, that is, $\left|\dot{Z}(\tau, \Delta f, \Delta\varphi) + \xi\right| = \left|\dot{Z}(\tau, \Delta f, \Delta\varphi)\right| + \xi_1$, where the interference component ξ_1 is distributed according to the Rayleigh-Rice law. Then (5) can be rewritten as:

$$\widehat{\tau_1}, \widehat{\Delta f_1} = \underset{\tau_1,\Delta f_1}{arg\max}(|\dot{\chi}(\tau, \Delta f, \Delta\varphi)| + \xi_1). \quad (6)$$

At the outputs of the low-pass filters (LPF) of the quadrature channels of the SLS detector, the functions $Re\left[\dot{S}(t)e^{j(2\pi\Delta f t+\Delta\varphi)}\right] = \cos\Delta\varphi Re\left[\dot{S}(t)e^{j2\pi\Delta f t}\right]$ and $Im\left[\dot{S}(t)e^{j(2\pi\Delta f t+\Delta\varphi)}\right] = \sin\Delta\varphi Im\left[\dot{S}(t)e^{j2\pi\Delta f t}\right]$, are extracted, where Δf and Δφ are the values of the unknown differences between the carrier frequency of the received SLS and the reference frequency of the quadrature receiver f_1, as well as their initial phases, respectively. Then, according to (4), two convolutions of each of them with $\dot{S}^*(t)$, which in this case is a real function, are calculated separately.

The results presented below were published by the author of this dissertation in [20, 22]. The form of $|\dot{\chi}(\tau, \Delta f, \Delta\varphi)| = |\dot{\chi}(\tau, \Delta f)|$ when forming a signal-to-noise ratio based on a magnetic field with $N_e = 1023$ in the case of a rectangular shape $S_0(t)$ is shown in Figure 1. In this case, the ranges of variation of the parameters τ and Δ*f* correspond to the width of the interval of the uncertainty region of the received signal-to-noise ratio in time T_s and frequency *F*, respectively, where T_s is the duration (repetition period) of the signal; F is the width of the uncertainty region in frequency. Within each of these intervals, there are indistinguishable values of any of the parameters from the point of view of its evaluation. The number of distinguishable discrete values of the parameter τ is determined as

$n_в = T_s / \Delta\tau$, and the number of distinguishable values of the parameter Δ*f* is determined as $n_{ch} = F / \Delta f_i$, where $\Delta\tau, \Delta f_i$ are the sampling periods of the SLS in time and frequency.

The selected sampling periods are twice as large as the periods corresponding to Kotelnikov's theorem. In this case, $\tau = zT_э$ $(z = -n_в, \dots, -1,0,1 \dots, n_в)$ is the shift of the reference signal's pseudorandom frequency relative to the pseudorandom frequency of the received signal, $\Delta f = \frac{\gamma}{T_s}$ $(\gamma = -n_ч, \dots, -1,0,1 \dots, n_ч)$ is the shift of the reference signal's carrier frequency relative to the frequency of the received signal. If the pseudorandom frequency of the received signal shifts to the left relative to the pseudorandom frequency of the reference signal, then *z* takes on negative values, otherwise it takes on positive values. Accordingly, shifts of the received signal's carrier frequency towards values lower or higher than the frequency of the reference signal are possible. The origin of the coordinate system in this figure corresponds to the coinciding values of the delay time and frequency of the received signal and the reference signal.

Figure 1 shows the discrete function $\left|\dot{\chi}\left(zT_e, \frac{\gamma}{T_s}\right)\right|$ of dimensionless z and γ, the values of which are connected by continuous lines corresponding to the form of the function $|\dot{\chi}(\tau, \Delta f)|$ between adjacent points of the discrete function corresponding to it. Also shown in this figure are the sections of the DCF along the time axis $|\dot{\chi}(zT_e, 0)|$ and along the frequency axis $\left|\dot{\chi}\left(0, \frac{\gamma}{T_s}\right)\right|$. The first zero values of $|\dot{\chi}(zT_e, 0)|$ are achieved at $z = \pm 1$, as a result of which the width of the section of the main peak of the DCF in time is $2T_e = 2/f_T$, from which it follows that the accuracy of estimating the delay time of the SL increases with an increase in the width of its spectrum, where $f_T = 1/T_e$ is the clock frequency of the SL. At the same time, as follows from (1.4), the width of the cross-section of the DCF of the frequency axis is determined by the values $\gamma = \pm 1$, at which $\left|\dot{\chi}\left(0, \frac{\gamma}{T_s}\right)\right| = 0$, therefore the width of the DCF along the frequency axis will be $2/T_s$, and $T_s = T_n = T_e N$, where *N* is the number of elementary pulses of the SLS, the energy of which is accumulated in the receiver.

Thus, with increasing N, the accuracy of the SLS frequency estimation also increases. It is generally believed that if $\Delta f_1 > 1/3T_n$, then the probability of detecting the SLS is low, since in this case the level of the useful signal at the RU input, corresponding to the DCF value, is significantly less than its maximum possible value [12, 17]. That is, for large values of Δf_1, long-term accumulation of the SLS energy in the convolution device is meaningless, but for relatively small T_n, the accumulated energy may be insufficient to detect the SLS with the required reliability. Therefore, it is necessary to reconfigure the reference frequency of the quadrature receiver with a step of $1/3T_n$ in the uncertainty region of the received SLS in frequency with a repeated calculation of the DCF.

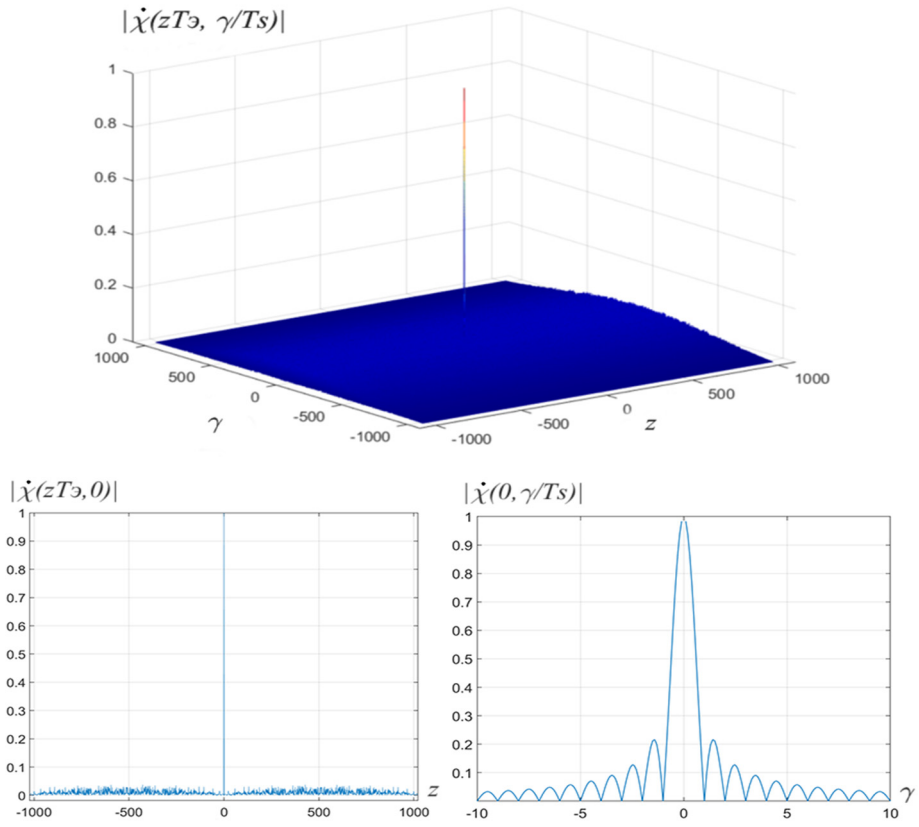


Figure 1. Typical view of the DCF module of the SLS at N_e = 1023 and its cross-sections in time and frequency.

Detection of a signal-to-noise ratio (SIR) also involves the simultaneous measurement of its frequency and delay time parameters with an accuracy corresponding to the cross-sectional dimensions of its DCF main peak. That is, two adjacent values of any parameter can be considered indistinguishable if the difference between them is less than the cross-sectional width of the central DCF peak. As a result, any of the SIR parameters under consideration can be considered discrete. When discretizing a SIR, the values of $\Delta\tau$ and Δf_i and should be selected in accordance with Kotelnikov's theorem; that is, when selecting signal sampling intervals in time and frequency in accordance with the dimensions of the main DCF peak, they will be twice the signal sampling interval recommended by this theorem. Then, if the width of the spectrum is equal to ΔF_s, and the duration of the accumulation time of its energy is equal to the period of its repetition, then $\Delta\tau \approx 1/\Delta F_s$, and $\Delta f_и \approx 1/T_s$. If we take into account that for $\Delta F_s \approx 1/T_e$, then we can estimate the total number of analyzed intervals of the uncertainty region by frequency and delay $n_{v,ch} = n_v n_{ch}$.

Figure 2 shows a time-frequency plane in which the uncertainty region of the SLS parameters – delay time and frequency – Is bounded by a rectangle.

The uncertainty region of the parameters is divided by a grid into rectangular cells with sides of $\Delta\tau$ and Δf_i The total number of cells is $n_{v,ch}$.

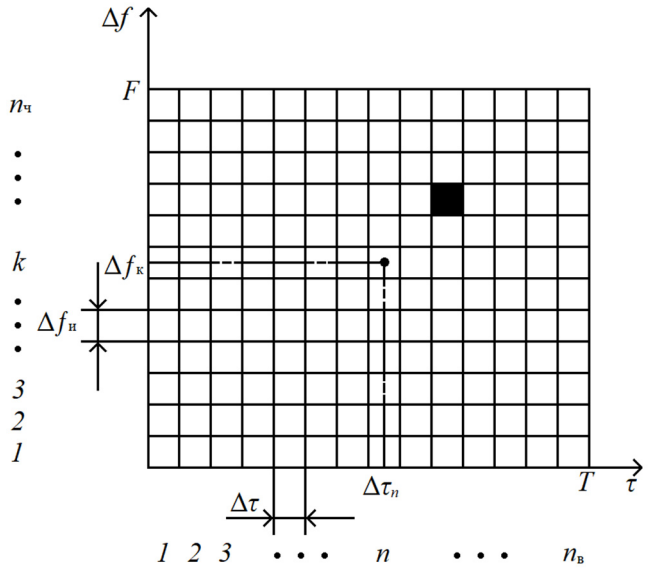


Figure 2. The uncertainty region of the parameters of the SLS.

The area of each of them is approximately equal to the area of the central peak of the DCF of the SLS, that is, each cell can accommodate only one central peak of the DCF. Therefore, the grid defines the boundaries between the recognized parameter values, and the parameters themselves can take any values from their total number n_v and n_{ch}. Thus, the discrete values of the SLS parameters can be numbered and designated as τ_n, where $n = 1, \ldots, n_v$ and Δf, where $k = 1, \ldots, n_{\text{ch}}$. In Figure 3, the shaded cell corresponding to the parameter values of the received SLS is highlighted.

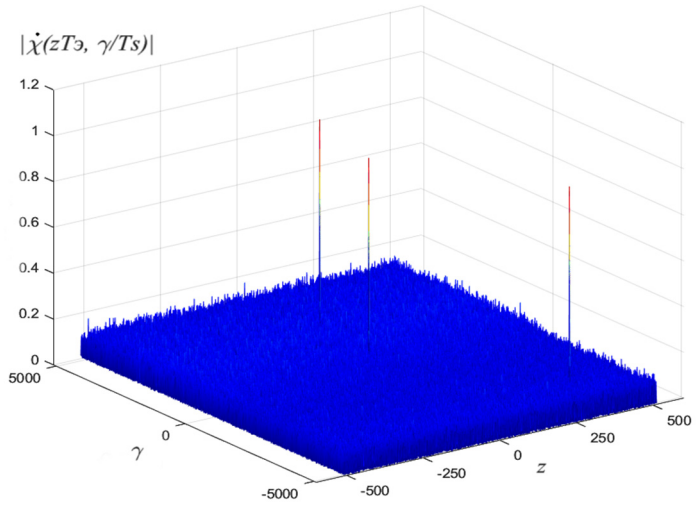


Figure 3. The DCF module of three copies of the SLS, shifted relative to each other in frequency and time delay and formed on the basis of the Gold PSP with N_e = 511.

Thus, the structural diagram of a device implementing the maximum likelihood estimate of the frequency and time delay of the SLS can be represented as a set of quadrature correlators. The output signal of the correlators after calculating the absolute values of their responses will be the absolute value of the SLS DKF $|\dot{\chi}(\tau, \Delta f)|$ (up to a factor corresponding to the signal energy and the additive noise component), whose values for discrete τ_n and Δf_k will appear simultaneously at the correlators' output. A decision unit (DU), which is a maximum selector, is then used. In the latter, the values of the correlators' responses are compared and the maximum one is selected. The reference signal parameters of the correlator with the largest output response are output as the maximum likelihood estimate of the signal frequency and time delay.

In practice, the phase-shift keyed signal generator (PSG) can be implemented as an analog device. Surface acoustic wave (SAW) devices are often used to construct phase-shift keyed signal generators (PSGs) [5], but due to limitations associated with their manufacturing technology (limited substrate sizes), they can process SAGs with a base of no more than 512 or 1024 with a sequential arrangement of two substrates.

When detecting *P* additive copies of the same signal, mismatched in frequency and time delay, the value of T_нак should be selected such that within any frequency band $[f_1 - 1/3T_n, f_1 + 1/3T_n]$, $[f_2 - 1/3T_n, f_2 + 1/3T_n]$,..., $[f_P - 1/3T_n, f_P + 1/3T_n]$ there is only one copy of the received signal with an unknown time delay, or a set of signal with the same carrier frequencies and different time delays. In this case, the nonlinear transformation in calculating $|\dot{\chi}(0, \Delta f)|$ will not lead to the appearance of significant mutual interference between copies of the same SLC, since at each moment in time only one SLC is subject to the nonlinear transformation, and mutual interference is minimized by choosing the value of T_n [1]. Figure 3 shows the form of the DCF of the group SLC for *P* = 3.

Vector-matrix multiplication in detection of noise-like signals

Digital processing of the signal in a detection device involves extracting its complex envelope and then sampling it in time at a clock rate of $f_T = 1/2T_e$. This means that for each elementary pulse of the signal, there are two samples, shifted relative to each other in time by $T_e/2$. However, the two groups of signal samples, each obtained by sampling in time at intervals of duration T_e, must be processed separately – each in its own digital device, and the decision to detect the signal should be made based on the maximum response of the two devices.

It should be noted that the doubled signal sampling frequency does not exactly correspond to the received signal's clock frequency, equal to $2f_T$, due to the instabilities of the master oscillators on both the transmitting and receiving sides. Furthermore, at the SSC detection stage, its clock synchronization has not yet been achieved. As a result, after a certain period of time, a slip will inevitably occur; that is, two SSC samples, when

sampled at a time interval of T_e, will fall on the same elementary pulse, or one such pulse will be missed. However, due to the sample shift by $T_e/2$, a slip will never occur simultaneously at the inputs of two subsequent digital SSC processing devices. Nevertheless, the SSC processing time in these devices should not exceed the time between two consecutive slips, which is easily estimated from the instability of the master clock oscillators on the transmitting and receiving sides. So, if $\frac{\Delta f_T}{f_T} = 10^{-4}$, then it is easy to calculate that the duration of the PSP that can be processed in each of the digital devices should not exceed approximately 5000.

Omitting the obvious intermediate calculations and simplifications [6, 10-12], we will describe a digital algorithm for the joint detection and estimation of the parameters of a set of SLS: from the outputs of the low-pass filters (LPF) of the in-phase and quadrature channels of the receiver, analog-to-digital converters (ADC) are used in order to obtain discrete readings of the functions $Re\left[\dot{S}(t)e^{j(2\pi\Delta ft+\Delta\varphi)}\right] = \cos\Delta\varphi Re\left[\dot{S}(t)e^{j2\pi\Delta ft}\right]$ and $Im\left[\dot{S}(t)e^{j(2\pi\Delta ft+\Delta\varphi)}\right] = \sin\Delta\varphi Im\left[\dot{S}(t)e^{j2\pi\Delta ft}\right]$ at a sampling frequency of $f_T = 1/T_e$. As a result, discrete periodic signals X_1 and X_2 are formed. After re-sampling with the same clock frequency, but with a time shift of $T_e/2$, discrete signals X_3, X_4 are obtained [4]. Next, it is necessary to calculate four discrete convolutions, which in the matrix interpretation are described as: $\mathfrak{Ж}_{ц(1,-1)}\boldsymbol{X}_{1N}$, $\mathfrak{Ж}_{ц(1,-1)}\boldsymbol{X}_{2N}$, $\mathfrak{Ж}_{ц(1,-1)}\boldsymbol{X}_{3N}$, $\mathfrak{Ж}_{ц(1,-1)}\boldsymbol{X}_{4N}$, where $\mathfrak{Ж}_{ц(1,-1)}$ is the circulant matrix of the PRS used in the formation of the SLC of dimension N×N in the alphabet (1,-1), and $\boldsymbol{X}_{1N}$, $\boldsymbol{X}_{2N}$, $\boldsymbol{X}_{3N}$, $\boldsymbol{X}_{4N}$ are vectors that are segments of the discrete functions $\boldsymbol{X}_1$, $\boldsymbol{X}_2$, $\boldsymbol{X}_3$, $\boldsymbol{X}_4$ of length *N*, respectively. In the RU, a decision is made on the number of detected SLS and the time shifts of their PSP relative to its conditionally zero cyclic shift after calculating $\sqrt{(\mathfrak{Ж}_{ц(1,-1)}\boldsymbol{X}_{1N})^2 + (\mathfrak{Ж}_{ц(1,-1)}\boldsymbol{X}_{2N})^2}$ and $\sqrt{(\mathfrak{Ж}_{ц(1,-1)}\boldsymbol{X}_{3N})^2 + (\mathfrak{Ж}_{ц(1,-1)}\boldsymbol{X}_{4N})^2}$. The carrier frequencies of all detected SLCs will be in the frequency range $[f_1 - 1/3T_n, f_1 + 1/3T_n]$, $T_n = NT_e$,, where f_1 is the carrier frequency of the reference SLC used to extract the complex envelope. Then, it is necessary to change the reference frequency of the quadrature receiver by $1/3T_n$ and repeat the calculations described above. To detect all SLC copies mismatched in frequency and time delay, it is necessary to either sequentially reconfigure the reference frequency of the quadrature receiver with a step of $1/3T_n$, or to generate reference frequencies in parallel with the same step, covering the uncertainty region of the SLC in frequency during parallel calculation of convolutions.

Thus, the basis of the optimal algorithm for detecting and distinguishing SLS is the procedure of synchronization of the PRS, on the basis of which it is formed. This procedure can be described as the multiplication of the circulant matrix of the PRS $\mathfrak{Ж}_{ц(1,-1)}$,, the rows of which represent all of its possible cyclic shifts, by the vector X_N, obtained from the input of the receiver and containing one of the rows of this matrix, with subsequent determination of the number of the maximum component of the obtained vector. Obviously, this algorithm corresponds to the matrix form of the discrete convolution operation of the PRS, the result

of which we will call its PACF [5, 10]. The order of cyclic shifts of the PRS in the rows of the matrix $\mathfrak{I}_{\text{ц}(1,-1)}$, as a rule, is not of fundamental importance [7, 9, 29]. In what follows, we will consider the MP and Gold's PRS, which are widely used at present in many radio engineering systems [6, 10, 11]. As shown below, a fast algorithm for multiplying $\mathfrak{I}_{\text{ц}(1,-1)}$ and any of its rows transposed into a column using the fast Hadamard transform (FHT) depends not only on the choice of the PSP, but also on the way this matrix is constructed.

Fast spectral transforms in the Walsh-Hadamard basis and detection of complex signals

As shown in the previous section, the algorithm for detecting a signal is reduced to digital vector-matrix multiplication, the computational complexity of which is proportional to the length of the square of the sequence of sequences on the basis of which the signal is formed, which significantly complicates its software implementation. Therefore, to generate such signals, it is advisable to use sequences of sequences that are reduced to special orthogonal functions, in systems of which fast algorithms for vector-matrix multiplication can be constructed [6, 29]. In what follows, we will consider the Walsh-Hadamard system as the initial system of orthogonal functions.

Rademacher functions and the Walsh-Hadamard system

Any discrete Rademacher system of N-th order is described by the formula:

$$r_i(x) = (-1)^{x_i} = cos\pi x_i, \qquad (7)$$

where $r_i(x)$ is the Rademacher function, $x = 0,1,\dots,(N-1)$ is its integer argument, $i = 1,2,\dots,m$ is the function number in the Rademacher system, $m = log_2 N$ is the system volume, $x_i \in \{0,1\}$ are the values of the *i*-th digit of the binary representation of *x*. Thus, the Rademacher system for *m* = 4 is a 16th-order system. It consists of four functions: $r_1(x) = 11111111 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1$, $r_2(x) = 1111 - 1 - 1 - 1 - 111 \quad 11 - 1 - 1 - 1 - 1$, $r_3(x) = 11 - 1 - 111 - 1 - 111 - 1 - 111 - 1 - 1$ and $r_4(x) = 1 - 11 - 11 - 11 - -11 - 1$. If a number x varies from 0 to (N-1), then the value of any digit x_i of its binary representation changes periodically with a period of $2^{N/2}$. Consequently, any Rademacher function is periodic, and exactly 2^{i-1} of its periods fit on an interval of length *N*. Furthermore, it is obvious that the Rademacher functions in any system are orthogonal and odd, as a result of which they can be used to decompose only odd discrete signals, i.e., the system is not complete.

Any complete orthogonal system of Walsh functions of order *N* can be obtained from the corresponding Rademacher system of the same order. In particular, the Walsh-Hadamard system can be obtained by the rule:

$$had(h,x) = \prod_{i=1}^{n}[r_i(x)]^{h_i} = [r_1(x)]^{h_1}[r_2(x)]^{h_2} \dots [r_n(x)]^{h_n}, \quad (8)$$

where $had(h,x)$ is the Walsh function, $h = 0, \dots, (N-1)$ is its number in the Walsh-Hadamard system, and $h_1, h_2, \dots, h_n$ are the digits of the binary representation of h (h_n - is the least significant digit). Thus, the volume of the complete Walsh-Hadamard function system A_m is *N*, and the matrix A_m describing this system contains N rows. Its rows with numbers $y = 2^v, v = 0,1,2, \dots, 2^{m-1}$ contain Rademacher functions, since in this case the binary representation of *y* contains a unity in only one digit.

Otherwise, the Walsh-Hadamard matrix A_m of order *N* is defined as the m-th Kronecker power of the second-order 2x2 Hadamard matrix:

$$A_m = A_2^{[m]}, \quad (9)$$

where

$$A_2^{[m]} = A_2^{(1)} \times A_2^{(2)} \times \dots \times A_2^{(i)} \times \dots \times A_2^{(m)},$$

$$A_2^{(i)} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \ i = 1,2, \dots, m,$$

$\times$ - is the notation for Kronecker matrix multiplication.

Walsh-Hadamard matrix factorization and fast Hadamard transform

The matrix A_m can be factorized, that is, represented as a simple product of matrices containing a large number of zero symbols, that is, in the form:

$$A_m = B_m^m, \quad (10)$$

where B_m is a square matrix of order $N = 2^m$. The values of its elements $b_{h,x}$ can be found using Good's theorem, which is applicable only to matrices A_m that are Kronecker powers of simpler matrices B_m, where *h* is the row number and x is the column number in which the element $b_{h,x}$ is located. According to this theorem

$$b_{h,x} = \{\lambda_{\varepsilon,r}\delta_Q^G\}, \varepsilon = h_1, r = x_m, \quad (11)$$

where $\lambda_{\varepsilon,r}$ – matrix elements A_2, $\varepsilon = 0,1$ and $r = 0,1$ – the numbers of its rows and columns, respectively,

$$\delta_Q^G = \begin{Bmatrix} 1 & \text{при } G = Q \\ 0 & \text{при } G \neq Q \end{Bmatrix} - \quad (12)$$

Kronecker delta, where $G = [\frac{x}{2}]$ is the integer part of the number $x/2$, $Q = ((h))_{N/2}$ is the remainder of dividing *h* by $N = 2^{m-1}$; h_1 is the most significant digit of the representation of the number *h* in the binary number system, where $h = h_m + 2h_{m-1} + \cdots + 2^{m-1}h_1$; $x_m$is the least significant digit of the representation of the number *x* in the binary number system.

In order to determine the structure of the matrix B_m, we note that the values of the discrete function $[x/2]$ are equal to $0,0,1,1,2,2,3,3,\ldots,2^{m-1}-1,2^{m-1}-1,2^m,2^m$, and the values of $((h))_{N/2}$ are respectively equal to $0,1,2,3,\ldots,2^{m-1}-1,0,1,2,3,\ldots,2^{m-1}-1$. But then it follows from (11) that in each of its rows there will be only two elements different from zero, that is,

$$B_m = \begin{bmatrix} 1 & 1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 1 & 1 & \ldots & 0 & 0 \\ & & & \ldots & & & \\ 0 & 0 & 0 & & \ldots & 1 & 1 \\ 1 & -1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 1 & -1 & \ldots & 0 & 0 \\ & & & \ldots & & & \\ 0 & 0 & & & \ldots & 1 & -1 \end{bmatrix}. \quad (13)$$

Thus, the decomposition of any discrete signal, represented as a vector *X*, into the basis functions of the Walsh-Hadamard system, taking into account the factorization of the matrix A_m, is described by the formula:

$$\boldsymbol{Y} = \boldsymbol{B}_m^m \boldsymbol{X} = \boldsymbol{B}_m[\boldsymbol{B}_m \ldots [\boldsymbol{B}_m \boldsymbol{X}]]. \quad (14)$$

According to (14), column $\boldsymbol{Y_1} = \boldsymbol{B}_m \boldsymbol{X}$ is calculated first, then column $\boldsymbol{Y_2} = \boldsymbol{B}_m \boldsymbol{Y_1}$, and so on. Lastly, column $\boldsymbol{Y_m} = \boldsymbol{B}_m \boldsymbol{Y_{m-1}}$. is calculated. The procedures for calculating columns $\boldsymbol{Y_1}, \boldsymbol{Y_2}, \ldots, \boldsymbol{Y_m}$ are identical and are described by an elementary graph taking into account the Hadamard matrix factorization algorithm. An example of an elementary FPA graph for *m* = 5 is shown in Figure 4.

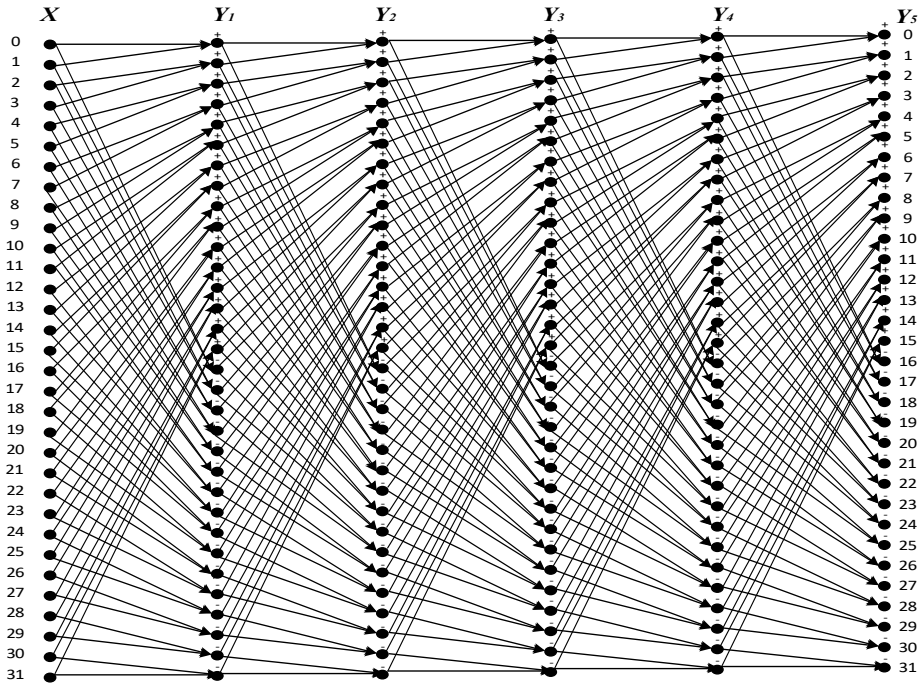


Figure 4. Example of a FPA graph with m=5.

Fast transform in the truncated Walsh-Hadamard basis

The PSPs used to form the SLS can be reduced to a limited set of rows of the Walsh-Hadamard matrix, so fast transformations in a truncated Walsh-Hadamard basis can be important. As an example, consider a fast transformation in the Rademacher system. In order to develop such an algorithm, we will take into account that the Rademacher functions are located in the rows of the Hadamard matrix $\boldsymbol{A}_m$ with numbers $y = 2^v, v = 0,1,2, \dots, 2^{m-1}$ (for example, for *m* = 5 – in rows with numbers 1,2,4,8,16, for *m* = 9 – in rows with numbers 1,2,4,8,16,32,64,128,256), for *m* = 10 – in rows with numbers 1,2,4,8,16,32,64,128,256,512, etc.), as well as the possibility of representing $\boldsymbol{A}_m$ as a simple product of sparsely filled matrices $\boldsymbol{B}_m$, as described above.

The rules for fast spectral transformations in truncated Walsh-Hadamard bases are described in. By storing only *m* rows with numbers *y* in the matrix $\boldsymbol{A}_m$ out of a total of2^m, we obtain a truncated Hadamard matrix.

In the matrix $\boldsymbol{B}_1$, only m rows are stored with the same numbers $y = 2^v, v = 0,1,2, \dots, 2^{m-1}$ that were stored in the matrix $\boldsymbol{A}_m$. This means that multiplying the resulting truncated matrix $\boldsymbol{B}_{1y}$ by the result of multiplying $\boldsymbol{B}_{2y} \dots \boldsymbol{B}_{my}$ by the input vector *X* requires only m summations. We obtain the matrix $\boldsymbol{B}_{2y}$ taking into account that the $(N - 2m)$ columns of the matrix B_1y consist only of zero elements. These columns must also be excluded from $\boldsymbol{B}_{1y}$, simultaneously excluding the rows of matrix $\boldsymbol{B}_2$, the numbers of which coincide with the numbers of the columns excluded in $\boldsymbol{B}_{1y}$, therefore matrix $\boldsymbol{B}_{2y}$ contains 2*m* rows, and when multiplying it by $\boldsymbol{B}_3 \dots \boldsymbol{B}_m \boldsymbol{X}$, only 2*m* summation operations will be required, in the last matrix $\boldsymbol{B}_{my}$ 2^m rows are always preserved, that is, $\boldsymbol{B}_{my} = \boldsymbol{B}$.

Thus, the number of rows stored in the matrices $\boldsymbol{B}_{sy}$, $s = 1, \dots, m$, which coincides with the number of elementary summation operations required to multiply a vector with each matrix, is described as $m + 2m + (2 * 2m - 4) + (2 * (2 * 2m - 4) - 8) + (2 * (2 * (2 * 2m - 4) - 8) - 16) + \cdots$. A recurrence formula can be derived for calculating the number of nonzero rows of the matrices $\boldsymbol{B}_{sy}$:

$$\boldsymbol{B}_s = \begin{cases} m\text{, если } s = 1, \\ 2m\text{, если } s = 2, \\ 2B(s-1) - 2^{s-1}\text{, если } s = 3,4, \dots, \end{cases} \quad (15)$$

where $\boldsymbol{B}_s$ is the number of rows stored in the $\boldsymbol{B}_{sy}$ matrix. Then the number of elementary mathematical summation operations during accelerated multiplication of a matrix of Rademacher functions by a vector is:

$$S = B(1) + B(2) + \sum_{s=3}^{m} 2B(s-1) - 2^{s-1}, \quad (16)$$

and the gain in the number of such operations, compared to simple multiplication of a matrix of the same dimension by a vector, will be $I(m) = m2^m/S$. For m = 5 it is approximately 1.84, but for typical lengths of the PBS used in constructing, for example, navigation codes, it is more significant – for N = 511(m = 9) the gain is 3 times, and for N = 1023(m = 10) – 3.4 times. Figure 5 shows the gain in the number of elementary operations for accelerated multiplication of the matrix of Rademacher functions and a vector, compared to simple multiplication.

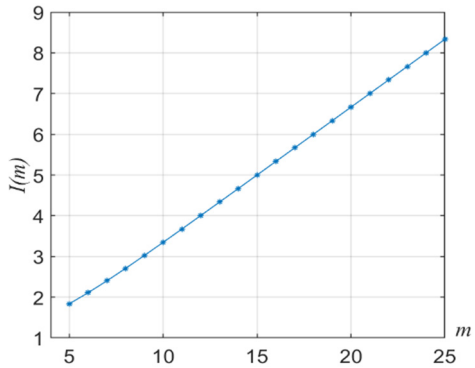


Figure 5. Gain in the number of elementary arithmetic operations during accelerated multiplication of a matrix of Rademacher functions and a vector, compared to simple multiplication.

An example of a fast transformation graph for accelerated multiplication of the Rademacher function matrix for m=5 and a vector is shown in Figure 6.

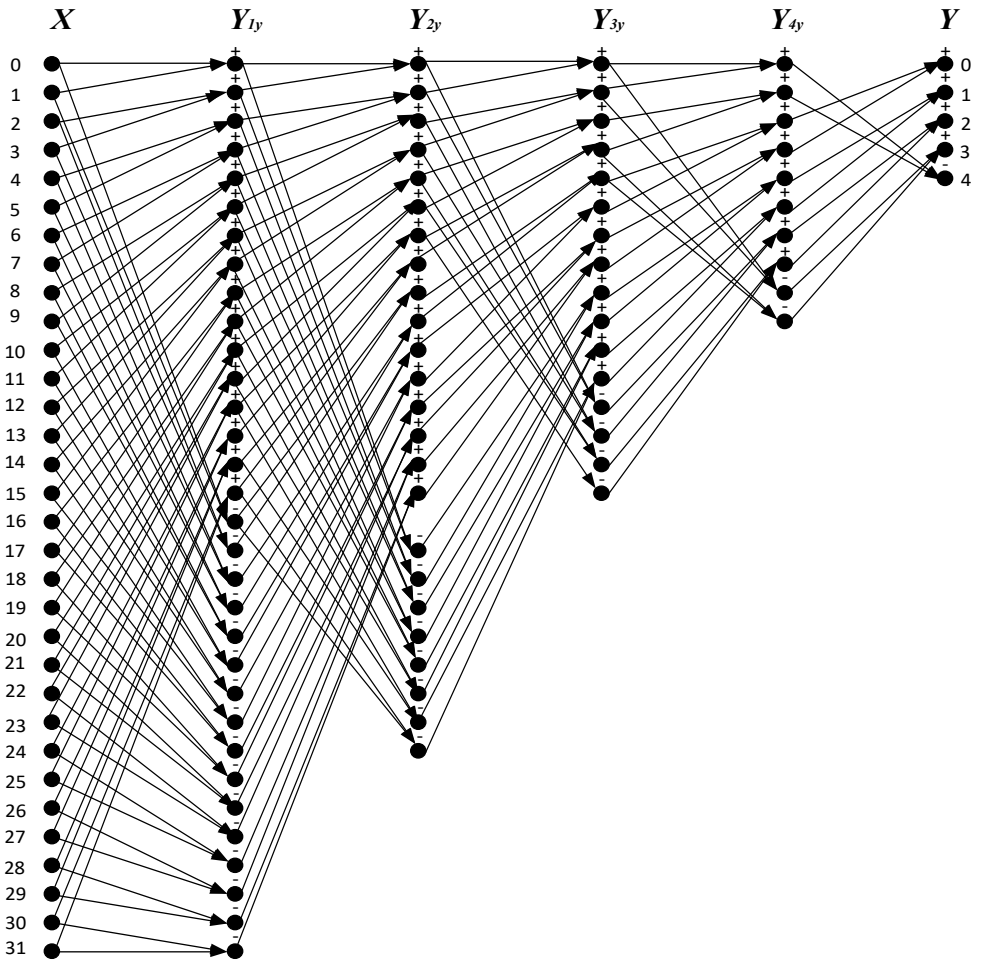


Figure 6. Fast transform graph for accelerated multiplication of the Rademacher function matrix for m=5 and the vector

Conclusion

1. When jointly detecting and estimating the parameters of a set of noise-like CNS, including their copies randomly shifted relative to each other in frequency and time, using the maximum likelihood criterion against a background of white Gaussian noise, it is necessary to calculate the composition of the real parts of their DCFs using correlators or matched filters. In this case, the distribution function of the sum of mutual interference and transformed noise will correspond to a Gaussian law, and the estimated parameters of the CNS will be their carrier frequencies, carrier phases, and relative time delays. As a result, this approach can be used for relatively small phase shifts of the CNS carrier frequencies.

2. For significant phase instabilities of the carrier frequencies of the CNS composition, the DCF modulus is usually calculated, resulting in the distribution function of mutual interference and noise at the input of the receiver's decision device corresponding to the Rayleigh-Rice law. 3. When detecting either a single or a set of signal-to-noise ratios (STRs) with unknown carrier frequencies and time delays, it is necessary to repeatedly calculate the convolutions of the reference and received STRs. In digital terms, the convolution calculation operation is reduced to vector-matrix multiplication. When synchronizing using received STRs, it is reduced to multiplying the circulant matrices of the PRS used to generate the STRs by the vector of signal samples at the receiver input.

4. When using binary STRs, fast multiplication of its circulant matrix by a vector can be implemented using the fast Hadamard transform if a linear transformation of the circulant matrices of the used STRs to a Hadamard matrix is possible. The number of elementary arithmetic operations required in this case is $Nlog_2N = Nm$, while direct matrix-vector multiplication would require elementary N^2 arithmetic operations.

REFERENCES

[1] S.F. Gorgadze, Sh.D. Wu, “Detection and synchronization of low-power noise-like signals in a satellite radio system,” *T-Comm*. 2023. Vol. 17. No. 8, pp. 4-20. DOI: 10.36724/2072-8735-2023-17-8-4-20

[2] S.F. Gorgadze, Sh.D. Wu., A.V. Ermakova, “Synchronization of M-sequences based on the fast Hadamard transform,” *Radio Engineering and Electronics*. 2024. Vol. 69. No. 2, pp. 122-136.

[3] S. F. Gorgadze, Sh. D. Wu, A. V. Ermakova, “Synchronization of Gold Sequences Based on Fast Transformation in a Truncated Basis of Walsh-Hadamard Functions,” *Radio Engineering and Electronics*. 2024. Vol. 69. No. 2, pp. 137-145.

[4] L. E. Varakin, “Communication Systems with Noise-Like Signals,” Moscow: Radio and Communications, 1985. 384 p.

[5] N. I. Smirnov, S. F. Gorgadze, “Duration of the Time for a Receiver to Enter Synchronism with a Noise-Like Complex Signal in a Satellite Asynchronous Information Transmission System,” *Foreign Radio Electronics*. 1997. No. 5, pp. 41-51.

[6] R. W. Middlestead, “Digital Communications with Emphasis on Data Modems. Theory, Analysis, Design, Simulation, Testing and Applications,”Lesly (USA): Wiley, 2017. 832 p.

[7] V. V. Losev, E. B. Brodskaya, V. I. Korzhik; Ed. V. I. Korzhik, “Search and Decoding of Complex Discrete Signals,” Moscow: Radio i Svyaz, 1988. 224 p.

[8] G. Maral, M. Bousquet, Z. Sun, “Satellite Communications Systems,” United Kingdom: Wiley, 2020/ 800 p.

[9] V. V. Losev, V. D. Dvornikov, “Address Sequence Recognition Using Fast Transformations,” *Radio Engineering and Electronics*. 1983. №8, pp.15-40.

[10] V.P. Ipatov, “Broadband systems and code division multiplexing. Principles and applications,” Moscow: Tekhnosfera, 2007. 487 p.

[11] C. Beard, W. Stallings, “Wireless Communication Networks and Systems,” L.: Pearson, 2016. 595 p.

[12] S.F. Gorgadze, “Synchronization in infocommunication systems,” Moscow: Media Publisher, 2022. 44 p.

[13] R.V. Volkov, V.N. Sayapin, V.V. Sevidov, “Model for measuring the time delay and frequency shift of a radio signal received from a repeater satellite when determining the location of an earth station,” *T-Comm*. 2016. Vol. 10. No. 9, pp. 14-18.

[14] V.I. Kulakova, “Detection of weak signals by the cross-correlation method with compensation for phase instabilities in radio monitoring of the frequency resource of satellite communication systems,” *Control, Communications and Security Systems*. 2020. No. 1, pp. 33-48.

[15] V.M. Smolyaninov, L.E. Nazarov, I.V. Prokofiev, “Some properties of discrete frequency-modulated signals defined on the generalized Vilenka-Krestenson basis,” *Radio Engineering and Electronics*. 1989. Vol. 34. No. 8, pp. 1686-1689.

[16] W. K. Li Ping, K. Y. Leung, “Low-Rate Turbo-Hadamard Codes,” *IEEE Transactions on Information Theory*. 2003. Vol. 49. No. 12. P. 3213.

[17] Sh. D. Wu, “Statistical characteristics of two-dimensional autocorrelation functions of noise-like signals,” Electrosvyaz. 2024. No. 6, pp. 53-61.

[18] Potapov, A. A. Determination of detection thresholds of radio signals for the energy detector method,” *Journal of Radio Electronics*. 2021. No. 9.

[19] A. Suneel, S. Shiyamala, “Peak detection based energy detection of a spectrum under Rayleigh fading noise environment,” *Journal of Ambient Intelligence and Humanized Computing*. 2021. No.12, .4237-4245. DOI: 10.1007/s12652- 020-01818-1.

[20] Sh.D. Wu, S.F. Gorgadze, “Device for accelerated search of noise-like signal*,” Technologies of the Information Society. Collection of works of the XVI International industry scientific and technical conference.* Moscow, 2022, pp. 88-90.

[21] S.F. Gorgadze, “Accelerated digital algorithm for synchronization of noise-like signals in time and frequency,” *Systems of synchronization, formation and processing of signals*. 2016. Vol. 7. No. 4, pp. 16-18.

[22] Sh.D. Wu, S.F. Gorgadze, “Efficiency of a device for rough estimation of synchronization parameters of a noise-like signal,” *DPSA: Issues of application of digital signal processing*. 2023. Vol. 13. No. 1, pp. 31-39.

[23] T.M. Gut, S.F. Gorgadze, “Characteristics of covariance functions and estimation of noise-like signal parameters,” *Telecommunications and information technologies*. 2019. Vol. 6. No. 2, pp. 35-41.

[24] N.Yu. Muzychenko, “Search and detection of noise-like signals under conditions of frequency instability of the communication channel,” *Radio engineering and electronics*. 2019. Vol. 64. No. 1, pp. 44-49.

[25] I.I. Snytkin, T.I. Snytkin, “The "third decision scheme" method for increasing the efficiency of search and synchronization of complex broadband noise-like signals,” *Electromagnetic Waves and Electronic Systems*. 2021. Vol. 26. No. 6, pp. 44−56. DOI: 10.18127/j15604128-202106-05.

[26] S.F. Gorgadze, A.V. Ermakova, “Efficiency of IDMA and CDMA Technologies with a Small Spectrum Spreading Factor,” *DPSA: Application Issues of Digital Signal Processing*. 2023. Vol. 13. No. 2, pp. 22-29.

[27] Y. Be’ery, J. Snyders, “Optimal Soft Decision Block Decoders Based on Fast Hadamard Transform,” *IEEE Trans*. 1986. Vol. 32. No. 3, pp. 355-364.

[28] V.S. Kuznetsov, A.S. Volkov, A.V. Solodkov, V.A. Doroshenko, “Development of a synchronization system based on complex wideband signals,” *T-Comm*. 2020. Vol. 14. No. 5, pp. 4-14.

[29] V.M. Smolyaninov, “Discrete multiplicative group signals and their relationship with group codes,” *Radio Engineering and Electronics*. 1985. Vol. 30. No. 12, pp. 2391-2394.

[30] R. Gold, “Optimal binary sequences for spread spectrum multiplexing (Corresp.),” *IEEE Trans. on Information Theory*. 1967. Vol.1. Vol. 13. No. 4, pp. 6-19. DOI: 10.1109 / TIT.1967.1054048. //

[31] V.S. Kuznetsov, I.V. Shevchenko, A.S. Volkov, A.V. Solodkov, “Generation of Gold Code Ensembles for Direct Spread Spectrum Systems,” *Proceedings of MAI*. 2017. No. 96. http://trudymai.ru/.

[32] V.S. Kuznetsov, K.A. Mordasov, “Fast Decoding Based on Passive Matched Filtering of Long Pseudo-Random Codes,” *News of Higher Educational Institutions. Electronics*. 2010. No. 1 (81), pp. 57-62.

[33] V. Yu. Mikhailov, R. B. Mazepa, “Application of transformations in Galois fields for fast search by delay of Gold sequences,” *T-Comm*. 2018. Vol. 12. No. 4, pp. 4-9.

[34] V. Y. Mikhaylov, R. B. Mazepa, “Estimation of the Features of Application of the M-Sequences Subset with the Possibility of Joint Processing,” *2021 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO)*. 2021, pp. 1-6. DOI: 10.1109/SYNCHROINFO 51390.2021.9488414

SYNCHROINFO JOURNAL

www.media-publisher.eu/synchroinfo-journal

EXPERIMENTAL COMPARISON OF REST AND SOAP WEB SERVICES FOR REAL-TIME FACE RECOGNITION

Haia Kablan [1]

[1] Latakia University, Latakia, Syria, haiakabalan3@gmail.com

Lilia I. Voronova [2]

[2] Moscow Technical University of Communications and Informatics, Moscow, Russia

ABSTRACT

The primary objective of this study is to identify the optimal platform for IoT applications with limited resources and real-time requirements. With the development of the Internet of Things, interest in performance testing of web platforms supporting these applications has increased. This study compares REST and SOAP technologies for use in a smart home with facial recognition. Experiments were conducted on Raspberry Pi OpenCV, and testing was performed on JMeter. The results showed significant improvements in metrics: REST throughput was 1.5-5.2 times higher, latency was 2.0-2.5 times lower, and errors were reduced by 50% compared to SOAP. Based on the data obtained, an optimized web service architecture was proposed for an intelligent real-time monitoring system for a smart home environment.

DOI: 10.36724/2664-066X-2026-12-2-26-35

Received: 10.02.2026
Accepted: 12.04.2026

Citation: Haia Kablan, L.I. Voronova, "Experimental comparison of rest and soap web services for real-time face recognition," *Synchroinfo Journal* **2026**, vol. 12, no. 2, pp. 26-35.

Licensee IRIS, Vienna, Austria.

KEYWORDS: *Internet of Things (IoT), face recognition, Raspberry Pi, OpenCV, Haar cascade algorithms, LBPH (Local Binary Patterns), Web services, REST SOAP.*

Introduction

With the development of the Internet of Things (IoT), interest in performance testing of web platforms supporting its applications has increased. This paper compares the performance of RESTful and SOAP APIs using a Raspberry Pi-based intelligent video surveillance system implemented using facial recognition technologies (Haar cascade and LBPH).

The primary goal of this study is to determine the optimal platform for resource-constrained IoT applications with real-time requirements.

Previous research in this area

Researchers identify three areas of research related to object recognition in smart home design. First, they address the problem of practical implementation of facial recognition systems for real-world smart home projects. The approach described in [1-4] involves using a Raspberry Pi microcomputer with computer vision algorithms such as Haar Cascade/LBPH. This approach can be considered the basis for developing functional prototypes.

The second area of research includes work on the architecture and communication of IoT platforms, with a particular focus on device integration, interaction paradigms, and security. The main conclusion of [5, 6] is the key role of a universal "link" between devices and the user.

The third area of research explores and compares two protocols used for developing web services (REST and SOAP) in the IoT. The works are theoretical or demonstrative in nature, discussing the advantages of the REST protocol (simplicity, efficiency) and presenting models of its application [7-9]. There are no practical tests of protocols in real-world IoT conditions, with limited resources and high protocol speed requirements.

As is well known, the operation of the Internet of Things involves a number of integrated stages, such as collecting environmental data, processing and decision-making, control actions, storage, and analysis [10].

The Department of Information Systems and Automation at MTUCI is developing a number of projects related to the application of intelligent technologies in the fields of the Internet of Things, computer vision, and embedded systems cybersecurity [11-13]. These projects include the development of intelligent monitoring systems, performance analysis of communication protocols under limited resources [14], and the development of automated methodologies for improving the reliability and efficiency of intelligent systems in real time. This research is carried out practically using prototypes and performance tests with the goal of creating innovative solutions [15].

Recognition technologies

The facial recognition process consists of three stages: face recognition using classifiers, feature extraction, and identification by comparison.

Face Recognition Using the Haar Cascade Classifier

A pre-trained classifier (haarcascade_frontalface_default.xml) is used for efficient real-time face recognition [16]. The method is based on Haar features, which are calculated as the difference between the sum of pixel intensities in adjacent rectangular regions (Fig. 1).

Fig. 1. Haar Feature [17]

Value = ∑(pixels in black region) - ∑(pixels in white region)……..……. (1)

To speed up the computations, an integral image is used, as shown in (b), which allows the sum of pixels in any rectangle to be calculated as follows:

$$\mathbb{S}(D) = \mathrm{II}(4) - (\mathrm{II}(3) + \mathrm{II}(2)) + \mathrm{II}(1).....(b)[17] \quad (2)$$

where S(D) is the sum of the pixels in rectangle D alone and is the sum of the pixels in rectangles A + B + C + D, represented as II(4); II(3) is the integral image of rectangles A + C; II(2) is the integral image of B + A; and finally, II(1) is the integral image of rectangle A. The addition is performed due to the fact that the integral image is defined as follows:

$$\mathrm{II}[x, y] = \mathrm{I}[x', y'].....(c)[13] \quad (3)$$

where II[x,y] represents the original image, and I[x', y'] is the entire image.

The Adaboost algorithm is used to select the most significant features from ~160,000 possible features, reducing them to ~6000 [17-20]. A cascade approach is used to quickly remove non-edge regions [17-21].

Feature Extraction with LBPH

After face recognition, facial features are extracted using the LBPH (Local Binary Patterns Histograms) algorithm with the following parameters: radius = 1, neighbors = 8, 8x8 grid [21].

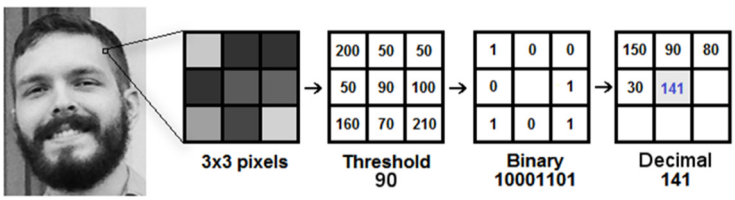


Fig. 2. LBP Algorithm [20]

For each pixel, a binary pattern is calculated (Figure 2), local histograms are calculated, and then combined into a descriptor with 16,384 dimensions (8x8x256).

Face Identification

Face identification is performed by matching the LBPH descriptor of a new image against the processed database, based on Euclidean distance. The output provides a face identifier and a confidence level [21].

Web Platform and Services

The developed platform is based on a three-tier architecture consisting of a server part, a user interface, and APIs for interaction between them, with support for both fundamental web service paradigms: REST and SOAP [22]. The service uses a standard architecture based on a service provider, consumer, and registry [23] and is characterized by loose coupling, flexibility, reusability, interoperability, and automatic discovery [24]. SOAP is a standardized XML-over-HTTP messaging protocol that provides platform independence and security, and its message structure consists of an envelope, header, body, and error element [25]. Meanwhile, REST is an architectural style for developing web applications that relies on the basic HTTP methods (GET, POST, PUT, DELETE) and returns data in JSON-like formats based on the principles of client-server separation, statelessness, caching, a uniform interface, and a multi-tier system [26-27].

Implementation of a Web Service Comparison Monitoring System Prototype

Using a three-tier architecture, a real-time web service monitoring system for a smart home environment was developed. The camera module and HC-SR501 motion sensor are installed on a Raspberry Pi 3 Model B+ device at the Edge tier (Fig. 3).

Fig. 3. Final connection setup

The device runs the Raspberry Pi Buster operating system and was configured to operate as an IP camera using motion tracking software, enabling streaming. H.264 video with a resolution of 640x480 pixels and a frame rate of 15 frames per second is transmitted via port 8081 on the local area network (LAN).

The main server, which collects HTTP streams from the Raspberry Pi, runs Ubuntu 20.04 LTS, a Core i7, and 12 GB of RAM. Django 3.2.4 and OpenCV 4.5.1 are used for video processing.

Each video frame is processed to perform face recognition using the Haar cascade method, feature extraction using the LBPH method with parameters radius=1, neighbors=8, grid=8x8, and comparison with a database of 500 images of 50 faces, saving the result in SQLite.

The web interface allows you to register, log in, and interact with the dashboard. The dashboard has two main actions.

1. Create a service: For the service creation action, the user can select either real-time face recognition or video face recognition.

2. Training data: For the training data action, the user can select Train the system and upload images and names for face recognition.

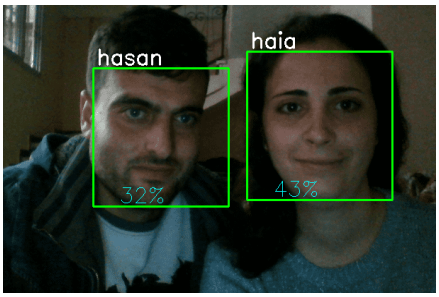


Fig. 4. Live Page View Result

The results are displayed on the live stream page (Fig. 4).

Users can view live video streams and perform facial recognition.

```
API/service/<str:API_key>
API/service/faces/<str:API_key>
API/face/<str:fid>
```

Fig. 5. Endpoints Provided by the Two Platforms

The architecture of the system using the two developed platforms, REST and SOAP, is shown in Fig. 5.

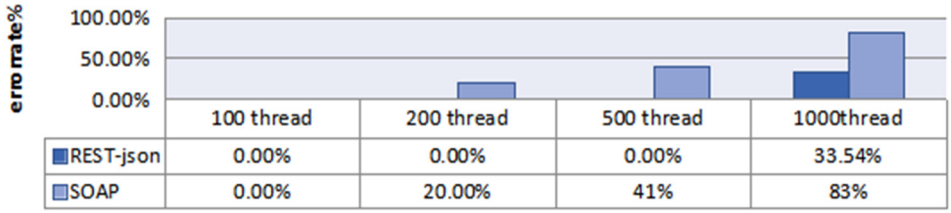
System Testing and Performance Evaluation

To test and measure the relative performance of the RESTful and SOAP APIs, Apache JMeter was used, simulating a series of user interactions in a predefined testing environment. Four parameters were considered when evaluating RESTful and SOAP API-based applications: throughput, which measures the ability of a single system to process multiple requests within one second; initial response time, latency; average overall response time; and error rate. Each parameter was implemented 30 times to obtain an average value.

The first scenario involves varying the number of users (10, 100, 200, 500, 1000) attempting to access the getfaces service, which returns information on 250 images with a ramp-up time of 10 seconds, and calculating the error rate for 5 request iterations.

A group of threads executes the same scenario. The number of threads is the number of virtual users that can connect to the server and was set to 50, 100, 150, and 200, respectively.

The ramp-up time is the amount of time it will take Apache JMeter to add all tested users during the test.

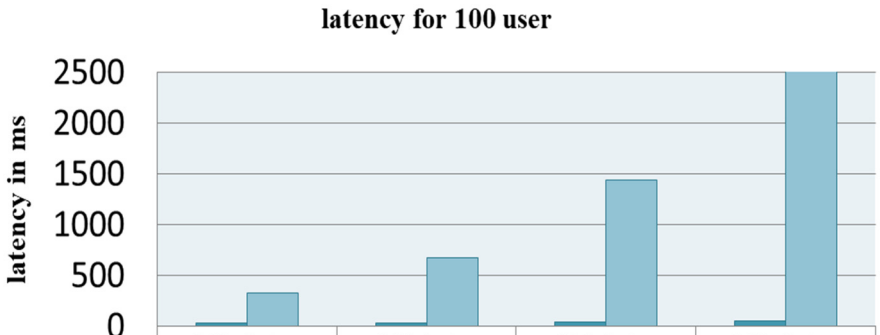


	100 thread	200 thread	500 thread	1000thread
REST-json	0.00%	0.00%	0.00%	33.54%
SOAP	0.00%	20.00%	41%	83%

Fig. 6. Error rate for 250 photos using getfaces

The REST platform can handle 1,000 users with 5,000 requests (with 5 retries) and has an error rate of 33.54%, while the SOAP error rate is 83%, as shown in Figure 6.

The second scenario involves changing the number of images (100, 150, 200, 250) in the face collection for 100 users accessing the getfaces service and calculating the response time and throughput with 5 retries. The ramp-up time is 10 seconds, meaning 10 users are added every second. Each time, the number of images returned by getfaces changes, and the requests are retried 5 times, resulting in a total of 500 requests.



	100 photos	150photos	200photos	250 photos
rest-latency	26.2	33.3	40.68	48.58
soap-latency	325.626	676.614	1441.882	3178.74

Figure 7. Latency in the Second Scenario

We note that as the response size increases from 100 to 250 images, there is a significant difference in latency between the SOAP-based platform and the REST-based platform, as shown in Figure 7.

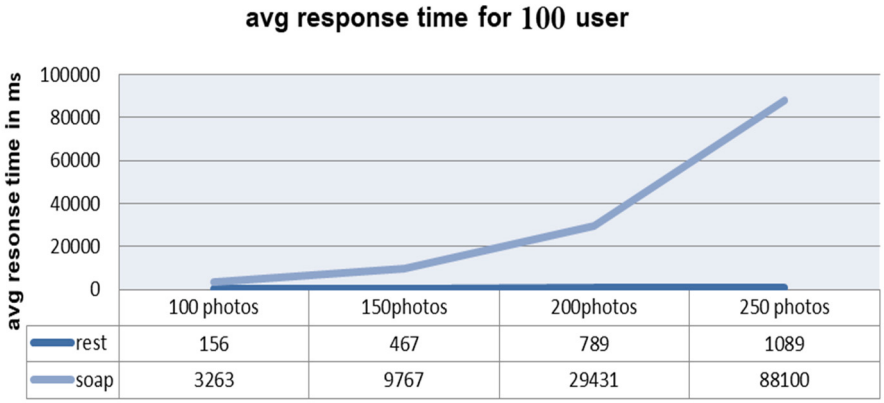


Figure 8. Average response time for the second scenario

As Figure 8 shows, REST requires less than 1 second for 250 images, while SOAP takes approximately 88.1 seconds, which is a significant difference.

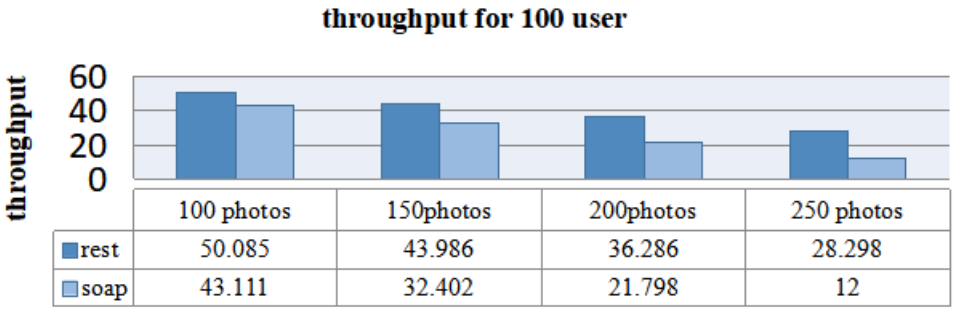


Figure 9. Performance for the Second Scenario

Figure 9 shows the performance for the second scenario. These results indicate that REST yields the best results.

Third Scenario: Launching 15 live video streaming services (15 sensors) and providing access to the service to 500 users with a startup time of 10 seconds.

Table 1

Results of the Third Scenario

Label	# Samples	Average	Throughput	Received KB/sec	Sent KB/sec	Avg. Bytes	latency
rest	500	20.9	50.44022	23.27	6.06	492	20.676
soap	500	27	49.5491	37.16	23.61	768	26.948

This scenario allows users to monitor more than one room. Table 1 illustrates the results of this scenario.

Scenario Four: Spike Testing

Spike testing analyzes the system's response to unexpected, sharp increases or decreases in system traffic.

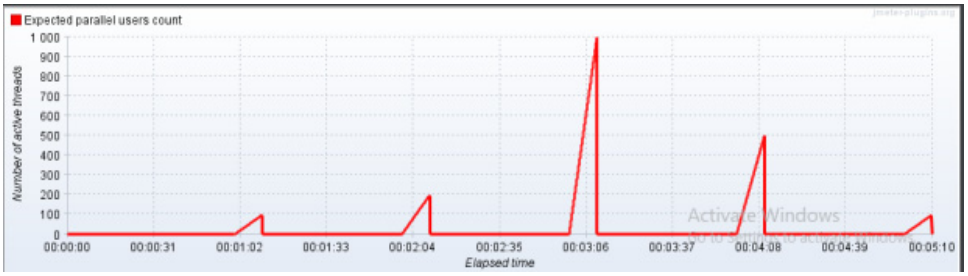


Figure 10. Configuration Jump Testing

Figure 10 below shows an example of flow testing using a finite set of flows in JMeter with various parameters: Initial Number of Users, Initial Latency, Startup Time, Load Hold, and Shutdown Time.

Table 2

Results of the Fourth Scenario

Label	# Samples	Average	Min	Max	Error %	Throughput	Received KB/sec	Sent KB/sec	Avg. Bytes
soap	14771	953	6	6860	39.45%	47.57518	69.81	13.73	1502.5
Rest	21504	556	4	1077	43.14%	69.27768	95.69	4.92	1414.4

It is noted that the actual number of requests also depends on the response time. These test results are presented in Table 2.

Conclusion

An experimental study demonstrates the superiority of using a REST architecture over SOAP, achieving a 1.5x–5.2x throughput increase, a 2.0x–2.5x latency improvement, and a 50% improvement in error rate. This demonstrates that this efficiency is due to its ability to effectively manage limited resources and process intelligent IoT applications in a timely manner. It is recommended that this effective methodology be standardized for intelligent IoT applications. Furthermore, this system has the potential to effectively serve up to thousands of cameras in a commercial environment, leverage AI and deep learning techniques, and utilize various APIs to meet varying energy needs.

REFERENCES

[1] R. Kazi, G. Chaudhary, “Live Video Streaming using Raspberry PI with Face Detection,” *International Journal of Engineering Research & Technology (IJERT),* 2019. Vol. 8, No. 11. November, pp. 716-717.

[2] F. Rahamanm, A. Al Noman, M. Ali, M. Rahman, “Design and implementation of a face recognition—based door access security system using Raspberry Pi,” *International Journal of Research in Engineering and Technology (IRJET).* 2021. Vol. 8, No.11. December, pp. 1705-1709.

[3] D. Mali, R. Patil, N. Dharwadkar, Ch. Devale, O. Tembhurne, “Real-Time Smart Surveillance System Using Raspberry Pi,” *SSRN Electronic Journal.* 2019. January, pp. 1851-1857.

[4] R. Novosel, B. Meden, Z. Emer, V. Struc, P. Peer, “Embedded Engineering IoT – face recognition with Raspberry Pi,” *ResearchGate.* 2017. September 8.

[5] Z. Yang, X. Guo, D. Janowsky, X. Guo, C. Chang, “A web platform for globally interconnected 6Lowpan networks,” *Proceedings of the 2019 International Conference on Embedded Wireless Systems and Networks*. Beijing, China, 2019. 25-27 February, pp. 367-372.

[6] S. Cavalieri, G. Cantali, A. Susinna, “Integration of IoT technologies into smart grid systems,” *Sensors.* 2022. Vol. 22, No. 7. March. DOI: 10.3390/s22072475.

[7] R. Maurya, K. Nambiar, P. Babbe, J. Kalokhe, Y. Ingle, N. Shaikh, “Application of Restful APIs in IoT: A Review,” *International Journal for Research in Applied Science and Engineering Technology (IJRASET).* 2021. Vol. 9, no. 2, pp. 145 -151. DOI: 10.22214/ijraset2021.33013.

[8] L. Pan, M. Xu, Xi L., Y. Hao, “Research of Livestock Farming IoT System Based on RESTful Web Services,” *5th International Conference on Computer Science and Network Technology (ICCSNT).* 2016, pp. 45-50.

9. F. Halili, E. Ramadani, “Web Services: A Comparison of Soap and Rest Services,” *Modern Applied Science.* 2018. Vol. 12, no. 3. P. 175. DOI: 10.5539/mas.v12n3p175.

[10] Leverage. How IoT Systems Work [Electronic resource]. IoT eBook. URL: https://www.leverege.com/iot —ebook/how —iot —systems —work (date of access: 3.12.2025)

[11] O. L. Antonycheva, L. I. Voronova, “Teaching the discipline "Machine Learning" using visualization tools,” *Technologies of the Information Society: Coll. proc. XVIII Int. industry scientific and technical. conf*. (Moscow, February 27-28, 2024). Moscow: Moscow Technical University of Communications and Informatics, 2024, pp. 369-371.

[12] A. G. Vovik, L. I. Voronova, "Methodology of automated management of information security in the Internet of Things systems," *H&ES Research*. 2024. Vol. 16. No. 4, pp. 4-11. doi: 10.36724/2409-5419-2024-16-4-4-11.

[13] K. A. Kalushev, L. I. Voronova, “Implementation of an approach to determining the coordinates of objects in the field of technical vision,” *DSPA: issues of digital signal processing application*. 2024. Vol. 14, No. 3, pp. 30-36.

[14] N. F. Mohammad, L. I. Voronova, V. I. Voronov, S. A. Rozhkov, “Software complex for modeling routing in a heterogeneous model of wireless sensor network,” *Systems of signals generating and processing in the field of on-board communications*. 2024. Vol. 7, no. 1, pp. 281-285. ISSN 2768-0096. eISSN 2768-0118.

[15] V. A. Smolnikov, L. I. Voronova, V. I. Voronov, S. A. Rozhkov, V. M. Petukhov, “Simulation of the digital twin of the technological process of creating a demonstrator using R-PRO digital,” *Systems of signals generating and processing in the field of on board communications*. 2024. Vol. 7, No. 1, pp. 438-442. ISSN 2768-0096. eISSN 2768-0118.

[16] S. Singh, P. Anap, Y. Bhaigade, J.Chavan, “IP Camera Video Surveillance using Raspberry PI,” *Journal of Advanced Research in Computer and Communication Engineering (JARCCE).* 2015. Vol. 4, No. 2. February, pp. 326-328.

[17] M. Raoa, H. Palleb, P. Dasaric, Sh. Jannaikode, “Implementation of Low Cost IOT Based Intruder Detection System by Face Recognition using Machine Learning,” *Turkish Journal of Computer and Mathematics Education.* 2021. Vol. 12, no. 13, pp. 353-362.

[18] R. Senthamizh, D. Sivakumar, S. Sandhya, S. Siva, S. Ramya, K. Suba, S. Raja, “Face Recognition Using Haar-Cascade Classifier for Criminal Identification,” *International Journal of Recent Technology and Engineering (IJRTE).* 2019.Vol. 7, no. 6S5. April, pp. 1871-1876.

[19] Willberger. Deep learning: Haar-cascade explained [Electronic resource]. 2022. November 26. URL: www.willberger.org/cascade — haar — explained (date of access: December 5, 2025).

[20] W. Zhao, R.Chellappa, “Face Recognition: A Literature Survey,” ACM Computing Surveys. 2003. Vol. 35, No. 4. December, pp. 399-458.

[21] P. Singh, “Understanding Face Recognition Using LBPH Algorithm [Electronic resource],” *Analytics Vidhya*. 10.21.2024. URL: https://www.analyticsvidhya.com/blog/2021/07/understanding-face-recognition-using-lbph-algorithm/ (access date: 12/27/2025).

[22] C. Reiff, S. Oechsle, F. Eger, A. Verl, “Web-based Platform for Data Analysis and Monitoring,” *Procedia CIR*P. 2019. Vol. 86. January, pp. 31-36.

[23] M. Gashti, “Investigating Soap and Xml Technologies in Web Service,” *International Journal on Soft Computing (IJSC).*

[24] M. Govindaraju, A. Slominski, K. Chiu, P. Liu, R. Engelen, M. Lewis, “Toward characterizing the performance of SOAP toolkits,” *Proceedings of the 5th IEEE/ACM International Workshop on Grid Computing*. Pittsburgh, PA, 2004. November, pp. 365-372.

[25] C. Kiama, L. Muchemi, “Comparative Study of REST and SOAP: Case of Registrar of Political Parties’ Kenya,” *Trends in Distributed Computing.* 2014. January, pp. 105-116.

[26] R. Sinha, M. Khatkar, S. Gupta, “Design & Development of a REST based Web Service Platform for Applications Integration on Cloud,” *International Journal of Innovative Science, Engineering & Technology (IJISET).* 2014. Vol. 1, Iss. 7, pp. 385-389.

[27] M. Agarajan, Ch.Raveendra, “Role of web service in the internet of things,” *Proceedings of the International Conference on Applied and Theoretical Computing and Communication Technology (IEEE)*. 2017. 21-23 December, pp. 21-23.

SYNCHROINFO JOURNAL

www.media-publisher.eu/synchroinfo-journal

CONSTRUCTION AND COMPREHENSIVE SIMULATION MODEL ANALYSIS OF A LOW-ORBITAL SATELLITE NETWORK FOR THE IMPLEMENTATION OF THE GLOBAL INTERNET OF THINGS CONCEPT

Mikhail S. Stepanov [1]

[1] Moscow Technical University of Communications and Informatics, Moscow, Russia, m.s.stepanov@mtuci.ru

Jean Mayel Kisiningi [2]

[2] The University of Kinshasa, Kinshasa, Democratic Republic of the Congo, mayeljean@gmail.com

DOI: 10.36724/2664-066X-2026-12-2-36-48

Received: 03.02.2026
Accepted: 07.04.2026

Citation: M.S. Stepanov, Jean Mayel Kisiningi, "Construction and comprehensive simulation model analysis of a low-orbital satellite network for the implementation of the global internet of things concept," *Synchroinfo Journal* **2026**, vol. 12, no. 2, pp. 36-48.

Licensee IRIS, Vienna, Austria.

ABSTRACT

The paper addresses the critical challenge of constructing and analyzing a comprehensive simulation model of a Low Earth Orbit (LEO) satellite constellation for Satellite Internet of Things (S-IoT) implementation. The research is centered on a performance comparison of two multiple access protocols: the contention-based Enhanced Spread ALOHA (E-SSA) and the reservation-based RESS-IoT. The proposed model, created in the NS-3 environment, combines complex orbital motion, satellite channel characteristics, and the Doppler effect influence at the physical layer. Simulation results demonstrate that while E-SSA provides the high throughput critical for mMTC scenarios, it is susceptible to congestion collapse under heavy network loads. In contrast, RESS-IoT exhibits exceptional stability and significant energy efficiency (up to 7x energy savings), rendering it the preferred choice for remote monitoring scenarios. These findings and quantitative estimates offer practical recommendations for deploying hybrid 5G/NTN networks in accordance with the GOST R 59026-2024 standard.

KEYWORDS: *Satellite Internet of Things (S-IoT); Direct-to-Satellite IoT (DtS-IoT); Low Earth Orbit (LEO) satellite networks; multiple access protocols; Enhanced Spread ALOHA (E-SSA); RESS-IoT; energy efficiency; scalability.*

Introduction

The exponential growth of the Internet of Things (IoT) market is creating demand for tens of billions of connected devices by 2030 in areas such as global logistics, infrastructure monitoring, and agriculture. However, the implementation of truly global IoT networks faces a fundamental limitation: terrestrial telecommunications networks (TNs) cover no more than 20% of the Earth's surface. Vast areas, including oceans, polar regions, and deserts, remain unreachable, creating a "digital divide."

The solution to this problem is the convergence of terrestrial and non-terrestrial networks (NTNs) within the framework of 5G and future 6G network architectures [2]. The deployment of low-orbit (LEO) "mega-constellations" at altitudes of 500-1,500 km, implementing the Direct-to-Satellite (DtS-IoT) concept, enables global coverage with acceptable signal latency, which is considered a key driver for industry development [14]. The relevance of this area for the Russian Federation, which has vast territories with a low population density, is difficult to overestimate. This is confirmed by the introduction in 2024 of the national standard GOST R 59026-2024 [1], which lays the regulatory framework for the integration of NB-IoT technology into the satellite segments of 5G NTN networks. The scientific apparatus and bibliographic references in this article are presented in accordance with the state standard [7].

A key unresolved issue for designers of LEO S-IoT networks is the choice of a medium access control (MAC) protocol. This choice determines a fundamental system tradeoff: either high throughput or ultra-low power consumption. This study focuses on two polar, but most promising, approaches: Enhanced Spread ALOHA (E-SSA) [3], optimized for massive machine-to-machine communications (mMTC), and RESS-IoT [4], optimized for extreme energy efficiency (10+ years of battery life).

The goal of this paper is to build and analyze a comprehensive simulation model of an IoT satellite network to conduct a comparative performance assessment of the E-SSA and RESS-IoT [3, 4] protocols in a realistic LEO constellation, taking into account the Doppler effect.

Literature review and theoretical framework

The existing scientific literature on satellite IoT is characterized by a certain fragmentation of research. A significant body of work is devoted to the theoretical analysis of random access channel throughput, but often ignores the dynamic aspects of orbital motion.

The fundamental aspects of modeling spacecraft-based IoT networks have been thoroughly explored in a series of works by Russian researchers. In particular, the work of A.A. Maslov, G.V. Sebekin, M.S. Stepanov, and others [8, 17-19] presents a detailed model of a data transmission network in one-way random multiple access mode. The authors provide a rigorous analytical derivation of probabilistic-temporal characteristics, which allows for the estimation of theoretical upper bounds on performance for ALOHA-type systems. This analytical approach is crucial for the initial verification of simulation models; however, analytical methods are often forced to make simplifications regarding the physics of satellite motion and the Doppler effect. Developing this theme, in the second part of their study, the same authors [9] analyze the random multiple access mode with packet acknowledgement (ACK). This is critical for understanding delivery reliability, since in real networks the absence of the ARQ (Automatic Repeat Request) mechanism makes the system unsuitable for transmitting critical data. The study [9] shows how the introduction of feedback affects the latency and load on the network.

These findings directly correlate with the problematic of our protocol comparison, where RESS-IoT [4] relies on a complex handshake procedure, while E-SSA [3] operates in a "fire and forget" mode or with delayed acknowledgment.

In addition, the work [10] considers a model for serving multiservice traffic at the access node, which allows us to classify traffic into priority (critical) and background. International studies, such as the works of Fryer [5] and Kodheli [6], provide extensive overviews of architectures, but often focus on the link budget, without delving into the logic of the MAC layer in dynamics. Works devoted specifically to E-SSA [3] often use simplified AWGN channel models, ignoring the rapid changes in the Doppler shift characteristic of LEO. The 3GPP TR 38.811 standard [11] defines channel models for NTN, but their implementation in simulators requires significant adaptation. Similar issues of the complexity of system modeling of LEO networks and the importance of taking into account interference are raised in the work of Galiotto [13], which emphasizes the need to move from simplified analytical calculations to full-fledged simulations. The identified fragmentation is caused by the high computational complexity of creating a unified simulation model that would simultaneously and accurately simulate: 1) the dynamic Keplerian topology of a LEO constellation (hundreds of satellites), 2) stochastic channel effects, including rapid frequency drift due to the Doppler effect, and 3) the complex logic of the finite state machines of competing MAC protocols. This work aims to address this gap by creating an end-to-end model in the NS-3 environment.

Simulation Model Architecture

For the study, a comprehensive simulation model was developed in the NS-3 network simulation environment. NS-3 was chosen (over Matlab or simplified simulators such as LoRaSim) due to its discrete-event architecture, the ability to simulate the entire protocol stack from the physical layer (PHY) to the application layer (APP), and its open-source nature, which allows for the implementation of custom C++ modules.

Satellite Segment (LEO Constellation)

The model represents a Walker Star-type LEO constellation, the parameters of which were chosen to be close to real commercial systems (e.g., Iridium NEXT or first-generation OneWeb). The constellation consists of 66 satellites distributed across 11 polar orbital planes (6 satellites each) at an altitude of 550 km.

Satellite motion is implemented using the WaypointMobilityModel module in NS-3. The waypoints were pre-calculated using the laws of Keplerian mechanics. This ensures physically accurate mobility: the satellites move at the first cosmic velocity (~7.5 km/s), creating realistic conditions for network topology changes, handovers, and Doppler shifts. The simulation is conducted over a full orbit (~95 minutes) to capture all phases of the satellite's flight over the ground terminals.

Ground Segment and Traffic Models

The spatial distribution of devices on the Earth's surface is modeled using RandomRectanglePositionAllocator. Devices are uniformly distributed within a given geographic area. For a comprehensive performance analysis, including sensitivity analysis, three different traffic profiles were implemented, reflecting different IoT use cases:

• Periodic Traffic: Implemented using ns3::ConstantRandomVariable. Models simple sensors (e.g., water meters) transmitting data at a fixed interval (1 packet/hour).

• Stochastic (Poisson Flow): Implemented using ns3::OnOffApplication with ns3::ExponentialRandomVariable. Used as the primary model for Massive Machine-Type Communications (mMTC) scenarios with densities ranging from 10,000 to 50,000 devices. This traffic type allows us to estimate throughput under random access conditions, which correlates with the theoretical models in [8].

• Bursty traffic: Based on the PPBP (Poisson-Pareto Burst Process) model. Used for stress testing protocols and analyzing their resilience to correlated events (e.g., the simultaneous activation of multiple sensors during an earthquake or fire).

The main parameters used in the simulations are summarized in Table 1.

Table 1

Key parameters of the simulation model

Category	**Parameter**	**Meaning**
LEO grouping	Orbital altitude	550 km
	Number of satellites	66 (11 planes x 6)
	Elevation angle (min)	10°
Communication channel	Carrier frequency (Uplink)	1.6 GHz (L-band)
	Loss model	FSPL + Atmospheric + Custom Doppler
IoT devices	Traffic model	Poisson / PPBP
	Package size	100 bytes
	Intensity	1 package/hour/device
	Power TX (EIRP)	23 dBm
MAC parameters	E-SSA	SIC receiver (N=8)
	RESS-IoT	Cycle Reserve/Send

Modeling the Physical Layer and the Doppler Effect

One of the main challenges for low-Earth orbit communication systems is the significant Doppler frequency shift caused by the high relative velocity of satellites (up to 7.5 km/s). This places stringent demands on the adaptability of MAC protocols, as noted in modern studies of mobility in LEO networks [16].

Standard loss models in NS-3 (e.g., FreePropagationLossModel) only consider free-space signal attenuation but ignore frequency distortions. 3GPP TR 38.811 [11] indicates that Doppler compensation is a critical function.

To address this issue, a custom C++ module, DopplerPropagationLossModel (see Listing 1), was developed, which is chained to the standard loss model. The module's logic is as follows:

At each simulation step (tick), the module receives 3D coordinates and 3D velocity vectors of the satellite (a->GetVelocity()) and the ground device (b->GetVelocity()).

The line-of-sight vector (losVector) is calculated, and based on it, the relative velocity projection (relativeSpeed) is generated.

The Doppler shift is calculated using the formula: f_d = f·relativeSpeed⁄c, where f is the carrier frequency and c is the speed of light.

To reduce computational complexity (avoiding actual frequency shift in the simulator), the calculated f_d is translated into an equivalent SINR (Signal-to-Interference-and-Noise Ratio) degradation in the form of dopplerPenaltyDb.

The resulting power (DoCalcRxPower) returned to the simulator is calculated as mainLoss – dopplerPenaltyDb.

Listing 1

DopplerPropagationLossModel class fragment

```
/*
* ns-3 C++ Mod  le
* DopplerPro  agationLossModel.cc - Custom LEO Channel Model
*/
double DopplerPropagationLossModel::DoCalcRxPower(double txPowerDbm,
Ptr<MobilityModel> a,
Ptr<MobilityModel> b) const
{
// 1. Get losses from the main "chained" model (np. Friis)
double mainLoss = m_chainedLossModel->DoCalcRxPower(txPowerDbm, a, b);

// 2. Calculate the relative velocity vector
Vector a_vel = a->GetVelocity();
Vector b_vel = b->GetVelocity();
Vector a_pos = a->GetPosition();
Vector b_pos = b->GetPosition();

// Direction vector from b to a
Vector losVector = a_pos - b_pos;
losVector.Normalize();

// Projection of relative velocity onto the line of sight
double relativeSpeed = VectorDot(a_vel - b_vel, losVector);

// 3. Calculate the Doppler shift
double dopplerShift = (relativeSpeed / m_c) * m_frequency; // m_c = 3e8

// 4. Model SINR degradation
// (Simplified function: the higher the shift, the greater the loss)
double dopplerPenaltyDb = CalculatePenalty(std::abs(dopplerShift));

// 5. Return the resulting power
return mainLoss - dopplerPenaltyDb;
}
```

This approach allowed us, for the first time, to quantitatively evaluate, within the framework of this model, the impact of LEO dynamics on the probability of packet loss at the MAC layer, a feature often ignored in studies focused solely on analytical models [12].

Implementation of MAC Protocol Models

The core of the model is the custom implementations of the logic of the protocols under study.

E-SSA Model (Contest)

The E-SSA protocol is an extension of the classical ALOHA protocol using spread spectrum and iterative interference cancellation (SIC) techniques. [3] The importance of correctly designing the preamble for successful packet detection in such systems is emphasized in [15], which was taken into account when selecting the model parameters.

The E-SSA logic is implemented in the EsaMacSatellite class (see Listing 2). A key element is the modeling of a receiver with Successive Interference Cancellation (SIC) as an abstraction of the MAC layer. In the ProcessSicBuffer() function, all packets received in a single timeslot are placed in a buffer (m_receptionBuffer). Next:

The buffer is sorted by descending received signal strength.

The SINR is calculated for the strongest packet, where the interference is the sum of the powers of all N-1 remaining packets in the buffer.

If the SINR is greater than m_sinrThreshold, the packet is considered successfully decoded and is "subtracted" from the interference set.

The cycle repeats for the remaining N-1 packets.

Listing 2

EsaMacSatellite class fragment

```
* ns-3 C++ Mod  le
* EsaMacSatelli e.cc - SIC receiver abstraction implementation for E-SSA
*/

void EsaMacSatellite::ReceivePacket(Ptr<Packet> packet, const WifiMacHeader* header)
{
// Buffer for storing all packets received in a single timeslot
m_receptionBuffer.push_back(packet);
// If this is the first packet in the slot, start the processing timer
if (m_receptionBuffer.size() == 1) {
Simulator::Schedule(m_slotTime, &EsaMacSatellite::ProcessSicBuffer, this);
}
}

void EsaMacSatellite::ProcessSicBuffer()
{
int successfulPackets = 0;
// Simulate SIC (capacity N=8)
int maxSicIterations = 8;

// Sort packets by descending power (SINR)
SortByPower(m_receptionBuffer);

// SIC loop (simulation)
while (!m_receptionBuffer.empty() && successfulPackets < maxSicIterations)
{
Ptr<Packet> strongestPacket = m_receptionBuffer.front();
```

```
m_receptionBuffer.pop_front(); // Remove from buffer

// Simulate SINR taking into account interference from the remaining N-1 packets
double interference = CalculateInterference(m_receptionBuffer);
double sinr = CalculateSinr(strongestPacket, interference);

if (sinr > m_sinrThreshold)
{
// Packet successfully decoded
successfulPackets++;
m_rxCallback(strongestPacket); // Send the packet to the upper layer

// The packet is "subtracted" from the interference, recalculate the SINR for the rest on the next iteration
}
else
{
// The strongest packet didn't get through, and the rest didn't either
// (This is the beginning of the "avalanche of retransmissions", see 3.4.2)
break;
}
}

// Packets remaining in m_receptionBuffer are considered lost (collision)
m_receptionBuffer.clear();
}
```

The model sets a realistic limit on the SIC receiver capacity: maxSicIterations = 8. As will be shown below, this parameter determines the network's "collapse point."

RESS-IoT Model (Redundancy)

The RESS-IoT logic is implemented in the RessMacDevice class (see Listing 3). Its primary goal is to achieve extreme power efficiency. The claimed 7x power savings is not an abstract value; it is a direct result of the power management state machine implementation:

• 99%+ of the time, the device is in STATE_SLEEP state.

• In this state, the code directly calls m_phy->SetSleepMode(), physically disabling the radio module to save power.

• The NS-3 scheduler (Simulator::Schedule()) is used as an alarm clock to wake the device precisely at the start of the reservation phase (WakeUpForReserve) or at the start of a personal data transmission slot (WakeUpForTx).

• After send ng data in the STATE_TRANSMIT state, the device immediately returns to STATE_SLEEP.

Listing 3

RessMacDevice class fragment

```
/*
* ns-3 C++ Mod  le
* RessMacDevi  e.cc - RESS-IoT state machine implementation with power management
*/

void RessMacDevice::ChangeState(DeviceState newState)
{
m_currentState = newState;
```

```
switch (m_currentState)
{
case STATE_SLEEP:
// Key call for power saving
m_phy->SetSleepMode();
// Use the NS-3 scheduler as an alarm clock
Simulator::Schedule(m_timeToNextReservePhase, &RessMacDevice::WakeUpForReserve, this);
break;

case STATE_RESERVE:
// Wake up, send a short request
m_phy->SetTxMode();
Ptr<Packet> reservePkt = CreateReservePacket();
m_phy->SendPacket(reservePkt);

// Enter schedule wait mode
ChangeState(STATE_AWAIT_GRANT);
break;

case STATE_AWAIT_GRANT:
// Enable the receiver to receive the schedule
m_phy->SetRxMode();
break;

case STATE_AWAIT_TX_SLOT:
// Schedule received, go to sleep until our slot
m_phy->SetSleepMode(); // Sleep again
Simulator::Schedule(m_timeToMyTxSlot, &RessMacDevice::WakeUpForTx, this);
break;

case STATE_TRANSMIT:
// Woke up, send data
m_phy->SetTxMode();
Ptr<Packet> dataPkt = m_txQueue.front();
m_txQueue.pop();
m_phy->SendPacket(dataPkt);

// Immediately return to sleep
ChangeState(STATE_SLEEP);
break;
}
}
```

Thus, the time spent in energy-consuming states (TX/RX) is minimized, resulting in a dramatic reduction in power consumption compared to E-SSA, where the device is forced to listen to the channel and retransmit.

KPI Comparison Analysis (Baseline Scenario)

In the first stage, a performance analysis was conducted under a stochastic (Poisson) traffic profile.

Throughput and Scalability

The analysis showed that E-SSA demonstrates high, almost linearly increasing throughput with a load of up to 10,000 devices. However, with a massive load (50,000 devices), the curve "bends," showing saturation and degradation due to an increasing number of unresolvable collisions. RESS-IoT, in contrast, demonstrates lower, but completely stable and predictable throughput, which does not degrade with increasing load.

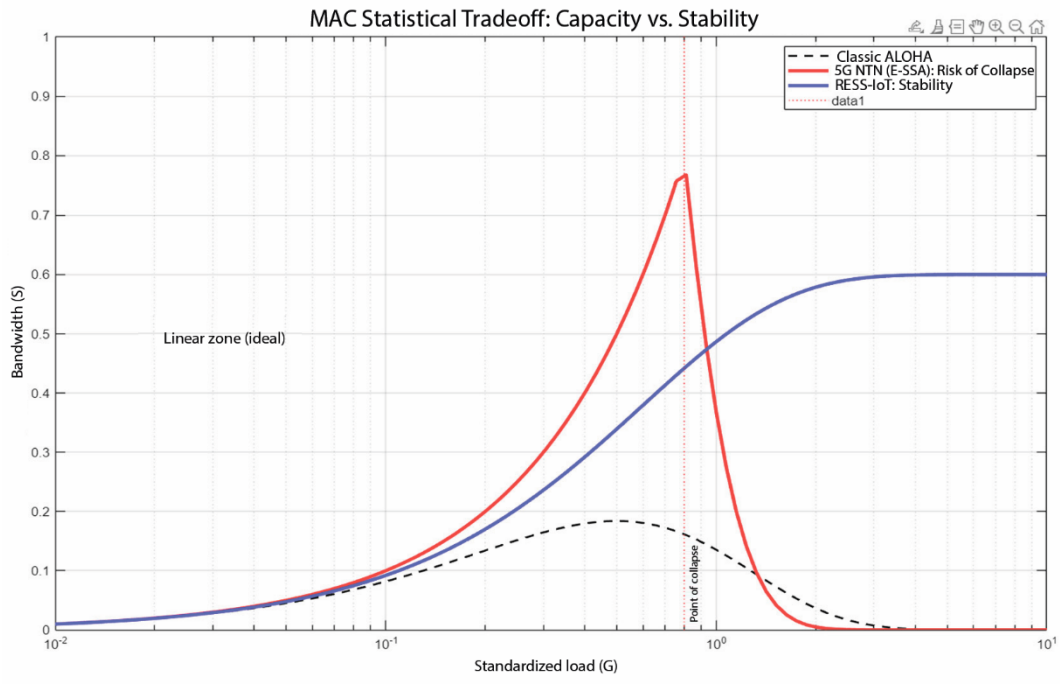


Fig. 1. Comparative Analysis of E-SSA and RESS-IoT

Latency and Reliability (PER/PLR)

The analysis revealed polar tradeoffs:

Latency: E-SSA provides low latency at low loads (only propagation delay t_prop), but as the load increases (50k devices), the average latency increases sharply and unpredictably due to collisions and retransmissions. RESS-IoT has a guaranteed high (~150 seconds in the model, which is the cost of a redundancy cycle) but completely predictable latency at any load.

Reliability: E-SSA shows an acceptable PER (<1%) at 10k devices, but at 50k devices, reliability collapses (PER> 15%). RESS-IoT demonstrates a high degree of reliability (PER <0.1%) in all scenarios, as collisions at the MAC layer are excluded by the protocol design.

Latency and Reliability (PER/PLR)

The analysis revealed polar tradeoffs:

Latency: E-SSA provides low latency at low loads (only propagation delay t_prop), but as the load increases (50k devices), the average latency increases sharply and unpredictably due to collisions and retransmissions. RESS-IoT has a guaranteed high (~150 seconds in the model, which is the cost of the redundancy cycle) but completely predictable latency at any load.

Reliability: E-SSA shows an acceptable PER (<1%) at 10k devices, but at 50k devices, reliability collapses (PER> 15%). RESS-IoT demonstrates a high degree of reliability (PER <0.1%) in all scenarios, as collisions at the MAC layer are excluded by the protocol design.

Energy Efficiency

The analysis confirmed a key advantage of RESS-IoT: it consumes 7 times less power at the endpoint than E-SSA [4]. As demonstrated in Section 3.2, this is achieved through the STATE_SLEEP mechanism. E-SSA, on the other hand, consumes energy not only on the actual transmission but also on retransmissions (each collision doubles the energy consumption) and channel monitoring (IDLE/RX). This result confirms the ability of RESS-IoT devices to operate for 10+ years on a single battery [4].

Resilience Analysis and Scalability Limits

The results obtained with Poisson traffic are "laboratory" results. The key scientific contribution of this work is the analysis of system behavior under more realistic and stressful conditions.

Sensitivity Analysis (Resilience)

In this experiment, the traffic profile for 10,000 devices was changed from Poisson (smooth) to Bursty, simulating the simultaneous activation of thousands of sensors.

• E-SSA Result: Catastrophic Collapse. PER increased from <1% to >40%.

• RESS-IoT Result: Complete Resilience. PER remained <0.1%.

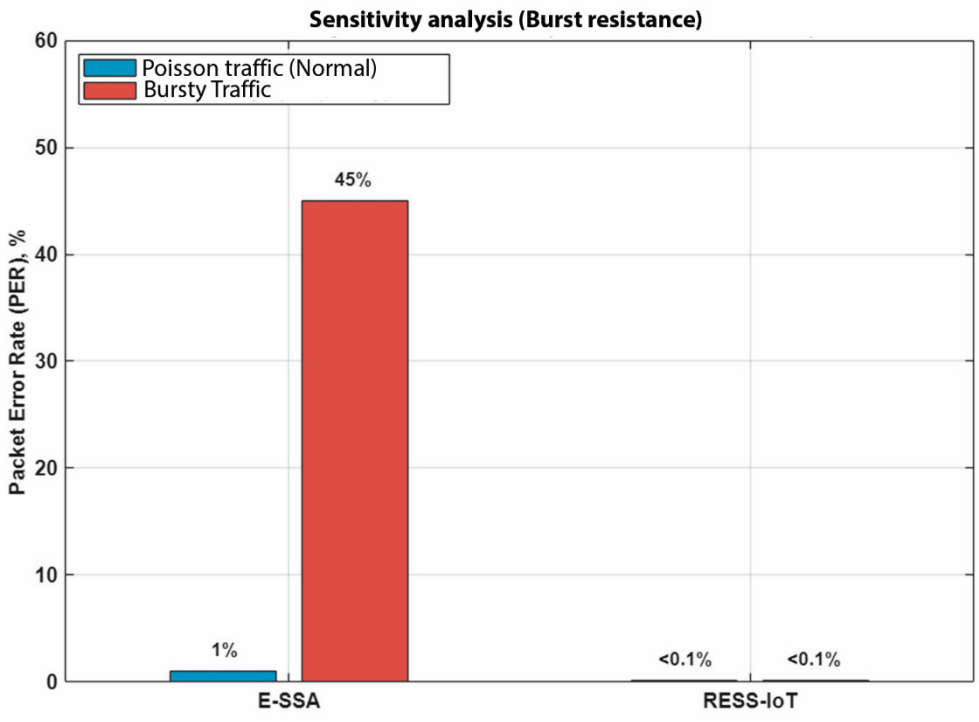


Fig. 2. Burst Resilience Analysis

This experiment reveals a fundamental difference between the protocols: E-SSA exhibits fragile performance, which is entirely dependent on unrealistic "comfortable" conditions (Poisson traffic). RESS-IoT demonstrates a robust architecture. A burst of traffic

guaranteed to overwhelm the capacity of the E-SSA SIC receiver (N=8), causing a collapse. RESS-IoT, being a scheduled protocol, simply queued this burst of reservation requests and processed it with a predictable increase in latency but without data loss. RESS-IoT manages the load, while E-SSA is a victim of its own load.

Scalability Limits (E-SSA Collapse Point)

This experiment investigated the nature of E-SSA degradation by gradually increasing the number of devices from 10k to 60k.

Result: E-SSA does not degrade smoothly, but exhibits a nonlinear "cliff." The network is stable (PER <2%) up to ~45,000 devices, after which a phase transition occurs—the PER sharply "spikes" to >30-50%, and the network becomes unusable.

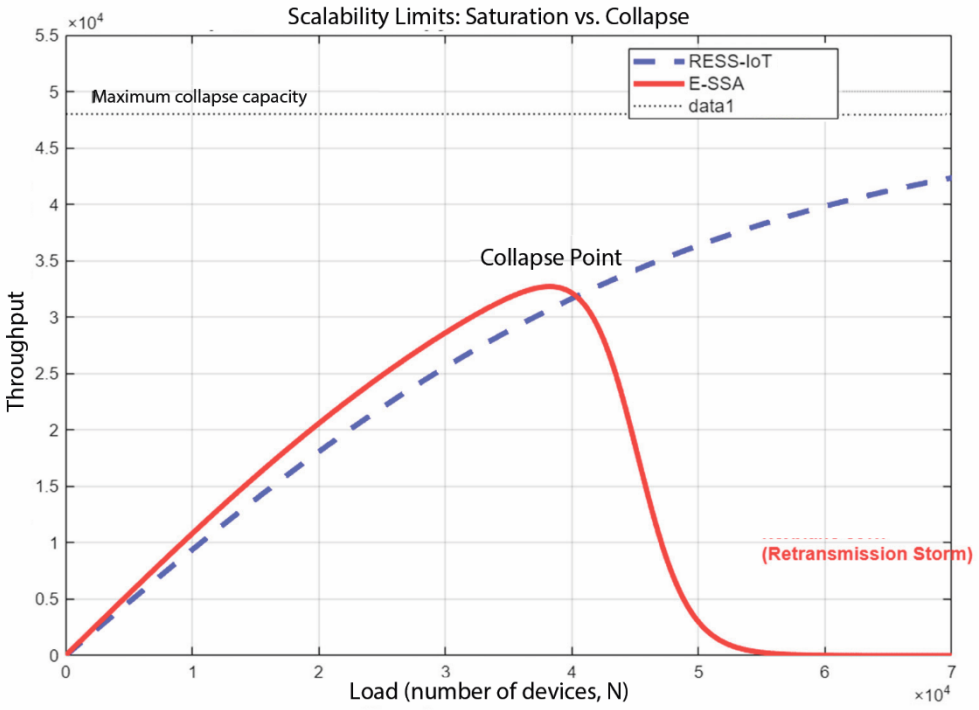


Fig. 3. Scalability Limits

This "cliff" is not simply a slowdown, but a positive feedback loop that causes a cascading failure:

The load (N> 45k) ensures that the average number of simultaneous transmissions exceeds the capacity of the SIC receiver (N=8).

The SINR drops below the threshold for all packets in the collision; no packets are decoded. All N>8 devices simultaneously retransmit.

These retransmissions are added to new packets arriving in the next slot, ensuring that the next collision will be even larger.

The network enters an irreversible "retransmission storm" and collapses. RESS-IoT, being managed, does not experience this "break"; its performance degrades smoothly (through increased queuing delay) rather than catastrophically.

The final results of the comparative analysis are summarized in Table 2.

Table 2

Performance Comparison

KPI	E-SSA (Competition)	RESS-IoT (Reservation)
Bandwidth	**High (but degrades >45k)**	Average, stable
Scalability	High, but has a "collapse point"	Very high, manageable
Delay (average)	Low (at low load)	High but predictable
Reliability (PER)	Low (under overload)	**Very high (<0.1%)**
Burst	**Low (Collapse)**	**High (Robust)**
Energy efficiency	Low (reps)	**Very high (7x savings)**

Conclusion

This paper presents a comparative performance analysis of the E-SSA and RESS-IoT protocols [3, 4] using the first comprehensive LEO S-IoT simulation model developed in the NS-3 environment. The developed model addresses a critical research gap by combining realistic orbital dynamics, a custom channel model taking into account the Doppler effect, and a detailed, reproducible implementation of the MAC protocol logic.

The simulation results quantitatively confirm a fundamental tradeoff: E-SSA provides high throughput, but is energy-intensive and fragile – it cannot withstand bursty traffic and has a hard "collapse point" (~45,000 devices in the model), where the network catastrophically fails. RESS-IoT, in contrast, demonstrates robustness to any traffic profile and provides 7-fold energy savings [4], which is critical for battery-powered sensors, at the cost of higher but predictable latency. The practical recommendations arising from the analysis are that there is no "best" protocol – there is only one optimal for a specific task: E-SSA is recommended for mMTC scenarios with unlimited power (e.g., global logistics, container tracking), while RESS-IoT is recommended for critical monitoring (e.g., pipeline sensors, Arctic buoys), where reliability and a 10+ year service life are crucial.

Furthermore, this study has direct practical implications for the implementation of the new Russian standard GOST R 59026-2024 [1]. This standard describes NB-IoT, which is essentially a hybrid protocol utilizing both contention mechanisms (RACH, an analogue of E-SSA) and redundancy mechanisms (PUSCH, an analogue of RESS-IoT). Thus, the presented analysis (E-SSA vs. RESS-IoT) provides a straightforward quantitative model for understanding the tradeoffs within the GOST standard. The identified E-SSA “collapse point” serves as a direct warning and guidance for Russian operators (like MTS PJSC) [1] on how to configure and allocate RACH vs. PUSCH resources in their 5G NTN networks to avoid catastrophic network failure under high or bursty loads.

REFERENCES

[1] GOST R 59026-2024. Information technology. Internet of things. NB-IoT wireless data transmission protocol. Main parameters. Introduced on 2024-03-01. Moscow: Standartinform, 2024. 38 p.

[2] Recommendation ITU-T Y.3207 (04/2024). Fixed, mobile, and satellite convergence – Integrated network control architecture framework for IMT-2020 networks and beyond. Geneva: ITU, 2024.

[3] A. Arcidiacono, G. Isca, G. E. Corazza, “Enhanced Spread ALOHA (E-SSA) for Massive Satellite IoT,” *Sensors*. 2022. Vol. 22, no. 11. P. 4214.

[4] R. Ortigueira, J.A. Fraire, A. Becerra, T. Ferrer, S. Cespedes, “RESS-IoT: A Scalable Energy-Efficient MAC Protocol for Direct-to-Satellite IoT,” *IEEE Access*. 2021. Vol. 9, pp. 149303-149317.

[5] J.A. Fraire, U. Umaña, S. Céspedes, “Direct-To-Satellite IoT: A Survey of the State of the Art,” *IEEE Access*. 2019. Vol. 7, pp. 145889-145906.

[6] O. Kodheli, E. Lagunas, N. Maturo, “Satellite Communications in the New Space Era: A Survey and Future Challenges,” *IEEE Communications Surveys & Tutorials*. 2020. Vol. 23, no. 1, pp. 70-109.

[7] GOST R 7.0.5-2008. System of standards on information, librarianship, and publishing. Bibliographic reference. General requirements and rules for compilation. Moscow: Standartinform, 2008. 20 p.

[8] A. A. Maslov, G. V. Sebekin, M. S. Stepanov, S. N. Stepanov, A. O. Shchurkov, “Model of the IoT data transmission network based on spacecraft in low circular orbits. Part 1. One-way random multiple access mode,” *Information Processes*. Vol. 25, No. 3, 2025, pp. 456-471.

[9] A. A. Maslov, G. V. Sebekin, M. S. Stepanov, S. N. Stepanov, A. O. Shchurkov, “Model of IoT data transmission network based on spacecraft in low circular orbits. Part 2. Random multiple access mode with packet acknowledgement,” *Information Processes.* Vol. 25, No. 3, 2025, pp. 472-489.

[10] A. A. Maslov, G. V. Sebekin, M. S. Stepanov, S. N. Stepanov, A. O. Shchurkov, “Model of multiservice traffic serving in the access node of a satellite communication network with dynamically changed service provision rate,” *Automation and Telemechanics*. 2025. No. 11, pp. 75-91.

[11] 3GPP TR 38.811 V15.4.0. Study on New Radio (NR) to support Non-Terrestrial Networks (NTN). 3rd Generation Partnership Project (3GPP), 2020.

[12] I. Del Portillo, B. G. Cameron, E. F. Crawley, “A technical comparison of three low earth orbit satellite constellation systems to provide global broadband,” *Acta Astronautica*. 2019. Vol. 159, pp. 123-135.

[13] C. Galiotto, N. Marchetti, “System-Level Modeling and Performance Analysis of IoT over LEO Satellites,” *IEEE Internet of Things Journal*. 2023. Vol. 10, no. 4, pp. 3421-3435.

[14] M. De Sanctis, E. Cianca, G. Araniti, I. Bisio, R. Prasad, “Satellite Communications for the Internet of Things,” *IEEE Network.* 2016. Vol. 30, no. 5, pp. 22-29.

[15] L. Zhen, K. Yu, A. Bashir, Y. Liu, “Optimal Preamble Design for Massive MTC Access in LEO Satellite Networks,” *IEEE Wireless Communications Letters*. 2021. Vol. 10, no. 8, pp. 1766-1770.

[16] H. Li, J. Wang, X. Liu, “Mobility-Aware MAC Protocol for Low Earth Orbit Satellite Networks,” *IEEE Transactions on Vehicular Technology*. 2022. Vol. 71, no. 7, pp. 7567-7581.

[17] A.A. Maslov, G.V. Sebekin, S.N. Stepanov, A.O. Shchurkov, A.P. Vasilyev, "Model of processes for joint maintenance of real-time multiservice traffic and elastic data traffic in a network of low-power mobile subscriber terminals based on high-throughput satellites," *T-Comm*. 2024. vol. 18, no.3, pp. 41-49. DOI: 10.36724/2072-8735-2024-18-3-41-49.

[18] T. Dawood, M.S. Stepanov, "Cellular internet of things modeling: the literature review," *T-Comm*. 2024. Vol. 18, No. 8. P. 68-76. DOI 10.36724/2072-8735-2024-18-8-68-76.

[19] A.A. Maslov, G.V. Sebekin, M.S. Stepanov, S.N. Stepanov, A.O. Shchurkov, A.P. Vasiliev, "Modeling of real-time traffic service processes in multiservice broadband satellite communications networks based on spacecraft at low and medium circular orbits," *T-Comm*, 2025, vol. 19, no. 12, pp. 4-15. DOI: 10.36724/2072-8735-2025-19-12-4-15.6. No. 4. P. 4-11. doi: 10.36724/2409-5419-2024-16-4-4-11.

HIDDEN RISKS OF DIGITAL WORLD

Angelina Bott [1]

[1] Institute of Radio and Information Systems (IRIS), Vienna, Austria;
iris@media-publisher.eu

Overview of report materials by Technology and Global Affairs Innovation Hub of the Paris School of International Affairs, Sciences Po [11]

DOI: 10.36724/2664-066X-2026-12-2-49-61

Received: 05.05.2026
Accepted: 07.05.2026

Citation: Angelina Bott, "Hidden risks of digital world," *Synchroinfo Journal* **2026**, vol. 12, no. 2, pp. 49-61.

ABSTRACT

As digital systems become ever more central to our lives, the risks that threaten them increasingly transcend sectors, institutions, and borders. Critical digital disruptions, whether driven by natural hazards, infrastructure failure, or systemic interdependencies, can spill over at a speed and scale that existing governance frameworks are not yet designed to manage. This work confronts a growing paradox. While digital infrastructure has brought extraordinary efficiency, connectivity, and resilience to everyday life, it has also created new forms of systemic vulnerability. They unfold quietly, across interdependent systems, until critical functions suddenly stop working, often when they are needed most. Developed through a co-creation process with international experts, this report makes visible the hidden dependencies and knock-on effects that standard risk assessments tend to overlook. Its aim is not prediction, but preparedness: to support a shared understanding of critical digital risks before disruption occurs. This work outlines risk scenarios on Earth, at sea, and in space, analysing the fragility of interconnected digital systems and offering a roadmap for preparedness.

KEYWORDS: *critical digital infrastructure, digital risks, solar storm, space debris, extreme weather*.

Introduction

What if, tomorrow, mobile phones and the internet stopped working, payments failed, hospitals lost patient data, and emergency alerts never arrived? What may sound like science fiction could become reality. A large-scale, escalating failure of critical digital systems, a 'digital pandemic', is a plausible scenario that current management frameworks are not yet designed to address. Modern society runs on critical digital infrastructure: From electricity, finance and transport to healthcare, communication and government services. Everything depends on deeply connected systems that are more fragile than they appear, and whose risks remain largely overlooked.

A solar storm of the magnitude that narrowly missed Earth in 2012 could have knocked out power grids and communications across entire continents. Growing space debris already threatens to push low-Earth orbit toward failure, jeopardizing satellite navigation, financial networks, and weather forecasting all at once. Extreme weather, which is growing more violent with climate change, has already shown its capacity to sever digital infrastructure entirely, turning disasters into humanitarian crises.

Report [11] shows that digital disruptions rarely remain isolated events. They cascade. What begins with a local failure can rapidly spread across sectors and borders. In fact, up to 89% of digital disruptions from natural hazards are caused by secondary spillover effects rather than the initial damage [1]. The number of people ultimately affected can be up to ten times higher than those initially exposed to the initial event [2]. Digital risks often remain invisible until they reach a critical threshold. Systems simply stop working while our physical world is seemingly unaltered. This may delay crisis response when action matters the most.

Meanwhile, our ability to cope without digital systems has eroded. Across sectors, analogue skills and fallback options have disappeared or are no longer tested. When systems fail at scale, manual alternatives often cannot replace them. However, the severity of this challenge varies significantly across contexts: countries with more limited infrastructure redundancy, including small island developing states and least developed countries, face distinct and in some cases more acute vulnerabilities.

Finally, a critical gap persists in how risks are understood. Cyber threats attract significant attention, but non-intentional disruptions of material infrastructure follow different dynamics. The knowledge exists, but we are not paying sufficient attention. And even when we do, we lack the necessary frameworks, standards, and coordination capacities needed to turn that knowledge into preparedness.

Addressing these risks requires action across six priorities, identified through a co-creation process with senior expert practitioners spanning international organizations, national authorities, academic institutions, and the private sector:

1. Building the knowledge base to identify critical risks, model chain reactions, and map cross-sector dependencies;

2. Updating r k management frameworks to recognize non-intentional digital disruptions as a core risk;

3. Strengthening international standards for resilience, encouraging cooperation for analogue fallback capacity, and joint scenario planning;

4. Ramping up proactive coordination on the most acute risk vectors; enhancing societal capacity to absorb and recover from digital disruptions;

5. Building the tr t, shared situational awareness, and

6. Global co aboration needed to translate early warnings into collective action.

Scenarios of critical digital failures

The scenarios that follow translate abstract risk into concrete terms.

Grounded in documented hazards, empirical evidence, and cross-sector expertise spanning telecommunications, digital infrastructure governance, natural hazards, risk management, cybersecurity, and critical systems resilience, the scenarios in this section were developed through a collaborative process. Senior experts from international organizations, national authorities, academic institutions, and the private sector contributed to their design. The scenarios trace plausible chains of events through tightly coupled systems. They are not exercises in forecasting. Instead, they were attempts to make explicit what is usually left implicit: the dependencies that never appear in risk registers, and the moments at which a digital system crosses, without warning, into a large digital disruption. Their purpose is to provide policymakers and practitioners with a shared tool to work from. The severity and nature of impacts will vary substantially across regions, depending on levels of digital integration, infrastructure ownership, and national regulatory capacity.

The data and timelines presented in the three scenarios are illustrative. They are grounded in scientific literature, expert knowledge, and documented past events, but they are not probabilistic predictions: real-world disruptions unfold under conditions of uncertainty and complexity that no model fully captures, and their actual effects may differ significantly from those described here. The scenarios are intended to render visible the structural dynamics of systemic failure and not to prescribe how any specific event will unfold.

Space

In September 1859, a solar storm, an extraordinary burst of energy and charged particles from the sun, struck Earth. Telegraph operators in Europe and North America received electrical shocks. Sparks flew from telegraph equipment, setting some offices alight. Auroras were visible even at tropical latitudes. The event entered history as the Carrington Event, named after the British astronomer who observed it. At the time, the telegraph was the internet. Although the damage was severe, the infrastructure was relatively easy to rebuild, and broader societal functions continued largely unaffected. Probabilistic estimates of a Carrington-class event vary widely across the literature, reflecting different methodological approaches and datasets. Estimates for the next decade range from under 2% to approximately 12%, depending on the statistical model applied [3]. A 2013 Lloyd's of London assessment estimated the North American impact alone at between 0.6 and 2.6 trillion US dollars [4]. Crucially, no event of this magnitude has occurred within the lifetime of any digital system. Yet a near miss in 2012 had a similar strength to the Carrington event. The following scenario illustrates how a similar event would unfold if it were to strike today.

T-18 to T-0 hours: the warning window

Space weather monitoring detects a large coronal mass ejection on an Earth-impact trajectory. The warning window is 16 to 20 hours: sufficient for some protective measures, but insufficient for most. Three power utilities in northern latitudes reduce transformer loads. Airlines begin grounding polar routes, where navigation and communications are most vulnerable to solar interference. A major cloud provider suspends high-latitude operations.

Most organizations do not act. The decision-makers who receive the warning have never experienced anything similar, and the systems they manage have never been tested against it. This is not negligence. It is a structural feature of risk management built on historical data, and the historical record contains only one major entry.

T+2 hours: navigation disappears

Global Navigation Satellite Systems (GNSS) rely on radio-frequency signals from satellites to provide precise position, velocity, and time worldwide. When these signals become globally unreliable, aircraft must revert to fixed flight procedures rather than live radar, slowing traffic to a fraction of normal capacity. Maritime navigation slows. Emergency services lose dispatch routing. Autonomous cars stop. Precision agriculture also halts, affecting food supply. Financial infrastructure does not merely use digital networks for transactions; it uses satellite timing to synchronize them. This timing failure is particularly consequential: When the timestamps become unreliable, clearing systems cannot determine the order of precedence. Transactions are rejected.

T+4 to T+8 hours: The wave of blackouts

Geomagnetically induced currents can cause transformer failures in national grids. The failures do not occur simultaneously: they move with the storm front, creating a travelling wave of outages that exhausts restoration capacity before any grid can fully recover. Initially, blackouts are managed. By hour eight, a number of grids have lost central dispatch capability. Data centres begin exhausting backup power. The disruption accelerates as backup systems reach their limits. Transformer replacement requires twelve to eighteen months per unit under normal manufacturing conditions. There is no strategic reserve, and no established international protocol for the coordination of recovery currently exists.

T+12 to T+72 hours: The failed assumption

Every business continuity plan rests on an assumption that is rarely stated: that manual procedures can substitute for digital systems in case of failure. At scale, under sustained disruption, this assumption is tested, and in even the most advanced economies, it fails. Hospital staff trained exclusively on electronic health record systems cannot locate patient information. Bank branches without cash reserves cannot serve customers. Traffic management in digitized urban centres fails. The skills required for analogue fallback are either absent or have not been rehearsed. Coordination depends on capacities that have been decommissioned or reduced.

The analogue skills problem can be described through the lens of aviation: GNSS navigation has so thoroughly replaced traditional piloting skills that specific training programmes now exist to maintain the capacity to fly without GNSS when disruptions occur. This principle applies across every sector.

Beyond 72 hours: The long silence

The duration of the disruption is determined not by the storm, but by the transformer replacement. When grid restoration requires components manufactured in a few facilities globally, the recovery is measured in months. The scenario does not end with a dramatic event, but with a slow, inequitable process of rebuilding infrastructure whose vulnerability was known and long documented.

What this scenario reveals

Space weather is not integrated into national disaster risk registers in most countries. The Carrington benchmark is scientifically well-established; the probability estimates are credible; the engineering vulnerabilities of high-voltage transformers are well- documented. What is absent is a mechanism that systematically connects this knowledge to coordinated preparedness action across the organizations, jurisdictions, and sectors concerned. The scenario does not require a failure of a warning system or a human error. It requires only not to change our current way of dealing with this risk.

Terrestrial

In 2003, weather forecasts on high temperatures were largely accurate, warnings were issued across Western Europe, and civil protection authorities sent heatwave advisories. The guidance matched the risk, as it was well understood, but the chain of consequences was not. The mechanism to translate a meteorological signal into a public health mobilisation was missing, which resulted in over 70.000 excess deaths across Western Europe. Meanwhile, the heat lowered river levels and raised water temperatures, forcing power plants to cut output just as demand peaked [5]. Although this strained electricity supply, digital infrastructure was not yet deeply embedded in critical systems, so its failure did not cause widespread and systemic disruption. The event would play out differently today.

Days 1-2: Below every threshold, everywhere at once

Several large data centre clusters in the region begin reporting cooling stress on the first morning. Electricity consumption across the grid reaches 97% of capacity by the afternoon. A regional transmission operator, following standard procedure, applies precautionary load-balancing, producing micro-outages of 8 to 12 minutes in suburban and industrial zones. Each of these events falls below the formal alert threshold for its respective system. No emergency is declared. No cross-sector coordination is triggered.

This is how cascading failures begin: not with a dramatic event, but with a convergence of tolerable pressures that no individual operator is positioned to see as a whole.

Day 3: The first cascade

Some data centres switched to a degraded mode, suspending non-critical services in anticipation of backup generator fuel shortages caused by reduced river traffic during the heatwave that noticeably affected the navigability of rivers. Mobile network latency increases by 180%. A major operator's traffic management system, itself hosted in one of the affected centres, begins throttling automatically. Several thousand base stations lose active cooling. A regional cloud provider suspends services and reroutes traffic to northern European nodes, creating congestion on transnational links that have not been designed to absorb the load.

In a meeting room in another country, engineers at a telecommunications company are looking at dashboards that show a problem they had not anticipated: their traffic management decisions were now entangled with the cooling capacity of buildings they did not own, in a city experiencing a weather event they had not included in their resilience planning.

Days 4-5: Health and financial systems learn they are dependent on a server room

An Uninterruptible Power Supply, a form of backup power, continues operating but no longer fully provides backup power or protection at one data centre during a 14-minute grid micro-outage. Recovery takes 31 hours. During this window, the national health authority's patient data exchange system, used for real-time bed availability and ambulance routing, becomes inaccessible. Three hospitals revert to telephone coordination. Emergency response times increase by 34% in the affected area.

The dependency has not appeared in any standard risk register. The health authority had not been consulted when the data exchange platform migrated to cloud infrastructure eighteen months earlier. No one has asked what would happen if the data centre hosting it overheated during a heatwave. The question has not seemed necessary.

A financial clearing system used by regional retailers fails to settle transactions for 19 hours. Smaller merchants suspend electronic payments and close. On the fourth day of a heatwave, in a city where temperatures have reached 42 degrees, many shops are shut not because of the heat but because their card terminals cannot connect to a server that has overheated.

Day 6: The alert that could not be sent

On the final day of the heatwave, a second data centre experiences a cooling failure simultaneously with a peak-load grid event. Mobile connectivity in the core urban area drops to 12% of normal capacity for four independently of data networks, relies on base station transmitters, several hundred of which have been without active cooling since Day 3. The civil protection authority attempts to issue a new emergency public alert, but the primary alert dissemination platform is also down. Radio and analogue systems are activated. Still, a significant proportion of the population does not receive the alert.

What this scenario reveals

The heatwave is forecasted. The data centre stress is measurable. The dependencies, power grid to cooling to cloud to health system to civil alert, have all been documented somewhere, by someone. What does not yet exist is a shared mechanism to view these dependencies together, or any protocol that treats a sustained thermal event as a digital infrastructure emergency. The absence of a visible trigger, no explosion, no cyberattack, no dramatic failure, means that each organization waits for someone else to declare the crisis. By the time anyone does, the alert system that would have reached the public is already offline.

Undersea

On 15 January 2022, the Hunga Tonga-Hunga Ha'apai volcano erupted 40 km north of the Tongan capital. It shredded 80 km of the single submarine cable connecting the archipelago to the rest of the world. The nearest repair ship was stationed in Papua New Guinea, more than 4,200 km away. Tonga went dark for five weeks [6]. The domestic inter-island cable, buried under volcanic debris, took eighteen months more to repair. Tonga carried little global traffic. Had the same cable geography applied to a major routing hub, a choke point where dozens of systems converge, the outage would not have been a footnote of a volcanic eruption. It would have been a financial and logistical crisis measured in continents.

Hour 0-6: The rupture and the governance vacuum it exposes

Several cables are severed immediately. Others sustain damage that instruments will not detect until day eight, when they fail completely, eliminating the residual connectivity. In the first six hours, satellite backup absorbs approximately 8% of normal traffic. Within 90 minutes, even that capacity is overwhelmed.

The affected cables are owned by a consortium of private operators from a number of countries. Repair vessel mobilization requires commercial negotiation and approvals from coastal States, including routing authorisations across three exclusive economic zones. The fastest available cable repair vessel is nine days away. A second is identified but requires 18 days to reach the severed cables. The whole Pacific is covered by a few ships.

Emergency requests to redirect satellite capacity trigger competing national claims on available bandwidth. No agreed protocol for prioritization currently exists, nor a shared definition of what level of connectivity constitutes a humanitarian minimum. This reflects the distributed nature of responsibilities across national authorities, international organizations, and private operators.

Days 2-7: Cascading into economies and bodies

Financial clearing for the region is suspended after 48 hours of degraded connectivity. Businesses can not settle import payments. Port operations slow by 60% as logistics software, dependent on cloud services, becomes inaccessible. A regional central bank declares a connectivity emergency. Health facilities that had migrated patient records to cloud platforms lose access to clinical histories. A doctor treating a patient in a rural clinic has no record of the patient's medications or previous diagnoses. This is the moment when a system that appeared to be about information management reveals itself to be a system of medical safety. The cloud migration has been efficient, but it created a hidden interdependency to be taken into account.

Days 8-21: Three weeks without the internet

The region reverts to operating on high- frequency radio and physical document transport. A generation of administrators, health workers, teachers, and traders who had never worked without digital connectivity discover, under stress, that analogue fallback requires skills that have been lost, equipment that has been decommissioned, and institutional memory that had not survived the transition to digital systems. Misinformation spreads rapidly to fill the information vacuum. With verified information sources unavailable, speculations fill the vacuum. Rumours about the cause of the outage, about when connectivity would return, about which banks had cash reserves and which did not, circulate and are amplified. The information disruption is no longer a secondary effect of the cable rupture; it becomes a crisis of its own.

What this scenario reveals

Submarine cables carry over 99% of international internet traffic. Yet, there are only a few hundred globally. Repair capacity is commercially contracted and geographically limited. While bodies such as the International Cable Protection Committee that include private and public actors, coordinate cable protection and facilitate repair operations, this capacity operates without a strategic reserve requirement or any public international governance framework adequate to a major multi-cable event. In this scenario, every relevant institution, national governments, international organisations, cable operators, satellite providers, and financial regulators have a partial role. However, no actor has the authority required to match its responsibility. The crisis is not only caused by an eruption; it is mainly caused by an architecture in which no single actor holds both the authority and the operational capacity required to match the scale of its responsibilities.

Shared patterns of systemic digital risks

Despite their different triggers, critical digital risk scenarios tend to follow a common set of structural patterns. Notably, different critical digital risk scenarios are equally possible. A prolonged drought could affect the river systems used for data centre cooling. A major volcanic eruption along a submarine cable corridor could replicate and amplify the governance vacuum the undersea cable scenario exposes, while adding atmospheric disruption that degrades satellite backup simultaneously. A major hurricane could level the mobile towers and poles carrying communications fibre of island nations. A progressive collapse of collisions in low Earth orbit makes large numbers of communications satellites inoperable and generates debris fields dense enough to render key orbital shells unusable for decades. Unlike the other scenarios in this report, the scenario, known as the Kessler effect, would leave no immediate recovery path. Read each scenario should therefore be read as a question: not 'could this happen?' but 'what would we do if it did?'

What do those three scenarios share?

These disruptions are preceded by warnings. In each case, the information required to anticipate the disruption existed. The probability of a major solar event was published. The heatwave was forecast. The cable corridor's vulnerability was mapped. What was absent in each case was not knowledge but the architecture to translate knowledge into coordinated action across the organizations, jurisdictions, and sectors that a disruption would cross. Yet this architecture must also extend to risks that have not yet been named: building the capacity to surface unknown unknowns as the vulnerabilities that exist before they appear in any forecast or risk register remains an equally pressing challenge.

They are invisible until they are not. None of these crises announces itself with a single dramatic event. Instead, they accumulate through thresholds that no individual organization is positioned to see in aggregate. By the time the crisis is legible as a crisis, the window for the most effective interventions has already closed.

They expose a specific kind of dependency: the hidden kind. Financial transactions depend on satellite timing. Transport systems depend on real-time data, GNSS navigation, and digital traffic management. Health systems rely on cloud platforms. Emergency alerts depend on the same data centres as everyday services. These dependencies were created through individually rational decisions, by people who were not asked, and had no mechanism to assess what those choices meant for the system as a whole.

Finally, digital risks do not depend simply on how digitalised a country is. The global digital divide, leaving about one quarter of the world offline, creates distinct vulnerabilities: in some Small Island Developing States, connectivity might depend on a single submarine cable, with critical data infrastructure often lying beyond national jurisdiction [7]. The second part of this report examines the analytical foundations that explain why these patterns recur, and what a management response adequate to their scale would require.

Understanding critical digital risks

The scenarios described in the first part of this report are not hypothetical curiosities. They are plausible projections of a risk landscape that has been systematically documented across technical literature, empirical studies of recent infrastructure failures, and the expert co-creation processes on which this report is based. This second part steps back from the narrative level to examine what we actually know about critical digital risks: how they are conceptualized, what structural conditions produce them, where our frameworks remain inadequate, and what forms of management could begin to match the scale of the challenge. Contemporary digital infrastructure is simultaneously more robust and more fragile than ever before. This is not a contradiction but a structural feature of how large-scale networked systems evolve. Decades of investment in redundancy, load balancing, and distributed architecture have made digital systems increasingly resilient to routine and localized failures. A single server outage, a cut fibre link, a software bug: these events can be absorbed by systems designed to handle such failures. Yet this same architecture, tightly coupled, deeply interdependent, optimized for efficiency over slack, creates conditions in which a sufficiently large initial shock can propagate across systems with a speed and scope that no single operator controls or even anticipates.

The literature describes this as the transition from additive to exponential failure dynamics. In traditional risk models, two concurrent hazards produce roughly the sum of their individual impacts. In a tightly coupled digital infrastructure, concurrent stresses interact nonlinearly: the failure of one system removes a redundancy that another depends upon,

which in turn overloads a third, triggering cascading collapse across sectors that were never explicitly connected in any operator's risk register. Empirical evidence confirms that this is not just a theoretical concern. Studies of observed outages show that up to 89 per cent of digital service disruptions caused by natural hazards result not from direct physical damage but from these secondary ripple effects. The number of people ultimately affected is estimated to be up to ten times higher than those exposed to the initial event [8].

This paradox has a second dimension that expert discussions have brought into sharp relief: digital risks are invisible. Unlike floods, earthquakes, or industrial accidents, digital infrastructure failures frequently produce no visible physical signal. Populations and organizations may wake to find nothing altered in their surroundings, yet critical systems have ceased to function. This invisibility delays recognition of severity and postpones activation of response mechanisms precisely when timely action proves most consequential. The 2011 Fukushima nuclear accident illustrates the principle: the multi-sector breakdown from earthquake to tsunami to nuclear crisis created critical information gaps that were themselves a secondary disaster. When the information infrastructure fails, the capacity to assess damage, coordinate response, and communicate guidance is destroyed simultaneously with, or even before, the physical systems it depends on.

Four infrastructure domains and their interdependencies

The core expert group on critical digital risks identified four critical infrastructure domains whose interdependencies constitute the material architecture of digital risks. These are not independent categories but layers of a single ecosystem, each depending on the others in ways that are only partially mapped.

1. Power grids as e foundational layer

Power grids serve as the foundational layer of digital infrastructure. Every other digital system, telecommunications networks, data centres, payment systems, navigation services, and mobile infrastructure, as well as satellite earth stations, depend on a reliable electricity supply. Power grid failures, therefore, ripple immediately across the entire digital ecosystem. The critical implication is that power infrastructure must be assessed in three phases: preventing failure, maintaining degraded operations during disruption, and restoring service within timeframes that prevent dependent.

Historical analysis shows that restoration delays produce sequential failures:

- The 2003 E ropean heatwave triggered power grid stress, which contributed to cascading failures across interdependent systems.
- The 2021 OVHcloud fire in Strasbourg was responsible for the disruption of ~3.6 million websites from a single physical facility failure.
- The Oregon eatwave in 2021 caused data centre outages at multiple cloud providers.
- In 2022, the Oracle and Google Cloud failures in London were linked to cooling capacity during a heat event.
- The 2025 blackout in Spain involved the sudden loss of 15 gigawatts of power, triggering cross-sector failures and knocking out telecommunications across Spain and Portugal. Internet, mobile, and messaging services were widely disrupted, with knock-on effects reaching Morocco and remote villages in Greenland.

2. Submar e cables as the connectivity backbone

Submarine communication cables transmit over 99 per cent of international internet traffic, yet their critical role remains poorly understood in public discourse and risk governance frameworks. Submarine cables are fragile and easily severed by natural hazards or

commercial fishing activities. What makes these events particularly severe is the repair timescale: specialized cable repair vessels exist in limited numbers globally, and restoration can require several months, during which traffic is rerouted through alternative paths, degrading service across the wider network.

The vulnerability of undersea cables to natural hazards is well documented:

- The 2006 Hengchun underwater earthquake severed eight cables simultaneously, degrading connectivity across several Asian countries for weeks.
- The 2022 unga Tonga volcanic eruption isolated an entire island nation from global communications.
- In 2022, a single cable failur on the Shetland Islands isolated communities for several days.
- The 2024 ed Sea cables disruption consisted of multiple cables cut within weeks, with 25% of traffic between Asia and Europe disrupted.
- Multiple precedents of repair ti elines of 3-6 weeks in international waters.

3. Satellite systems an space weather impact

Scientific literature on space weather has extensively documented the power grid vulnerability. Geomagnetically induced currents produced by major solar events can cause half-cycle saturation in high-voltage transformers, leading to permanent damage with replacement timescales measured in months. As the scenario of a Carrington-class event shows, a triggered network-wide effect would potentially destroy transformer infrastructure faster than global manufacturing capacity could replace it. This is not a marginal scenario; it is a credible planning horizon for which current preparedness frameworks are structurally inadequate.

Satellite systems face complementary vulnerabilities from space weather events, with implications for GNSS navigation, financial transactions, transport, and communications. The Kessler syndrome is a chain reaction of space debris collisions that can sustain itself. It is a longer-horizon risk, with some orbits already becoming dangerously crowded. It would unfold across years, creating a sense that it can be managed, while quietly moving past the point of no return.

Despite the singularity of the Carrington event, there are precedents of space weather disruption:

- In 1989, a ge magnetic storm, known as the Quebec blackout, caused a nine-hour total blackout affecting six million people.
- The 2003 alloween storms led to satellite failures, aviation disruption, power grid stress across Northern Europe.

Despite the singularity of the Carrington event, there are precedents of space weather disruption:

- In 1989, a ge magnetic storm, known as the Quebec blackout, caused a nine-hour total blackout affecting six million people.
- The 2003 alloween storms led to satellite failures, aviation disruption, power grid stress across Northern Europe.

4. Data entres as the hidden concentration risk

Despite their centrality to financial services, healthcare, supply chains, and public administration, data centres constitute what the literature identifies as a significant blind spot in critical digital risk scholarship. As of early 2024, the total number of data centre facilities globally, including hyperscale, colocation, and enterprise sites, exceeded 11,800, with the United States alone accounting for around 40% of that total. Growth is accelerating sharply: the sector added 137 new hyperscale facilities in 2024 alone, and AI and cloud computing are projected to drive a 14% compound annual growth rate through 2030 [9]. By 2030, global data centre electricity demand is expected to more than double, from 415 terawatt-hour in 2024 to approximately 945 terawatt-hour, approaching 3% of total global electricity consumption [10].

Geographic concentration amplifies vulnerability. Industry-led standards address some of these risks at the facility level, though they do not cover cross-facility cascade dynamics. Clusters mean that a single extreme weather event affecting a regional hub can simultaneously disrupt cloud computing platforms, content delivery networks, enterprise

systems, and telecommunications infrastructure. The 2021 European floods and multiple hurricane events in the United States of America provide recent empirical examples. Flooding causes immediate and irreversible damage to electrical and cooling systems, while extreme heat events can trigger emergency shutdowns that escalate through interconnected data centre networks as workload redistribution overloads remaining facilities.

Data centre failures, each with the risk of knock-on effects, are not uncommon:

• In 2009, a heavy rainstorm flooded the Vodafone data centre in Istanbul in just eight minutes, destroying equipment and causing a major customer outage.

• The 2012 Hurricane Sandy in New York led to several data centres in lower Manhattan going offline. Operators had to pump out flooded basements and generator rooms and replace damaged switchgear before restoring service.

• The 2015-2016 flooding of the Vodafone facility in Leeds, due to River Aire bursting its banks, caused an outage lasting several days and disrupting mobile services across the region.

• Multiple US hu ricane seasons (notably 2017) during the costliest hurricane season on record led to widespread generator failures, power outages, and data centre shutdowns across the Gulf Coast and East Coast.

Compound risks and the limits of current frameworks

Most risk planning today assumes that one problem happens at a time, lasts for a short period, and can be fixed using well-rehearsed procedures. This is how most emergency plans, risk registers, and business continuity strategies are designed.

But critical digital disruptions rarely work like that.

In reality, several pressures often hit at the same time, interact with each other, and last longer than backup systems were designed to handle. A heatwave may coincide with high electricity demand. A cable cut may occur while networks are already under strain. In such situations, failures do not stay confined to one system or sector. They spread.

Two common patterns explain why impacts quickly become much larger than expected.

• In some cases, one single event affects many systems at once. For example, a major solar storm, an extreme weather event, or damage to a key submarine cable can simultaneously disrupt electricity, communications, data centres, and financial services, even though these systems are often treated as separate.

• In other cases, the timing of events is the problem. One incident stretches backup systems and redundancies; a second, otherwise manageable event, then pushes the system beyond its limits. What would have been recoverable on its own becomes a serious disruption because the safety margin is already gone.

In both situations, systems that usually work reliably become fragile because they rely on each other in ways that are not always visible or fully understood.

These failures are hard to manage not only because they spread, but because they often begin out of sight. This becomes clear when contrasted with cyber threats, where the problem is usually visible, even if its consequences are not.

Cyber incidents usually announce themselves. When systems are hacked or hit by ransomware, it is clear that an attack has taken place, even if the details are not yet known. Non-intentional digital infrastructure failures are different. When they occur, the cause is often invisible to the people experiencing the disruption. Systems simply stop working. Payments fail. Data is unavailable. Alerts do not arrive without any obvious explanation.

For physical digital risks, the problem may lie far away: an overheated data centre, a damaged submarine cable, a power disturbance, or a satellite disruption. But from the user's perspective, there is no clear starting point. The failure looks local, temporary, or technical, even though it is part of a much larger system breakdown. This invisibility is what makes these risks so dangerous. Time is lost searching for the wrong causes, while failures quietly spread across sectors and borders. By the time the real source becomes clear, if it ever does, the disruption has already escalated.

This distinction is analytical, not hierarchical. Cyber and non-intentional risks are increasingly interconnected: a physical disruption can create vulnerabilities that malicious actors exploit, while a cyberattack can trigger cascading physical failures. Both dimensions warrant attention, and their interaction constitutes an additional layer of systemic risk.

Finally, the economic impacts of large digital disruptions are still poorly understood. While available estimates suggest that even a single day of mobile network failure can cause very large economic losses in highly digitalized economies, most analyses focus only on direct effects, such as missed transactions or service outages.

They rarely capture the wider knock-on effects: supply chains that stall, businesses that cannot operate, public services that fail to coordinate, or the longer-term damage to investor confidence and public trust. We still lack economic models that reflect how deeply modern societies depend on digital infrastructure and that could be reliably used for planning at the organisational, national, or international level.

Conclusion and recommendations

Critical digital risks are real, documented, systemic, and largely underestimated. They do not unfold as isolated incidents, but as disruptions across sectors and borders. While many of the risks are already understood in expert communities, they remain insufficiently recognized and acted upon.

Drawing on a co-creation process with senior expert practitioners spanning international organizations, national authorities, academic institutions, and the private sector, this report highlights six priorities for action:

1. Build k wledge:

– Identify critical digital r sks

– Cross-sector dependency mapping adapted to different national contexts, including low- and middle- income countries where infrastructure data availability is more limited and digital integration follows distinct patterns

– Model robabilistic chain reactions

2. Update nagement:

– R cognize non-intentional digital disruptions as a core risk

– Clari y legal definitions

– Re ise disaster risk frameworks

– Establish i centives for preparedness

3. C sider strengthening international standards:

– Ens re analogue fallback capacity

– Conduct joint scenario planning for energy, finance, telecommunications, and emergency management domestically (local + national), regionally and even globally

4. Ramp up proactive coordination on critical risks, especially:

– Space weather

– Submarine cables

– Satellites

– Data centres

5. Strengthen societal resilience:

– Upkeep of analogue skills across professional and public contexts

– Build societal capacity to absorb and recover from digital disruptions

6. Build trust:

– Build capacity for national authorities, local governments, and vulnerable communities

– Convene communities and stakeholders, including private operators across sectors and borders

– Foster shared situational awareness and mutual accountability

Whether these risks remain manageable or escalate into systemic crises will also depend on how these priorities are translated into action.

REFERENCES

[1] E. Koks, et al., “Infrastructure failure cascades quintuple risk of storm and flood-induced service disruptions across the globe,” *One Earth*, 2024, 7(4). https://doi.org/10.1016/j.oneear.2024.XX (available via ScienceDirect).

[2] E. Mühlhofer, D.N. Bresch, E.E. Koks, “Infrastructure failure cascades quintuple risk of storm and flood-induced service disruptions across the globe,” *One Earth*, 2024, 7(4), pp. 714-729. https://doi.org/10.1016/j.oneear.2024.03.010 (available via ScienceDirect).

[3] E.J. Oughton, M. Hapgood, G.S. Richardson, C.D. Beggan, A.W.P. Thomson, M. Gibbs, D. Burnett, C.T. Gaunt, M. Trichas, R., Dada, R.B. Horne, “A risk assessment framework for the socioeconomic impacts of electricity transmission infrastructure failure due to space weather: an application to the United Kingdom,” *Risk Analysis*, 2019, 39(5), pp. 1022-1043. doi:10.1111/risa.13229.

[4] Lloyd's of London and Atmospheric and Environmental Research (2013) Solar storm risk to the North American electric grid. London: Lloyd's of London.

[5] A. De Bono, G. Giuliani, S. Kluser, P. Peduzzi, “Impacts of Summer 2003 Heat Wave in Europe,” *Environment Alert Bulletin* No. 2. 2004, Nairobi: UNEP/GRID-Europe. Available at: https://www.unisdr.org/files/1145_ewheatwave.en.pdf (Accessed: 20 April 2026).

[6] M.A. Clare, et al. “Fast and destructive density currents created by ocean-entering volcanic eruptions,” *Science*, 2023, 381(6662). Available at: https://www.science.org/doi/10.1126/science.adi3038 (Accessed: 20 April 2026).

[7] ITU (International Telecommunication Union). 2025. Facts and Figures 2025: Internet Use. Geneva: ITU. https://www.itu.int/itu-d/reports/statistics/2025/10/15/ff25-internet-use/

[8] E. Mühlhofer, E. E. Koks, C. M. Kropf, G. Sansavini, D. N. Bresch, “A generalized natural hazard risk modelling framework for infrastructure failure cascades,” *Reliability Engineering and System Safety*, 2023, 234, p. 109194. doi:10.1016/j.ress.2023.109194.2024.

[9] International Energy Agency. Electricity 2024: analysis and forecast to 2026. Paris: IEA. Available at: https://www.iea.org/reports/electricity-2024 (Accessed: 14 April 2026).

[10] Synergy Research Group. Hyperscale data center count hits 1,136; average size increases; US accounts for 54% of total capacity [Press release]. 19 March. 2025. Available at: https://www.srgresearch.com/articles/hyperscale-data-center-ount-hits-1136-average-size-increases-us-accounts-for-54-of-total-capacity (Accessed: 14 April 2026).

[11] International Telecommunication Union, United Nations Office for Disaster Risk Reduction, Sciences Po et al. When Digital Systems Fail – An Expert Report on the Hidden Risks of Our Digital World, Paris: Sciences Po. 2026.