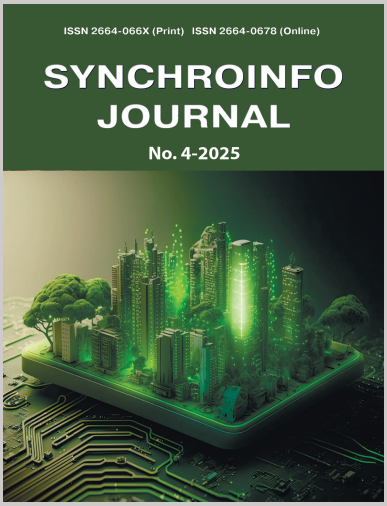
CONTENT
Vol. 11. No. 4-2025



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

SPEECH SIGNAL PROCESSING METHODS IMPLEMENTATION IN WEB APPLICATION DEVELOPMENT

M. V. Galickiy [1]

[1] Network Information Technologies and Services, MTUCI, Moscow, Russia

m.v.galickiy@mtuci.ru

ABSTRACT

Information systems are becoming more complex due to the integration of artificial intelligence and machine learning. The introduction of additional data entry methods has the potential to increase user productivity. To improve the accuracy and efficiency of speech-to-text conversion, it is essential to consider technologies such as voice activity detection and automatic speech recognition. They provide advanced mechanisms for user-system interaction through natural user interfaces, in particular, voice. The article will also discuss some ASR platforms with different levels of adaptation to linguistic and acoustic environments. The subject of research in this article is the methods of voice activity detection (VAD) and automatic speech recognition (ASR). The purpose of the study is to analyze the VAD and ASR modules and test them to make recommendations on their use. The results of the study will be useful for web application developers who are thinking about implementing this modules in their projects.

KEYWORDS: *voice recognition; algorithms; web application; speech synthesis; ASR; VAD; artificial intelligence*

DOI: 10.36724/2664-066X-2025-11-4-2-8

Received: 20.06.2025
Accepted: 23.08.2025

Citation: M. V. Galickiy, "Speech signal processing methods implementation in web application development", *Synchroinfo Journal* **2025**, vol. 11, no. 4, pp. 2-8.

Introduction

Currently, many organizations operate in a rapidly changing environment, where information systems (IS) are becoming more complex due to the integration of artificial intelligence and machine learning. In most computer workstations, manual input remains the main method for entering information. However, the introduction of additional data entry methods has the potential to increase user productivity.

To improve the accuracy and efficiency of speech-to-text conversion, it is essential to consider technologies such as voice activity detection (VAD) and automatic speech recognition (ASR). They provide advanced mechanisms for user-system interaction through natural user interfaces (NUI), in particular, voice. The article will also discuss some ASR platforms with different levels of adaptation to linguistic and acoustic environments.

Overview of ASR platforms and their capabilities

Mozilla DeepSpeech [1], CMU Sphinx [2], Vosk [3] and the Google Speech API are all interfaces that support speech recognition and synthesis for web applications. They allow you to create programs that can listen to the user and respond to them with a voice. These interfaces differ in their architecture, principles of operation, and scope of application. However, they share two key features:

1. A component that enables user speech recognition. This component enables listening to audio data from a microphone, converting it into text information, and creating convenient and intuitive user interfaces based on voice commands.
2. The component that enables the synthesis of speech and conversion of text information into audio data, thus allowing the program to produce a voice response.

By using these ASR platforms, developers have a wide range of options for working with voice technologies on the web platform. For example, you can create web applications that use built-in tools to recognize user speech. This feature is useful for creating voice-based searches, voice-controlled interfaces, and other applications where it is more convenient to interact with speech rather than text [4].

In addition, they are an excellent tool for creating voice assistants. With the help of this technology, applications can access a device's microphone, listen to audio, and transmit it for processing. They can then respond to the user's voice commands.

As for speech synthesis, the second feature allows you to convert text information into spoken words, making interfaces more accessible to users with hearing impairments.

However, it is important to note that these platforms do have some limitations. For instance, the Google Speech API cannot be used offline and requires a continuous Internet connection. Mozilla DeepSpeech needs a significant amount of resources for training, while Vosk consumes a significant amount of RAM. These factors should be taken into consideration when testing and using these tools.

Voice activity detection and automatic speech recognition

Automatic speech recognition (ASR) technologies have now reached a level of sophistication that they can be reliably used to improve web user interfaces. Some of the most important user operations include:

1. website navigation, including clicking on links that are not provided on the current page;
2. filling out input form (e.g., text fields, number fields, drop-down lists);
3. performi actions (for example, submitting or canceling completed forms).

Automatic speech recognition (ASR) and analysis of the algorithms used

Automatic speech recognition (ASR) technology allows electronic devices to recognize spoken words and has been the subject of research since the 1950s [5]. ASR can be seen as a mathematical model that transforms speech audio signals into text. It's important to differentiate ASR from voice biometrics, which is focused on identifying the speaker rather than the speech content [6].

Automatic speech recognition (ASR), now implemented in voice assistants, is an additional input method for devices such as mobile phones, tablets, and virtual assistants. Taking advantage of the widespread demand, ASR technologies have reached a level of maturity that justifies their use in web systems as an additional method of information input.

Among the approaches to automatic speech recognition (ASR), hidden Markov models (HMM) and deep neural networks (DNN) have been widely studied [7].

HMM is a statistical model developed in the 1960s that describes sequences of events and the probabilities of transitions between them. This algorithm has found wide application in speech recognition, as it allows modeling various phonetic units and predicting the most probable word order [8].

The HMM is a relatively simple and effective algorithm that can be used to recognize various types of sounds, including speech. It is based on the assumption that each observed position is the result of the previous position, with a certain transition probability. A device using this algorithm analyzes the data heard and predicts what word or sound will come next.

In order for the device to function with HMM, a set of training data is required. This includes sequences of observed symbols and corresponding sequences of hidden states. These parameters, such as the probability of transitions between states and the probability of observed symbols for each state, are used to train the HMM using mathematical techniques, such as the maximum likelihood method or the Baum-Welsh algorithm [9].

Once trained, the HMM can be used for speech recognition. This requires obtaining a sequence of observed symbols corresponding to the audio signal and using the model to determine the most probable sequence of hidden states corresponding to this data.

The advantages of this algorithm include its high speed of sound and speech recognition, even in noisy or distorted environments. Additionally, it has the benefit of having access to training data, allowing you to tailor the model to specific tasks. However, this data needs to be presented in large quantities in order to ensure high accuracy in recognition. The disadvantages also include the need for manual adjustment of model parameters and the potential for inaccurate results when detecting complex sounds.

Another algorithm is Deep Neural Networks (DNN). DNN is one of the most popular methods in the field of speech recognition. It consists of multi-layered networks of artificial neurons that are trained on a large amount of labeled data in order to achieve high accuracy in recognition [10].

Each layer of DNN neurons performs a specific function. The first layer of the neural network accepts audio data as input. This data is then processed by subsequent layers, which produce the final output. The number of layers and neurons in each layer is determined by the network's architecture and the specific tasks it is designed to solve.

DNN training involves adjusting the weights and biases of each neuron in the network to allow it to correctly process audio data. This is done using the backpropagation method, which allows the importance of different parts of the data to be adjusted based on the difference between actual and expected results.

DNN, like HMM, can achieve high speech recognition accuracy if high-quality training data is available in large quantities. But unlike HMM, DNN is self-learning, which allows it to be used to solve problems without explicit class labels. The disadvantage of this algorithm is the requirement for large computing resources and the choice of network architecture, which makes it difficult to use on mobile devices and other limited systems [11].

In most modern ASR systems, the audio signal is converted into a set of vector features, which are then used in subsequent processing stages. This process is sensitive to noise, accent, age, and gender of the speaker. In addition, context-independent and language models are used. The former is trained to recognize phonemes from a feature vector, which is used to construct words. The language model is responsible for grammatical rules and determines the most likely word order in a sentence. It is usually represented by n-gram models containing statistical data on word sequences.

Currently, many speech recognition systems are used as virtual assistants on mobile devices. For example, the most popular voice assistants based on this system are Alice from Yandex, Marusya from VK and Salute from Sber.

There are many commercial ASR platforms offering ready-made integration solutions, including the Microsoft Bing Speech API, Google Speech API, and IBM Watson Speech-to-Text.These platforms are available under a license. However, there are open source toolkits that allow developers to create their own speech-to-text conversion systems for various programming languages and platforms, such as Mozilla DeepSpeech, CMU Sphinx, and Vosk, already mentioned above. Google Speech API is also used for comparative analysis, as it has a high accuracy in speech recognition.

Mozilla DeepSpeech uses a recurrent neural network (RNN) architecture, which is implemented using the TensorFlow framework.

CMU Sphinx is a popular platform among the scientific community, offering a wide range of tools and a flexible design. This allows for the quick and easy development of speech recognition (ASR) applications.

Vosk API is a speech recognition tool that integrates offline models for 17 languages.

Voice activity detection (VAD)

Voice Activity Detection (VAD) refers to signal processing techniques used to detect speech in an audio signal. In speech processing systems, the problem of distinguishing between speech and non-speech signals remains relevant, especially for web applications operating in real time. Speech processing algorithms often place high demands on computational resources. However, speech is inherently intermittent, and incorporating VAD into these algorithms is an optimization strategy to reduce unnecessary computation [12].

VAD methods differ in their processing principles, but their main goal is to extract speech data from a given audio signal and separate it from non-speech fragments. In most cases, speech fragments are grouped for further processing, which allows noise to be removed from the input data.

In general, VAD methods can be classified into two categories:

1. Energy threshold-based methods. These methods rely on the fact that speech adds energy to the signal. This method allows one to distinguish between high- and low-energy regions, i.e., regions without speech. This approach is simple to implement and is widely used in systems with limited computing resources.

2. Machine learning-based methods. These methods involve selecting one or more speech characteristics, using learning algorithms, and training on large amounts of data suitable for the intended use cases. Despite their high accuracy, such methods require significant computational resources, and their implementation remains complex and requires further improvement [13].

Module results VAD

Any technology must meet several requirements in order to have the desired impact on users. In this case, the processing time from the moment the audio signal is captured to the execution of the associated operation is a critical factor in ensuring a smooth workflow. Excessive processing time may negatively impact system acceptance and implementation.

In addition, there are two major issues that may be of concern to both end users and company management: data privacy and information security [14-18]. However, these issues are beyond the scope of this study.

For voice-related applications, it is important to save bandwidth by disabling streaming when no voice content is detected. In speech recognition tasks, the processor load can be reduced by avoiding processing unnecessary fragments without speech content. On the other hand, if the speech signal is incorrectly classified as noise, the module will not be able to transmit all the necessary information for further recognition [19].

For testing, a VAD module was used, implemented based on the energy threshold level, having a binary output, where audio signals are classified as speech or non-speech.

To evaluate the performance of the VAD module, a criterion related to the correct segmentation of speech content was adopted. First of all, no important speech content that needs to be processed should be blocked. The Speech Hit Rate (SHR) [20], which reflects the percentage of correct speech detection, was used as an objective evaluation parameter. Additionally, the Noise Suppression Ratio (NSR) was used, which measures the amount of noise that was blocked relative to its total volume in the sound segment.

Five SNR (signal-to-noise ratio) levels were used in the testing:

• cl an sound,

• SNR = 0, 5, 10, and 15.

Three audio files with speech superimposed on background crowd noise (Sp01, Sp02, and Sp03) were tested. Each test audio segment at a given SNR level included three speech samples separated by noise fragments.

Figure 1 demonstrates the results of the VAD module for SNR = 10 (the dashed blue vertical lines indicate spch ON and the red ones indicate spch OFF, the real parts of the speech data are marked manually with a green background), and Table 1 shows the summary test results for each SNR level (the results of the speech hit rate (SHR) and noise reduction ratio (NSR) assessment).

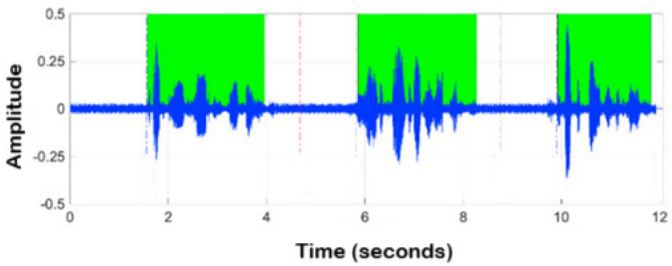


Figure 1. Results of the VAD module

Table 1

Summary test results

SNR	SNR sp01	SNR sp02	SNR sp03	NSR
clean	0.98	0.98	0.98	0.81
15	0.98	0.98	0.98	0.70
10	0.98	0.98	0.98	0.71
5	0.97	0.99	0.99	0.80
0	1.0	1.0	1.0	0.09

Module results ASR

Mozilla DeepSpeech, CMU Sphinx, Vosk and Google Speech API were used for testing.

DeepSpeech training involved data augmentation applied to 15% of the original dataset. The main hyperparameters used during training included:

• dr p_source_layers = 5 (to adjust all model weights),

• batch s ze = 16 (to account for hardware capabilities),

• num er of epochs = 200,

• n_h dden = 2048 (as recommended for DeepSpeech),

• learning_rate = 0.0001, and dropout_rate = 0.05, which yielded acceptable results after trial and error.

CMU Sphinx training was performed using sphinxtrain4 compiled for Linux. The training steps included:

1. creat g a dictionary with the required vocabulary,
2. setting u a phoneme file,
3. creat g a language model using the CMU Sphinx online tool.

In addition, a five-fold cross-validation process was conducted, where 80% of the data was used for training and 20% for validation.

To compare Vosk, DeepSpeech, CMU Sphinx, and the Google Speech API, we used a test dataset belonging to the best model obtained during cross-validation for CMU Sphinx.

For each audio file, the following were calculated:

• LD (Levenshtein Distance) – a measure of recognition errors;

• processing time (inference time).

The results are presented as histograms for English and Russian languages (Fig. 2 and Fig. 3).

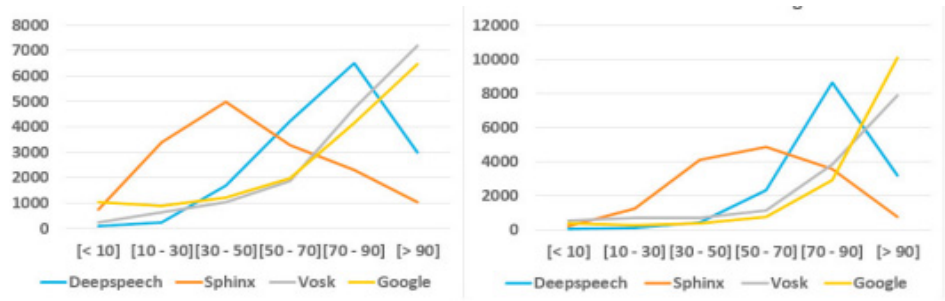


Figure 2. Results (Levenshtein Histogram)

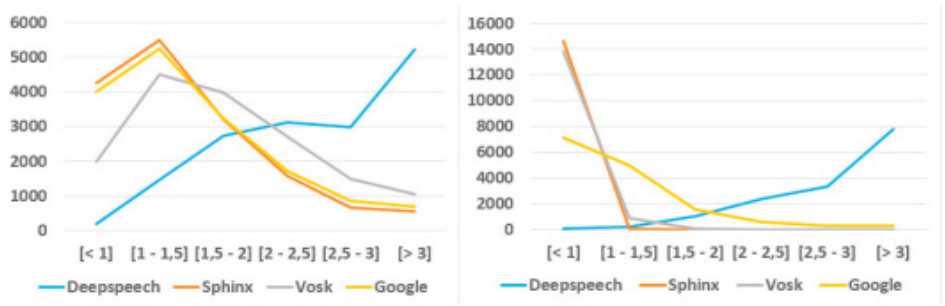


Figure 3. Results (Time Histogram)

Conclusion

In this article, the methods of voice activity detection (VAD) and automatic speech recognition (ASR) were reviewed and tested, and their effectiveness and accuracy were evaluated. The following results were obtained in the course of the study:

The VAD algorithm, implemented based on an energy threshold, does not guarantee effective speech-noise discrimination under conditions where the SNR is below 5.

At SNR = 0, an extreme case occurs: the algorithm is unable to separate speech from noise and classifies the entire signal as speech data.

For ASR:

• Vosk shows similar results t the commercial Google Speech API;

• Vosk outperforms other systems in recognition accuracy for two languages, achieving an accuracy of over 85%;

• D epSpeech ranked second in accuracy (according to the LD metric);

• C U Sphinx was the fastest in processing time (less than 1 second);

• Vosk showed a processing time of 1.0–1.5 seconds, similar to the Google Speech API;

• DeepSpeech was the slowest, with an average processing time of over 2.5 seconds for English and over 3 seconds for Russian.

REFERENCES

[1] DeepSpeech's documentation [Electronic resource]. Mode of access: https://deepspeech.readthedocs.io/en/latest/ (Date of access: 07.07.2025)

[2] Cmusphinx [Electronic resource]. Mode of access: https://cmusphinx.github.io/wiki/about/ (Date of access: 07.11.2025)

[3] Vosk Offline speech recognition API [Electronic resource]. Mode of access: https://alphacephei.com/vosk/ (Date of access: 07.07.2025)

[4] ASR [Electronic resource]. Mode of access: https://sonix.ai/resources/what-asr/ (Date of access: 07.07.2025)

[5] S. Furui, "Speech Recognition – Past, Present, and Future," *NTT review*, vol. 7, no. 2, 1995, pp. 13-18.

[6] R.S. Rocha, P. Ferreira, I. Dutra, R. Correia, R. Salvini, E. Burnside, "A Speech-to-Text Interface for MammoClass," *2016 IEEE 29th International Symposium on Computer-Based Medical Systems (CBMS)*, 2016, pp. 1-6.

[7] M. Bohac, M. Kucharova, Z. Callejas, J. Nouza, P. Červa, "A cross-lingual adaptation approach for rapid development of speech recognizers for learning disabled users," *EURASIP Journal on Audio, Speech, and Music Processing*, 2014.

[8] P. Barry, P. Crowley, "Modern Embedded Computing: Designing Connected, Pervasive, Media-Rich Systems," 2012, pp. 16-19.

[9] Hidden Markov chains [Electronic resource]. Mode of access: https://habr.com/ru/articles/188244/ (Date of access: 07.07.2025).

[10] DNN Neural Network [Electronic resource]. Mode of access: https://www.educba.com/dnn-neural-network/ (Date of access: 07.07.2025).

[11] B. Lindberg, "Low-Complexity Variable Frame Rate Analysis for Speech Recognition and Voice Activity Detection," *IEEE Journal of Selected Topics in Signal Processing*, 2010, pp. 798-807.

[12] A Real-Time Voice Activity Detection Algorithm [Electronic resource]. Mode of access: https://www.pvsm.ru/programmirovanie/42828 (Date of access: 07.07.2025).

[13] Skillbox media [Electronic resource]. Mode of access: https://skillbox.ru/media/code/kak-ustroeno-mashinnoe-obuchenie-zadachi-algoritmy-i-vidy-machine-learning/ (Date of access: 07.07.2025).

[14] V. A. Dokuchaev, "The impact of new information and communication technologies on the privacy of personal data," *Current problems and prospects of economic development: XXIII International Scientific and Practical Conference*, 2024, pp. 12-15.

[15] V. A. Dokuchaev, V.V. Maklachkova, A. A. Boiko, "The problem of data updating in CRM systems," *Economics and quality of communication systems*, 2025, no. 1(35), pp. 45-57.

[16] V.Y. Statev, V. A. Dokuchaev, V.V. Maklachkova, "Information security in the big data space," *T-Comm*. 2022. Vol. 16, no. 4, pp. 21-28. DOI 10.36724/2072-8735-2022-16-4-21-28.

[17] V. A. Dokuchaev, V. V. Maklachkova, V. Yu. Statev, "Classification of personal data security threats in information systems," *T-Comm*. 2020. Vol. 14, no. 1, pp. 56-60. DOI 10.36724/2072-8735-2020-14-1-56-60.

[18] V. A. Dokuchaev, "Digital transformation: New drivers and new risks," *2020 International Conference on Engineering Management of Communication and Technology, EMCTECH 2020* : Proceedings, Vienna, 2020. New York: Institute of Electrical and Electronics Engineers Inc., 2020. P. 9261544. DOI 10.1109/EMCTECH49634.2020.9261544.

[19] How ASR works [Electronic resource]. Mode of access: https://cloud.vk.com/blog/slushaet-i-ponimaet-kak-rabotaet-tehnologija-avtomaticheskogo-raspoznavanija-rechi/ (Date of access: 07.07.2025) (in Russian).

[20] Efficient voice activity detection algorithm [Electronic resource]. Mode of access: https://asmp-eurasipjournals.springeropen.com/articles/10.1186/1687-4722-2013-21 (Date of access: 07.07.2025).

SYNCHROINFO JOURNAL

www.media-publisher.eu/synchroinfo-journal

A STUDY OF SGD AND ADAM APPROACHES TO TRAINING AN LSTM ARTIFICIAL NEURAL NETWORK FOR MALICIOUS TRAFFIC RECOGNITION

Alexandr I. Timoshenkov [1], **Anastasia Y. Kudryashova** [2]

[1] Moscow Aviation Institute, Moscow, Russia

tim2_02@mail.ru

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

a.i.kudriashova@mtuci.ru

ABSTRACT

This paper examines the problem of binary classification of network traffic using an artificial neural network (ANN) based on the LSTM (Long Short-Term Memory) architecture. A comparative study of the effectiveness of two popular optimizers – stochastic gradient de-scent (SGD) and adaptive moment estimation (Adam) – Is conducted on various network attack scenarios from the CICIDS-2017 dataset. The focus is on classification quality metrics: accuracy, recall, prediction accuracy, and F1-score. Experiments demonstrate that the Adam optimizer demonstrates higher and more stable performance, especially under conditions of significant class imbalance characteristic of real-world network traffic. A detailed theoretical justification for the advantages and disadvantages of each optimizer is provided, and the causes of the observed experimental phenomena are analyzed in detail.

KEYWORDS: *intrusion detection; anomaly detection; neural network; LSTM; SGD; Adam; binary classification; malicious traffic; CICIDS-2017*

DOI: 10.36724/2664-066X-2025-11-4-9-14

Received: 20.06.2025
Accepted: 23.08.2025

Citation: Alexandr I. Timoshenkov, Anastasia Y. Kudryashova, "A study of SGD and ADAM approaches to training an LSTM artificial neural network for malicious traffic recognition", *Synchroinfo Journal* **2025**, vol. 11, no. 4, pp. 9-14.

Licensee IRIS, Vienna, Austria.

Introduction

With the rapid growth of digitalization and the spread of information technology, the issue of network security is becoming increasingly pressing. Modern computer networks are becoming increasingly vulnerable to various types of cyberattacks, including port scanning, intrusions, denial-of-service (DoS/DDoS) attacks, and malware. Traditional security methods based on signature analysis are often ineffective against new and modified types of threats, requiring more intelligent and adaptive solutions.

In recent years, network traffic has steadily increased, accompanied by an increase in the number and diversity of cyberattacks. This necessitates the development of effective systems for detecting anomalies and malicious behavior in computer networks. One promising area in this field is the use of machine learning methods, particularly recurrent neural networks (RNNs), including the Long Short-Term Memory (LSTM) variant.

The LSTM model is a type of recurrent neural network developed to solve the vanishing gradient problem characteristic of classical RNNs. The key feature of LSTMs is the presence of internal memory cells and control gates (input, output, and forget gates), which enable efficient processing of dependencies over long time intervals. This makes LSTMs particularly suitable for analyzing sequential data, including network traffic, which represents time-ordered information flows.

However, despite their high accuracy and ability to model temporal dependencies, standard LSTM implementations are characterized by significant computational costs. This manifests itself in a large number of parameters, high inference time, and memory consumption, making them difficult to use in resource-constrained environments, such as embedded or edge devices.

To reduce the computational complexity of LSTMs without replacing the architecture with lighter alternatives, various optimization methods are used. One such method is to reduce the number of layers and the size of the hidden state. This allows for a reduction in the number of model parameters and operations performed during the forward and backward passes. For example, switching from two LSTM layers with 128 neurons to a single layer with 64 neurons results in a significant reduction in resource consumption with a negligible impact on accuracy.

Another common method is the use of Truncated Backpropagation Through Time (TBPTT), which limits the length of the sequences through which the gradient propagates. This reduces the depth of the computational graph, reduces the amount of memory used, and speeds up the training process. Post-training quantization is also used, converting model weights from floating-point to integer format with reduced bit depth (e.g., int8). This reduces the model size and speeds up operations at the inference stage, especially on specialized hardware platforms.

Finally, one regularization measure that promotes both model robustness and reduces overfitting is the use of dropout. This method involves randomly zeroing some neurons during training, preventing the model from overadapting to the training data.

Methods of training neural networks

With the development of the internet and the increasing volume of data transferred, network security is becoming increasingly important. One of the key defense tools is intrusion detection systems (IDS), which can identify malicious activity in network traffic. Traditional signature-based methods are often ineffective against new, unknown attacks, which is driving the active implementation of machine learning and artificial intelligence.

Artificial neural networks, particularly recurrent networks with long short-term memory (LSTM), have proven themselves to be effective in analyzing sequential data such as network traffic [1]. However, the effectiveness of ANNs largely depends on the choice of optimization algorithm during the training process.

The aim of this study is to compare two widely used optimizers, SGD and Adam, in training an LSTM model for binary network traffic classification on the real-world CICIDS-2017 dataset [2]. The study included data preparation and preprocessing, designing the LSTM network architecture, conducting a series of experiments with both optimizers on datasets with varying degrees of class imbalance, and a subsequent detailed analysis of the resulting performance metrics to identify the strengths and weaknesses of each method.

The primary training method for ANNs is the backpropagation algorithm combined with gradient descent [3]. The training process is based on stepwise changes to the neural

network parameters in the direction opposite to the loss function gradient. This update gradually brings the model closer to its optimal state. This paper examines two main variations of this approach:

SGD (Stochastic Gradient Descent) is a stochastic gradient descent method in which parameters are updated based on a gradient calculated from a single sample or a small set. It is characterized by simplicity and low cost per iteration, but can converge slowly and requires careful selection of the training step.

Adam (Adaptive Moment Estimation) is an algorithm that uses estimates of gradient statistics to select its own learning rates for different parameters. This results in a more stable and faster optimization process for a variety of problems [4].

To combat overfitting during the training process, regularization methods such as Dropout and Early Stopping were used [5].

Experimental part. Dataset and preprocessing

The experiments were conducted using the open-source CICIDS-2017 dataset provided by the Canadian Institute for Cybersecurity. It contains realistic mixtures of normal and malicious traffic. Three subsets were selected for analysis, reflecting different attack types and the degree of class imbalance (Table 1).

Table 1

Subsets of the CICIDS-2017 dataset used

File name	Attack scenario	Normal/malicious traffic ratio
Friday-WorkingHours-Afternoon-DDos.pcap_ISCX.csv	DDoS attacks	43.3% / 56.7%
Friday-WorkingHours-Afternoon-PortScan.pcap_ISCX.csv	Port scanning	44.4% / 55.6%
Tuesday-WorkingHours.pcap_ISCX.csv	FTP/SSH attacks	96.9% / 3.1%

Data preprocessing included the following steps:

1. Binary markup: The original labels (Label) were converted to binary format: 'BENIGN' → 0 (normal traffic), all others → 1 (malicious traffic).

2. Feature scaling: Numerical features were normalized to the range [0, 1] using MinMaxScaler.

3. Preparation for LSTM: Data is transformed into a 3D format [samples, timesteps, features], where timesteps=1.

4. Sample s it: The data is split into training and testing sets in a ratio of 80/20, with 20% of the training set used for validation.

5. Exclusion of the Fwd Header Length.1 attribute (identical to the Fwd Header Length attribute)

6. Converting string values of Flow ID, Source IP, Destination IP, Timestamps attributes to numeric values [6]

Model architecture and training parameters

The experiments were conducted on identical LSTM models. Training parameters [7]:

- L ss function: binary_crossentropy
- Number of eras: 10
- Mini-batch size: 6

Results and discussion

Based on the obtained training results, graphs were constructed.

Below, in the figures, are graphs of the dependence of accuracy on the number of epochs during training using AGD and ADAM using the example of a dumpTuesday-WorkingHours.pcap_ISCX [8].

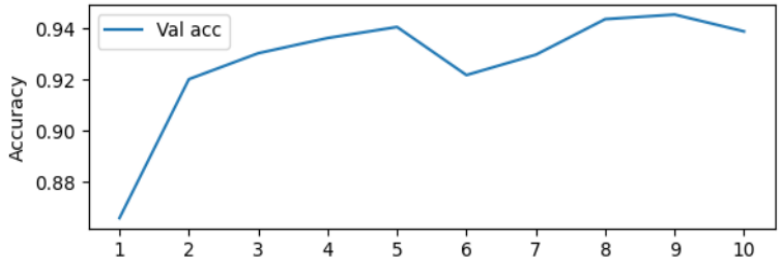


Figure 1. Validation accuracy during training (SGD) plot

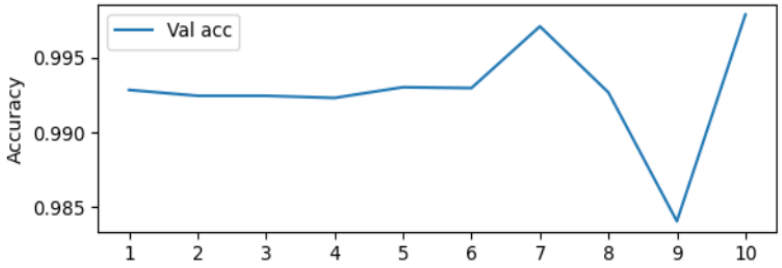


Figure 2. Accuracy plot during validation during training (Adam)

Comparative results of the SGD and Adam optimizers on three datasets for key metrics are presented in Table 2.

Table 2

Comparative results of Adam and SGD optimizers

Optimizer	Friday-WorkingHours-Afternoon-DDos.pcap_ISCX				Friday-WorkingHours-Afternoon-PortScan.pcap_ISCX				Tuesday-WorkingHours.pcap_ISCX			
	Accuracy	Recall	Precision	F1 score	Accuracy	Recall	Precision	F1 score	Accuracy	Recall	Precision	F1 score
SGD	0.9874	0.9811	0.9969	0.9889	0.9897	0.9916	0.9898	0.9907	0.9448	0.9989	0.3596	0.5289
Adam	0.9992	0.9991	0.9996	0.9993	0.9991	0.9991	0.9993	0.9992	0.9979	0.9949	0.9418	0.9677

Analysis of the results allows us to draw the following conclusions [9-14]:

1. On balanced datasets (DDoS and PortScan), both optimizers demonstrated high efficiency, but Adam demonstrated a slight but consistent advantage across all metrics.

2. On the unbalanced dataset (FTP/SSH), a dramatic difference in the optimizer performance was revealed. The model trained with SGD demonstrated an extremely low Precision value (0.36) with a very high Recall value (0.9989). This indicates that the model tends to classify most traffic as an attack, generating a large number of false positives.

3. The del trained with Adam on the same dataset maintained a balance between Precision (0.94) and Recall (0.99), indicating its ability to learn effectively even under conditions of strong class imbalance.

Adam's resilience to imbalance is explained by its adaptive nature, which allows it to more effectively adjust the model's weights for rare classes (malicious traffic), while SGD "overfits" on the dominant class.

Conclusion

This work posed and successfully solved the problem of developing an optimized version of an LSTM model for detecting malicious network traffic with reduced computational costs. The relevance of this topic stems from the increasing demands on the performance and resource efficiency of information security systems, especially in the context of limited hardware capabilities.

To achieve this goal, the architecture of the standard LSTM model was optimized, including the following changes: reducing the number of hidden neurons and layers, applying truncated inverse time error (TBPTT), implementing regularization using Dropout, and quantizing the model after training to int8 format. All these methods are aimed at reducing model complexity without significantly compromising its performance.

An experimental comparison of the standard and optimized models was conducted using the CIC-IDS2017 dataset, which includes both normal and malicious network flows. The analysis showed that the optimized model:

• h s approximately 4 times fewer parameters (34,000 vs. 133,000);

• requires approximately 4 times less memory (0.13 MB vs. 0.51 MB);

• demonstrates an average inference time that is approximately 1.8 times faster (0.0026 sec vs. 0.0047 sec);

• while maintaining high classification performance: Accuracy = 0.86, F1-Score = 0.82, which is only slightly inferior to the original version.

Thus, this study confirms the effectiveness of the proposed approach for reducing the computational complexity of LSTM without significantly losing accuracy.

The study successfully solved the problem of binary classification of network traffic using an LSTM network. A comprehensive comparison of the SGD and Adam optimizers was conducted.

Experiments have shown that the Adam optimizer is superior for malicious traffic detection. It not only demonstrates higher metric values on balanced data but, crucially, maintains high performance under conditions of significant class imbalance, which is typical of real-world network traffic. In contrast, SGD tends to generate an unacceptably high number of false positives under such conditions, making it less suitable for practical use in intrusion detection systems.

Thus, for building network security systems that require high accuracy and minimal false alarms, the use of adaptive optimization methods such as Adam is recommended.

REFERENCES

[1] B. B. Borisenko, S. D. Erokhin, A. S. Fadeev, I. D. Martishin, “Detection of computer attacks using a multilayer perceptron and long short-term memory networks,” *Systems for synchronization, formation and processing of signals*. 2021. Vol. 12, No. 5, pp. 4-13.

[2] S. S. Galizdra, A. Yu. Kudryashova, “Method of biometric identification of a person by a row of teeth based on a photograph with an open smile,” *Systems for synchronization, formation and processing of signals*. 2024. Vol. 15, No. 6, pp. 34-39.

[3] A. Yu. Kudryashova, A. A. Karavanova, “An encryption algorithm for hard drive partitions to protect against intruders,” *Telecommunications and Information Technologies*. 2024. Vol. 11, no. 2, pp. 32-37.

[4] www.unb.ca | Intrusion detection evaluation dataset (CIC-IDS2017) / [Electronic resource] // URL: https://www.unb.ca/cic/datasets/ids-2017.html

[5] studfile.net | Back Propagation Learning Algorithm (Back Propagation – bp)./ [Electronic resource] // URL: https://studfile.net/preview/21852300/page:6

[6] www. vc.ru | Optimizers (Adam, SGD) /[Electronic resource] // URL: https://vc.ru/id4616024/2263731-optimizatory-adam-i-sgd-upravlenie-shagami-obucheniya-nevrosotey
[7] education.yandex | 15.4. Optimization Methods in Deep Learning /[Electronic resource] // URL: https://education.yandex.ru/handbook/ml/article/metody-optimizacii-v-deep-learning/
[8] cyberleninka.ru | Synthesis of a Machine Learning Model for Detecting Computer Attacks Based on the CICIDS-2017 Dataset/[Electronic resource] // URL: https://cyberleninka.ru/article/n/sintez-modeli-mashinnogo-obucheniya-dlya-obnaruzheniya-kompyuternyh-atak-na-osnove-nabora-dannyh-cicids2017
[9] K. O. Safronov, A. Yu. Kudryashova, Yu. V. Molodtsova, “Study of the Relationship between AI Hallucinations, Prompt Length, and Logical Paradoxes: The Role of Kolmogorov Complexity and Semantic Analysis in Ensuring the Integrity of Information Systems,” *REDS: Telecommunication Devices and Systems*. 2025. Vol. 15, No. 3, pp. 22-26.
[10] S. S. Galizdra, A. Yu. Kudryashova, “Method of biometric identification of a person by a row of teeth based on a photograph with an open smile,” *Systems for synchronization, formation and processing of signals*. 2024. Vol. 15, No. 6, pp. 34-39.
[11] A. Y. Kudriashova, S. S. Galizdra and N. V. Toutova, "Designing Implementation of Additional Modules to Increase the Security and Stability of the Biometric Identification System," *2025 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF),* St. Petersburg, Russian Federation, 2025, pp. 1-5, doi: 10.1109/WECONF65186.2025.11017218.
[12] N. V. Toutova, A. Y. Kudriashova, and S. S. Galizdra, "Implementation of Additional Modules to Increase the Security and Stability of the Biometric Identification System," *2025 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF),* St. Petersburg, Russian Federation, 2025, pp. 1-5, doi: 10.1109/WECONF65186.2025.11017156.
[13] A. Yu. Kudryashova, V. A. Zakharova, “Development of information security measures for defense industry enterprises to implement the Digital Economy 2030 policy,” *Telecommunications and Information Technologies*. 2024. Vol. 11, No. 2, pp. 45-51.
[14] A.Yu. Kudryashova, "Development of a program for calculating additional distortions for various models of errors", *T-Comm*, 2022. vol. 16, no.1, pp. 51-58. DOI: 10.36724/2072-8735-2022-16-1-51-58

SYNCHROINFO JOURNAL

www.media-publisher.eu/synchroinfo-journal

RISKS OF TRADITIONAL PASSWORD SYSTEMS IN THE CONTEXT OF ENTERPRISE DISTRIBUTED INFORMATION SYSTEMS

V. A. Dokuchaev [1,2], **I. A. Safonov** [3], **J. Rahmani** [4]

[1] Network Information Technologies and Services, MTUCI, Moscow, Russia, v.a.dokuchaev@mtuci.ru

[2] International Telecommunication Union (GCBI ITU), Geneva, Switzerland

[3] Network Information Technologies and Services, MTUCI, Moscow, Russia

[4] Network Information Technologies and Services, MTUCI, Moscow, Russia

j.rahmani@mtuci.ru

ABSTRACT

Traditional password-based authentication systems continue to be used in modern corporate distributed information systems, despite their vulnerabilities. This article examines the threats associated with traditional password systems, including the psychological aspects of their use, technical shortcomings, and regulatory gaps. Examples of real-world attacks, such as phishing campaigns and credential compromises in industrial information networks, are discussed. Particular attention is paid to password protection in industrial Internet of Things (IIoT) and smart grid systems. Practical recommendations for improving security are offered, including the use of multifactor authentication, credential rotation, the elimination of preset passwords, and the implementation of the Zero Trust concept.

DOI: 10.36724/2664-066X-2025-11-4-15-24

Received: 20.06.2025
Accepted: 23.08.2025

Citation: V. A. Dokuchaev, I. A. Safonov, J. Rahmani, "Risks of traditional password systems in the context of enterprise distributed information systems", *Synchroinfo Journal* **2025**, vol. 11, no. 4, pp. 15-24.

KEYWORDS: *authentication; vulnerabilities; password; IIoT; Smart Grid; Zero Trust; cybersecurity*

Introduction

Traditional password authentication systems remain the primary means of authentication in corporate and critical infrastructures despite growing cyber threats. In 2024, 64% of data breaches worldwide were linked to password compromise, and the average cost of a single incident for businesses reached $4.45 million [1,2]. The number of targeted attacks on industrial facilities increased by 35% over the last two years in Russian Federation. We'll examine the risks of traditional password systems, supported by research and real-world examples from energy, banking, transportation, and the Industrial Internet of Things (IIoT). We'll focus on vulnerability analysis, regulatory requirements, and innovative information security solutions.

Key factors affecting data protection

Modern information security studies unanimously indicate that the human factor remains the main weak link in data protection. According to the Verizon Data Breach Investigations Report (2022), 30% of users still choose primitive passwords such as “123456” or “qwerty,” which demonstrates the persistence of cognitive economy—the tendency to minimize mental effort when memorizing [3]. This trend is exacerbated by the practice of password reuse: 65% of employees use the same credentials for work and personal accounts, violating the principle of account segregation [4].

Phishing attacks, which account for 85% of successful intrusions, exploit fundamental psychological triggers. For example, in 2021 attackers targeted the American company Colonial Pipeline by sending an email with a fake notification from management. An employee entered the password “Colonial2021!” into a phishing form, which allowed the attackers to deploy the DarkSide ransomware and paralyze the operation of the pipeline. The damage amounted to $4.4 million, including the ransom paid in bitcoins [5]. Figure 1 shows the distribution of methods of successful attacks on organizations.

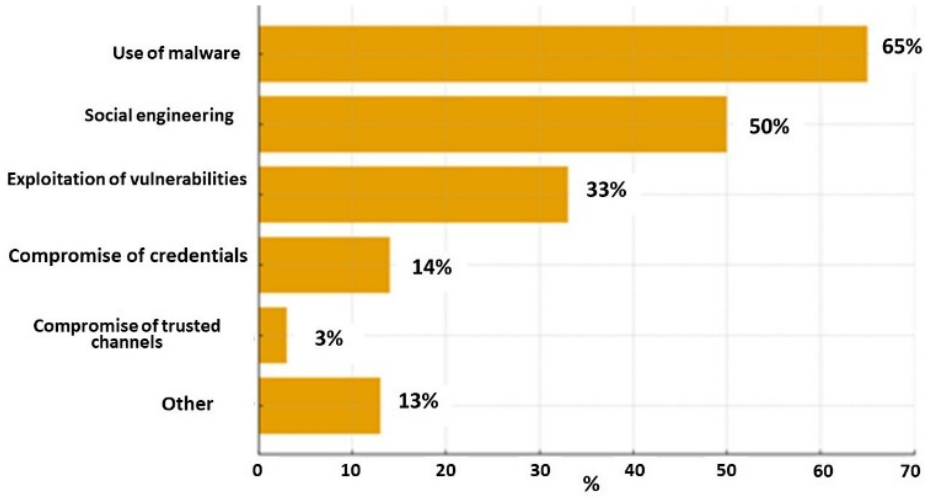


Figure 1. Distribution of Successful Attack Methods Against Organizations

Vulnerabilities of password systems are exacerbated by the technical archaism of infrastructures. According to the ENISA Report on ICS Security (2024), 40% of industrial systems in the EU still use the Telnet and FTP protocols, which transmit passwords in plaintext. This enables attackers to intercept data through sniffing attacks, as occurred in 2023 in Poland, where attackers decoded a password from unencrypted Telnet traffic of a power-grid control system [6].

Cryptographic algorithms also remain an Achilles’ heel. The MD5 and SHA-1 hash functions, used in 30% of corporate systems, are vulnerable to collisions and rainbow tables. For example, RFC 6238 (2024) estimates that cracking an MD5 hash for the password “admin123” takes only 2 seconds [7].

Organizational errors in password management often act as a catalyst for large-scale attacks. A vivid example is the Maersk incident (2017), where exploitation of the EternalBlue vulnerability in SMBv1 led to the spread of the NotPetya ransomware. The attack was made possible by the lack of network segmentation and the use of a single password for all administrative accounts. The company's losses exceeded $300 million, including the downtime of 76 port terminals [8].

A key problem remains the weak adoption of multi-factor authentication (MFA). According to NIST Special Publication 800-63B (2024), only 22% of companies use MFA for all employees, which contradicts the principles of Zero Trust – an architecture that requires verification of every request regardless of its source [9, 10].

Examples of attacks on critical information infrastructure

In the modern world, cyberattacks on critical infrastructure are becoming increasingly sophisticated, demonstrating how digital threats can transform into physical destruction and socio-economic crises (the transition of information-security incidents into industrial-safety incidents). The incidents considered below not only influenced approaches to information security but also showed that the vulnerabilities of industrial and energy systems require a global rethinking of defense strategies.

The use of the ransomware (encryptor) Stuxnet became the first cyberattack aimed at the physical sabotage of industrial equipment. The specialized malicious software was created to attack Siemens SCADA systems used at the Iranian nuclear facility in Natanz. The virus spread via infected USB drives, exploiting several zero-day vulnerabilities in Windows. Thanks to stolen digital certificates, Stuxnet remained unnoticed, gradually modifying the control parameters of centrifuges. This led to their abnormal operation, physical wear, and failure of about 1,000 units of equipment. The consequences of the attack forced the global community to revise standards for protecting critical facilities, emphasizing the need to isolate industrial networks from external threats [11].

The attack by attackers using the NotPetya encryptor quickly grew into a global cyber-pandemic. The malware used the EternalBlue vulnerability in the Windows SMB protocol, similar to the WannaCry exploit, to encrypt hard drives and block the operation of computers. Government agencies, logistics giants such as Maersk, and industrial enterprises around the world became victims. The economic damage exceeded $10 billion, and the scale of the spread showed how a local incident can trigger an international crisis. NotPetya also emphasized the importance of timely software updates and segmentation of corporate networks [12-14].

A group of attackers used the BlackEnergy malware, distributed through phishing emails, to penetrate the SCADA systems of energy companies. After gaining access, the attackers shut down several substations, leaving more than 200,000 people without electricity. Additional data-wiping methods complicated recovery, turning the attack into an example of well-planned sabotage. This incident became a starting point for the development of new standards for protecting energy facilities from cyberthreats [15].

Internet of Things (IoT) devices [16] are of significant interest to attackers. The Mirai botnet demonstrated the danger of the widespread use of unsecured IoT devices. The malware scanned the internet for gadgets with default passwords, combining them into a network for large-scale DDoS attacks. In October 2016, the attack on the DNS provider Dyn caused the collapse of services such as Twitter, Netflix, and GitHub. The event led to stricter security requirements for IoT devices and a reassessment of the role of "smart" technologies in critical infrastructure [17].

Password attack methods

Protecting credentials remains one of the key tasks of information security; however, attackers are constantly improving methods of compromising passwords. Modern attacks combine technical vulnerabilities with manipulation of the human factor, which makes them especially dangerous. Below are the main strategies used to steal or crack passwords, as well as their impact on the security of information systems.

Phishing, as a method of social engineering, is aimed at deceiving users in order to obtain their credentials. Attackers imitate trusted services by sending fake emails, SMS messages, or making voice calls. Victims are redirected to fake web pages that are visually indistinguishable from the original platforms, where they enter their logins and passwords. This method remains one of the most widespread due to its ease of implementation and high effectiveness, especially under conditions of insufficient user awareness [18].

Figure 2 shows the distribution of social-engineering channels used by attackers.

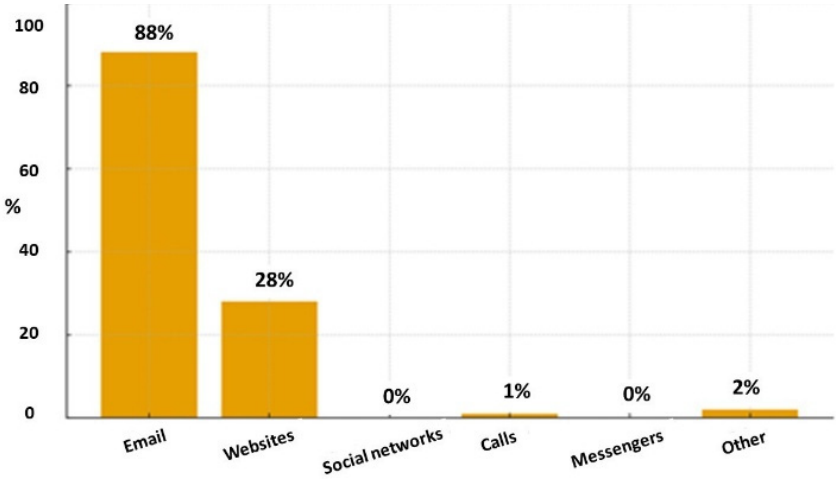


Figure 2. Distribution of Social Engineering Channels Used by Attackers

Credential stuffing attacks are based on exploiting the human habit of reusing passwords across different resources. Attackers use automated bots to test credentials that leaked in the past across numerous platforms. A login–password combination compromised as a result of a social-network breach can be used to access banking services or corporate systems. The effectiveness of this method grows due to large-scale database leaks and the weak adoption of multi-factor authentication.

Real-time data interception is another threat to password confidentiality. A Man-in-the-Middle (MitM) attack is carried out over unsecured public Wi-Fi networks, where an attacker inserts themselves into the communication channel between the user and the server. This attack technique includes substituting SSL certificates, which makes it possible to decrypt traffic, or redirecting the victim to phishing resources. This approach is especially dangerous for employees working remotely and underscores the need to use a VPN and strict certificate validation.

Direct password-guessing methods remain relevant despite the development of defensive mechanisms. Brute-force attacks involve systematically enumerating all possible character combinations, which requires significant computing resources but is effective against short or simple passwords. A dictionary attack, in turn, uses precompiled lists of popular words, phrases, or passwords from past leaks. Both methods are often combined with acceleration tools such as task parallelization on GPUs, which makes them a threat even to systems with basic protective measures.

Let us give an example of the probability of cracking a password by the brute-force method. In the modern digital world, the resistance of a password to brute-force attacks is a key aspect of data protection. Attackers use increasing computing power and optimized algorithms to crack weak combinations in a matter of hours. However, the reliability of a password depends not only on its length, but also on the diversity of characters, as well as on the strategies used to slow down attacks. We introduce the following designations:

N – total number of unique passwords;
C – size of the character set;
L – password length;
P – probability of a successful password guess;
K – number of attacker attempts;
T – time, in seconds;
R – guessing speed (attempts per second);
S – number of parallel processes;
$P(t)$ – probability of compromise within time t (in seconds);

H – entropy.

Total number of possible combinations: $N = C^L$.

Probability of a successful crack after K attempts: $P = K/N$.

Time required to crack: $T = \frac{N}{R * S}$.

Probability of a crack within time t: $P(t) = \frac{t * R * S}{N}$.

Password entropy: $H = L \cdot \log_2(C)$.

Password strength is determined by its entropy – a measure of uncertainty it creates for an attacker. According to NIST standards, the minimally acceptable entropy is 80 bits, which is achieved through a combination of password length (a minimum of 12 characters is recommended) and character diversity: letters (lowercase and uppercase), digits, and special symbols. For example, a 12-character password using 76 available symbols (Latin letters, digits, special characters) provides about 85 bits of entropy, which makes it resistant to attacks even at a high guessing speed (up to 1 billion attempts per second).

However, it is important not only to create a complex password but also to consider its lifetime: if an attacker would need years to crack it, such a password can be considered reliable. For critical systems, an additional level of protection is provided by two-factor authentication, which reduces the probability of a successful compromise to a minimum even if the password is exposed.

According to studies [18], phishing and credential stuffing occupy leading positions in terms of frequency of use, whereas brute-force attacks are gradually losing relevance due to the introduction of lockout mechanisms after multiple attempts. Thus, it can be concluded that password security depends not only on their complexity, but also on user behavior, the quality of traffic encryption, and the timely updating of security policies. A combination of technical measures – such as multi-factor authentication – and regular employee training makes it possible to reduce risks, turning the password from a weak link into a reliable barrier to attackers.

Regulatory legal documents defining password requirements

In Russia, the information security of critical infrastructures is regulated by a number of documents aimed at minimizing risks associated with vulnerabilities of password systems. FSTEC Order No. 239 establishes the mandatory use of passwords at least 12 characters long for state institutions and strategic enterprises, which is consistent with the international standards NIST SP 800-63B [19].

However, as shown by a 2024 study by Kaspersky Lab [20], 45% of Russian companies do not comply with this requirement, limiting themselves to passwords of 8-10 characters. This is due both to employees' cognitive resistance and to the absence of automated control systems.

The Decree of the President of the Russian Federation No. 250 [21] supplements these measures with a requirement for network segmentation and regular password audits at critical information infrastructure facilities. Despite this, studies by Positive Technologies show that 80% of attacks on industrial enterprises are associated with the use of default passwords such as "admin" or "1234" [22].

This indicates a systemic failure in identity and access management (IAM), especially in the segment of IoT devices, where firmware updates often require stopping production processes. Figure 3 shows the distribution of "victim organizations" by industry, which confirms the need to ensure security in the industrial sector.

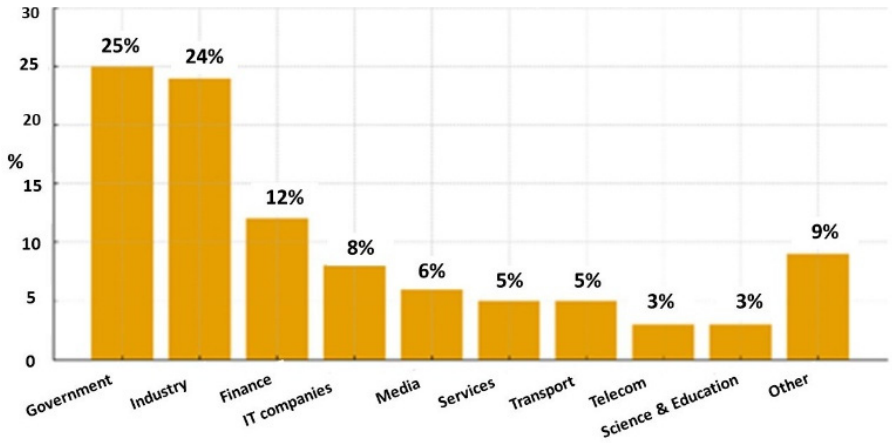


Figure 3. Victim Organizations by Industry

According to Kaspersky Lab's 2024 report [20], 60% of Russian companies do not conduct regular password audits, which contradicts the requirements of GOST R ISO/IEC 27002-2021. This creates conditions for latent threats such as unauthorized access to industrial process control systems (ACS TP).

A 2023 study by Positive Technologies [17] revealed that 55% of incidents in industry are associated with insiders abusing privileged accounts. For example, in the energy sector employees often use administrative passwords for remote access, ignoring the principle of least privilege (PoLP).

In an analysis of cyberattacks conducted by Rostelecom [23], it is noted that 30% of incidents start with employee phishing, which correlates with global trends. Targeted campaigns (spear phishing), in which attackers use social engineering to gain access to SCADA systems, are particularly dangerous.

Threats to critical information infrastructures

Critical information infrastructures (CII) around the world face a growing number of cyberthreats driven by increasing digitalization and the integration of network technologies. Among the most vulnerable areas are the Industrial Internet of Things (IIoT), smart grids (Smart Grid), and transport and logistics control systems. These domains are united by their reliance on network technologies and the need to maintain high reliability. However, these very characteristics make them targets for attackers.

The spread of industrial IIoT devices has made it possible to significantly increase production efficiency and automate many processes; however, this progress is accompanied by new threats [24,25]. One of the main problems is that a significant portion of such devices remains insufficiently protected due to the use of preinstalled passwords. A study by Positive Technologies showed that the owners of 15% of IIoT devices have never changed the default credentials, which makes them vulnerable to attacks using guessing methods [26]. In addition, industrial IIoT devices often have limited computing resources, which makes it impossible to use modern encryption algorithms and complex authentication mechanisms. As a result, attackers can intercept control commands and inject malicious commands into automated systems, which can lead to production downtime or even industrial accidents [27].

The energy industry, as one of the most important parts of critical infrastructure, also faces serious cybersecurity challenges. One key problem is the insufficient level of authentication when accessing control systems. In a number of energy companies there is no mandatory requirement to use multi-factor authentication (MFA), which increases the risk of credential compromise and unauthorized access to SCADA systems [28]. In addition, outdated software continues to be operated at many substations and distribution nodes. According to the European Union Agency for Cybersecurity (ENISA), about 40% of energy facilities in the EU run software with known vulnerabilities [29]. This creates preconditions for attacks that exploit zero-day methods, which can lead to power outages over large areas.

The transport [30,31] and logistics sector is also susceptible to cyberthreats, since traffic control systems, airports, seaports, and railway hubs actively use network technologies for coordination and process optimization. However, in many cases the security of such systems remains insufficient. One common problem is the use of default or weak passwords to access control systems. In a number of cases, the operational networks of transport hubs are not separated from corporate information and telecommunications networks, which creates an additional threat. The lack of clear segmentation allows attackers who have gained access to one system to spread the attack to other critical nodes. This can lead to transport delays, disruptions in logistics chains, and significant financial losses.

Recommendations for protecting industrial internet of things (IIoT) systems and devices

The Industrial Internet of Things (IIoT) is a rapidly evolving environment in which intelligent devices, sensors, and automated control systems interact. Under these conditions, traditional password-based authentication methods face significant risks, including brute-force attacks, phishing, and the exploitation of preinstalled credentials. In this regard, it is critically important to implement reliable mechanisms for protecting credentials.

First and foremost, it is necessary to completely abandon preinstalled passwords and apply methods of automatic password rotation. This will minimize the likelihood that attackers will successfully guess credentials. An important aspect of protection is the use of multi-factor authentication (MFA), including a combination of hardware tokens, biometric data, and cryptographic keys. This approach significantly increases the level of security and reduces the risk of account compromise.

Additionally, attention should be paid to network segmentation and access control. IIoT devices must operate in separate network segments with clearly defined routing rules and access restrictions through identity and access management (IAM) systems. This will prevent unauthorized interaction attempts between devices and increase resilience to attacks. It is also critically important to update firmware regularly and apply security patches, since software vulnerabilities can be used to bypass authentication mechanisms.

In addition, secure data-transfer protocols must be used. Outdated and insecure protocols such as Telnet and FTP should be replaced with protected alternatives. This will ensure reliable encryption of transmitted data and prevent the possibility of interception by attackers.

Smart grids are a key element of modern energy infrastructures, providing efficient management of power distribution. However, the high degree of digitalization of these systems makes them vulnerable to various attacks, including the compromise of operator credentials and the hacking of control devices. In this regard, protecting passwords and credentials in such environments requires a comprehensive approach.

The most promising authentication method in smart grids is the use of X.509 digital certificates in combination with hardware security modules (HSM). This makes it possible to eliminate dependence on traditional passwords and ensure a high level of account protection. It is also important to implement strict password-management policies, including the mandatory use of complex passwords of at least 14 characters with regular rotation.

To prevent privilege-escalation attacks, it is necessary to apply the principle of least privilege (PoLP) and use specialized privileged access management (PAM) systems. This will limit the possibility of unauthorized use of high-privilege accounts. In addition, special attention should be paid to monitoring authentication events using security information and event management (SIEM) systems. Analysis of account behavior will allow prompt detection of anomalies, such as login attempts from unusual locations or at unusual times.

Additionally, methods for encrypting communication channels should be employed. All communication between smart-grid components must be carried out through protected and certified VPN tunnels. This will prevent man-in-the-middle attacks and increase the overall resilience of the infrastructure to threats.

Control systems for critical facilities – such as water supply, transport hubs, and industrial enterprises – require strengthened protection of credentials, since their compromise can lead to catastrophic consequences. Under such conditions, it is necessary to implement the Zero Trust concept, in which trust in a user is formed on the basis of multi-factor identification regardless of their location.

One of the key aspects of protection is the regular auditing of accounts. All inactive and obsolete accounts must be removed in a timely manner, and access rights must be reviewed regularly using role-based models (RBAC). This will minimize risks associated with inherited or forgotten accounts that could be used by attackers.

The use of hardware authentication means – including PKI tokens and WebAuthn technologies – plays an important role. These methods eliminate dependence on static passwords and significantly complicate the possibility of account attacks. In addition, strict control over remote access must be ensured. Control systems must be completely isolated from external networks, and remote access must be carried out exclusively through protected gateways with additional verification.

Finally, increasing staff awareness remains an important element of protection. Regular training and testing will help employees promptly recognize phishing attacks and handle credentials safely, which will significantly reduce the likelihood of account compromise.

Prospective authentication methods

Biometric authentication is becoming increasingly popular due to its high reliability and ease of use. Modern methods include fingerprint recognition, iris scanning, facial recognition, and even gait or heartbeat analysis. These technologies significantly reduce risks associated with theft or leakage of credentials, since biometric data are difficult to forge or transfer to third parties. However, biometric authentication also faces challenges related to data privacy and the possibility of compromise in the event of leaks. It is important to use secure methods for storing biometric templates.

The FIDO2 and WebAuthn protocols offer a fundamentally new approach to authentication that eliminates the need for passwords. Instead, cryptographic keys stored on hardware tokens or in special device modules are used. This approach removes risks associated with phishing and password interception, because authentication is tied to a specific device and does not require transmitting secret data over the network. The development of this area promotes a transition to fully passwordless authentication, increasing the security level of corporate and critical systems.

The concept of decentralized identification systems (Decentralized Identifiers, DID) is based on the use of blockchain and distributed ledgers to store and verify digital identity credentials. Unlike traditional centralized systems, DID allows users to manage their own digital identifiers, removing the need to trust third parties. This is especially important in the context of protecting personal data and preventing information leaks. However, large-scale adoption is still limited by a lack of regulatory standards and the need to refine infrastructure to support decentralized solutions.

Artificial intelligence (AI) and machine learning play an increasing role in authentication systems. User-behavior analysis algorithms make it possible to detect suspicious activity and adapt authentication mechanisms in real time. Systems can track typing speed, geolocation, login time, and other parameters to automatically request additional authentication when anomalies are detected. This approach can significantly reduce the likelihood of compromise even if credentials are exposed. In addition, AI is used to improve biometric systems, increasing recognition accuracy and reducing false positives. In the future, artificial intelligence may become a key element of adaptive authentication, providing a balance between security and user convenience.

Conclusion

The analysis has shown that traditional password systems remain a vulnerable link in the protection of corporate distributed systems and critical infrastructures such as the Industrial Internet of Things, smart grids, and infrastructure control systems.

The main problems include the human factor, outdated protocols, shortcomings in access management, and non-compliance with regulatory requirements. The implementation of Big Data and Artificial Intelligence technologies, while being powerful drivers of economic development, simultaneously gives rise to new potential risks of unauthorized access to confidential information. To minimize risks, it is necessary to apply a comprehensive approach that includes strengthened authentication, strict password management policies, the use of hardware security measures, and continuous monitoring of security events. The implementation of the Zero Trust concept and multi-factor authentication will significantly reduce the likelihood of successful attacks and increase the resilience of the infrastructure to information security threats.

REFERENCES

[1] Verizon Data Breach Investigations Report [Online], 2022. Available: https://www.verizon.com/business/resources/reports/dbir (accessed 03.01.2025).

[2] V. A. Dokuchaev, “Digital transformation: New drivers and new risks,” *2020 International Conference on Engineering Management of Communication and Technology (EMCTECH 2020): Proceedings*, Vienna, October 20-22, 2020. New York: Institute of Electrical and Electronics Engineers (IEEE), 2020, p. 9261544. DOI: 10.1109/EMCTECH49634.2020.9261544.

[3] OWASP Authentication Cheat Sheet [Online]. Available: https://cheatsheetseries.owasp.org (accessed 17.01.2025).

[4] Google Security Blog [Online], 2019. Available: https://security.googleblog.com (accessed 12.02.2025).

[5] NIST Special Publication 800-63B. Digital Identity Guidelines: Authentication and Lifecycle Management [Online]. Available: https://doi.org/10.6028/NIST.SP.800-63b (accessed 07.01.2025).

[6] ENISA Report on ICS Security [Online]. Available: https://www.enisa.europa.eu (accessed 10.01.2025).

[7] RFC 6238 (TOTP): Time-Based One-Time Password Algorithm [Online]. Available: https://tools.ietf.org/html/rfc6238 (accessed 13.01.2025).

[8] Zero-Trust Network Architecture [Online] / Forrester Research, 2020. Available: https://www.forrester.com/zero-trust/ (accessed 15.02.2025).

[9] NIST Special Publication 1108R3. Framework for Improving Critical Infrastructure Cybersecurity. Gaithersburg: NIST, 2020.

[10] E. S. Yusifov, V. A. Dokuchaev, “Why Kubernetes security problems require a zero-trust strategy,” *Information Society Technologies: Proceedings of the XVII International Industry Scientific and Technical Conference*, Moscow, March 2-3, 2023. Moscow: Media Publisher, 2023, pp. 116-118.

[11] J. Rahmani, “Study of risk-management methods in the infocommunication system of an energy-producing company of the Islamic Republic of Iran,” *T-Comm*, 2022, vol. 16, no. 8, pp. 30-37. DOI: 10.36724/2072-8735-2022-16-8-30-37.

[12] V. A. Dokuchaev, N. S. Kalmykov, “Aspects of applying segment routing in software-defined networks,” *Prospective Technologies in Information Transmission Media: Proceedings of the 14th International Scientific and Technical Conference*, Vladimir, October 6-7, 2021. Vladimir: Vladimir State University named after A. G. and N. G. Stoletovs, 2021, pp. 164-168.

[13] J. Rahmani, “The main approaches to evaluating the effectiveness of applying the risk analysis and management methodology at energy company,” *T-Comm*, 2022, vol. 16, no. 9, pp. 46-55. DOI: 10.36724/2072-8735-2022-16-9-46-55.

[14] N. S. Kalmykov, V. A. Dokuchaev, “Analysis of the main methods for ensuring network security in software-defined networks,” *Telecommunication and Computing Systems 2020: Proceedings of the International Scientific and Technical Conference*, Moscow, December 14-17, 2020. Moscow Technical University of Communications and Informatics. Moscow: Goryachaya Liniya – Telecom, 2020, pp. 63-70.

[15] V. A. Dokuchaev, A. A. Kalfa, J. Rahmani, “Typical structure of the corporate infocommunication system of an energy-producing company (IRI),” *III Scientific Forum “Telecommunications: Theory and Technology” TTT-2019: Proceedings of the XXI International Scientific and Technical Conference*, Kazan, November 18-22, 2019. Vol. 1. Kazan: Kazan National Research Technical University named after A. N. Tupolev, 2019, pp. 298-299.

[16] V. A. Dokuchaev, A. V. Shvedov, A. V. Ermalovich, “The “Internet of Things” concept as the basis for the development of information and communication technologies (ICT),” *Current Problems and Prospects for Economic Development: Proceedings of the Jubilee XV International Scientific and Practical Conference*, Gurzuf, November 17-19, 2016 / Crimean Federal University named after V. I. Vernadsky. Gurzuf: IP Brovko A. A., 2016, p. 298.
[17] J. Rahmani, V. A. Dokuchaev, “Analysis of trends in the development of the communications industry in the Islamic Republic of Iran,” *Information Society Technologies: Proceedings of the XIV International Industry Scientific and Technical Conference*, Moscow, March 18-19, 2020. Moscow: Media Publisher, 2020, pp. 300-301.
[18] E. A. Petinova, N. Kh. Odinaev, “Phishing analysis: statistics, methods and solutions in cybersecurity,” *Youth. Science. Future. 2024: Collection of Papers of the II International Scientific and Practical Conference*, Petrozavodsk, April 22, 2024. Petrozavodsk: IP Ivanovskaya I. I., 2024, pp. 143-153. DOI: 10.46916/24042024-3-978-5-00215-361-9.
[19] Order of the FSTEC of Russia of December 25, 2017 No. 239 “On the approval of requirements for ensuring the security of significant objects of the critical information infrastructure of the Russian Federation” [Online]. Available: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239 (accessed 21.04.2025).
[20] Kaspersky. Kaspersky Lab analytical reports 2024 [Online]. Available: https://securelist.ru/kaspersky-incident-response-report-2024/112080/ (accessed 21.04.2025).
[21] Decree of the President of the Russian Federation No. 250 of 01.05.2022 “On additional measures to ensure the information security of the Russian Federation” [Online]. Available: http://publication.pravo.gov.ru/Document/View/0001202205010023 (accessed 21.04.2025).
[22] Positive Technologies. Outcomes of IS incident investigations in 2021–2023 [Online], 2023. Available: https://www.ptsecurity.com/ru-ru/research/analytics/outcomes-of-IS-incident-investigations-in-2021-2023-years (accessed 02.02.2025).
[23] Solar. Attacks on Russian companies in Q2 2023 [Online], 2023. Available: https://rt-solar.ru/analytics/reports/3610/ (accessed 13.02.2025).
[24] V. Yu. Statyev, V. A. Dokuchaev, V. V. Maklachkova, “Information security in the Big Data space,” *T-Comm*, 2022, vol. 16, no. 4, pp. 21–28. DOI: 10.36724/2072-8735-2022-16-4-21-28.
[25] V. A. Dokuchaev, “The impact of new information and communication technologies on the privacy of personal data,” *Current Problems and Prospects for Economic Development: Proceedings of the XXIII International Scientific and Practical Conference*, Simferopol–Gurzuf, October 17-19, 2024. Simferopol: IP Zueva T. V., 2024, pp. 12-15.
[26] Positive Technologies. Owners of 15% of IoT devices have never changed the default password — Xakep [Online]. Available: https://xakep.ru/2017/06/20/iot-stats/ (accessed 04.03.2025).
[27] Threats to IoT devices in 2023 | Securelist [Online]. Available: https://securelist.ru/iot-threat-report-2023/108088/ (accessed 10.03.2025).
[28] European Union Agency for Cybersecurity (ENISA). EU Cybersecurity in 2024: Insights from ENISA Latest Report [Online]. Available: https://cyble.com/blog/eu-cybersecurity-in-2024-insights-from-enisa-latest-report/ (accessed 14.02.2025).
[29] Threats to the energy sector. Analytical report. CISA, 2023 [Online]. Available: https://www.cisa.gov/sites/default/files/2024-09/FY23_RVA_Analysis_508.pdf (accessed 13.02.2025).
[30] V. A. Dokuchaev, “Analysis of international recommendations on transport security under digital transformation,” *Trends in the Development of the Internet and Digital Economy: Proceedings of the VI International Scientific and Practical Conference*, Simferopol–Alushta, June 1–3, 2023. Simferopol: IP Zueva, 2023, pp. 15-17.
[31] V. A. Dokuchaev, “Some aspects of transport security under digital transformation,” *Theory and Practice of Economics and Entrepreneurship: Proceedings of the XX International Scientific and Practical Conference*, Simferopol–Gurzuf, April 20-22, 2023 / Edited by N. V. Apatova. Simferopol: Crimean Federal University named after V. I. Vernadsky, 2023, pp. 31-34.

SYNCHROINFO JOURNAL

www.media-publisher.eu/synchroinfo-journal

DEVICE EFFICIENCY FOR ROUGH ESTIMATION OF NOISE-LIKE SIGNAL SYNCHRONIZATION PARAMETERS

Vu Sy Dao [1], **Svetlana F. Gorgadze** [2]

[1] Le Quy Don University of Science and Technology, Hanoi, Vietnam
vusydaomtusi@gmail.com

[2] Moscow Technical University of Communications and Informatics, Moscow, Russia
s.f.gorgadze@mtuci.ru

ABSTRACT

The functional diagram of a device for roughly estimating the synchronization parameters of a periodic, noise-like, complex signal using direct spread spectrum is considered. The device is based on a unit for accelerated digital convolution of the received and reference signals. The main criterion for its effectiveness is the duration of the acquisition time for synchronization parameters with the received signal, depending on the signal-to-noise ratio at the receiver input. As shown, this duration is related to the length of the pseudorandom code used to generate the signal, the energy of which must be accumulated in the convolution unit to ensure the specified values of the probabilistic characteristics for correct estimation of the synchronization parameters with predetermined errors.

DOI: 10.36724/2664-066X-2025-11-4-25-33

Received: 28.05.2025
Accepted: 22.07.2025

Citation: Vu Sy Dao, Svetlana F. Gorgadze, "Device efficiency for rough estimation of noise-like signal synchronization parameters", *Synchroinfo Journal* **2025**, vol. 11, no. 4, pp. 25-33.

KEYWORDS: *rough estimation of synchronization parameters, synchronization of noise-like signal with direct spread spectrum, digital convolution of received and reference signals, probabilistic characteristics of synchronization parameter estimation, digital device for convolution of pseudo-random sequences*

Introduction

A rough estimate of the synchronization parameters of a noise-like complex signal (NLS) – frequency and time delay – is usually performed with a predetermined accuracy, determined by the size of the projection of the main peak of its ambiguity function (AF) onto the frequency-time plane over which it is plotted, the shape of this peak, and the signal-to-noise ratio at the input of the receiver's decision unit (DM) [1-3]. Formally, such an estimate corresponds to the procedure for detecting and distinguishing quasi-orthogonal signals, which are distinguishable copies of the received signal, shifted relative to each other in frequency and time, against a background of white Gaussian noise [1]. The UF calculated in the receiver is formed as a multiple convolution of the received and reference NLS [4].

The aim of this work is to develop a methodology for studying the effectiveness of a rough estimate of the synchronization parameters of a periodic noise-like NLS, taking into account restrictions on the duration of the pseudorandom sequence (PRS), which can be processed in its digital convolution unit. It should be noted that periodic direct spread spectrum signals are often used in various digital radio systems as synchronization signals, as well as in satellite radio navigation systems [3, 4].

Functional device diagram for rough estimation of synchronization parameters

In accordance with the maximum likelihood criterion, a rough estimate of the frequency and time delay of the NLS, formed on the basis of a binary PRS, against the background of white Gaussian noise can be carried out in a device, the functional diagram of which is shown in Figure 1.

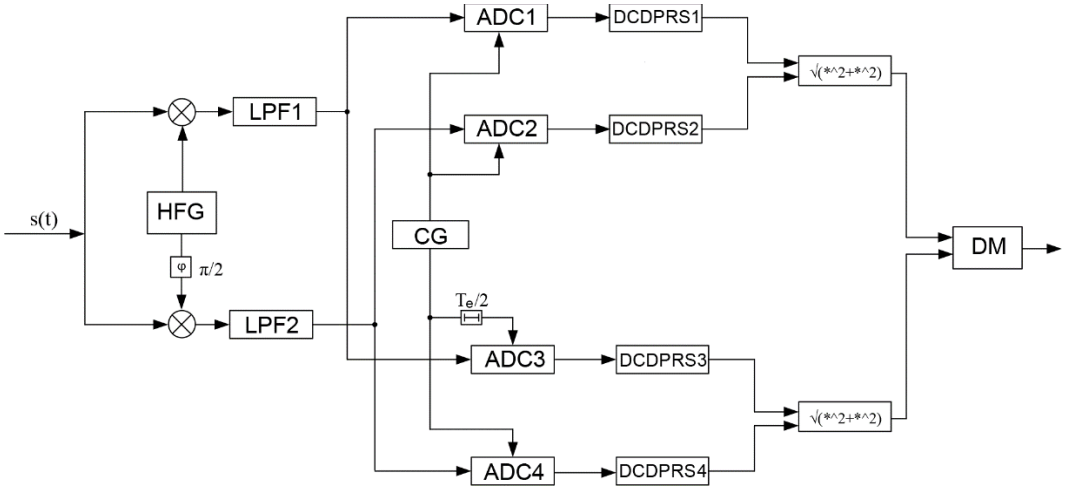


Figure 1. Functional device diagram for rough estimation of frequency and time delay parameters

Its successful operation, focused solely on estimating the time delay of the synchronization system, is possible only if the deviation of its carrier frequency from its known value is no greater than the permissible value [1, 2, 6-8]. Therefore, if the basic element of the receiving device is a digital PRS convolution device (DCDPRS), on the basis of which the synchronization system is formed, then sequential discrete tuning of the reference frequency signal at its input is necessary in order to isolate the corresponding video signal. In a more complex version of the device for rough estimation of synchronization parameters, it is necessary to parallelize the generation of reference frequencies with the same frequency step, covering the entire frequency uncertainty region of the synchronization system, or part of it. In the latter cases, it is necessary to simultaneously use DCDPRS, the number of which corresponds to the number of reference frequencies being generated. Thus, a rough estimate of the frequency of the received synchronization system will also be realized.

In Figure 1 shows the delay time estimation block of the SLC, when the high-frequency generator (HFG) generates one reference frequency f_0, i.e., for the in-phase channel – the signal $2\cos(2\pi f_0 t + \varphi)$, and for the quadrature channel – the signal $-2\sin(2\pi f_0 t + \varphi)$. Then, when an additive mixture of the useful SLC and white Gaussian noise acts at the receiver input, the signal component at the output of LPF1 $s(t)$ will be formed as a function $Re[\dot{S}(t)\exp(j(2\pi\Delta ft+\varphi)]$, and at the output of LPF2 – as $Im[\dot{S}(t)\exp(j(2\pi\Delta ft + \varphi)]$, where $\dot{s}(t)$ is the complex envelope $s(t)$ [2], is the Δf difference between f_0 and the carrier frequency $s(t)$, and φ is the random phase shift between the signals of these frequencies. Further, in order to use the digital convolution device of the PRS (DCDPRS), the received signals must be discretized in time using an ADC with a clock frequency generated by the clock generator (CG) and, according to Kotelnikov's theorem, twice the clock frequency f_c of the NLS. In this case, the frequency f_c generated by the CG must be equal to the clock frequency of the NLS1/T_e, and its doubling is realized by secondary sampling of the signal with the same frequency, but with a shift of half the duration of the elementary symbol of the NLS, where T_e is the duration of its elementary pulse.

It is necessary to take into account that f_c, in reality, it cannot precisely match the clock frequency of the received signal due to the instabilities of the master clock generators on both the transmitting and receiving sides. Moreover, at the stage of rough estimation of synchronization parameters, clock synchronization of the received signal cannot yet be achieved. In the case of small signal-to-noise ratios, when the latter can exceed the level of the useful signal at the receiver input by hundreds of times, clock synchronization of the ADC is performed only at subsequent stages during its refinement in the automatic time adjustment device [1, 2]. As a result, after a certain period of time, so-called slippage will inevitably occur at the output of either ADC (ADC1 or ADC2), i.e., two ADC samples will fall on the same elementary pulse, or one such pulse will be missed. However, due to the shift of the NLS samples at the inputs of DCDPRS3 and DCDPRS4 relative to the samples at the inputs of DCDPRS1 and DCDPRS2 on $T_e/2$, a slip will never occur simultaneously at the inputs of these devices. Nevertheless, it is obvious that the duration of the NLS processed in any of the USPS should not be greater than the time between two consecutive slips.

Note that, given the known relative instability of the master clock generators δ, this duration is easy to calculate, since each subsequent NLS sample in the ADC will be generated not after a time interval equal to T_e, but after $T_э + \delta T_э$ or $T_э - \delta T_э$. As a result, a slip will occur δ^{-1} after NLS samples, which corresponds to the permissible PRS length that can be processed in any DCDPRS. It is assumed that the value corresponds to the maximum possible relative deviation of the frequency of any of the master clock generators from its nominal value.

At the outputs of the DCDPRS, we obtain time samples of the in-phase and quadrature components of the AF of the NLS $\dot{\chi}(\tau, \Delta f, \varphi)$, where τ is the time shift of the received NLS relative to the reference. For averaging over φ, the modulus of this function $\dot{\chi}\left|(\tau, \Delta f)\right|$ is calculated. A decision on the value τ in the DM is made when the samples at both of its inputs, or at any of them, exceed the threshold level.

Note that if exceeds the projection size Δf of the main peak of the AF on the frequency-time plane, the NLS will most likely not be detected. Therefore, it is necessary to sequentially reconfigure f_0 each time by a step corresponding to the frequency sampling interval of the NLS, which is related to the projection size of the main peak of its AF on the frequency-time plane.

Efficiency of Accelerated Search for NLS

The performance indicator for a coarse estimate of the frequency and time delay of a synchronization system is the probability of its correct detection p_{cd} in one of the intervals of the uncertainty region for these parameters, given a false alarm probability p_{fa},

depending on the signal-to-noise ratio at the input of the receiver's decision unit (DU) in the presence of an input signal. However, this ratio depends on the duration of signal energy accumulation in the receiver. Therefore, for given values, the primary performance indicator for a coarse estimate of the synchronization parameters p_{cd} and p_{fa} will be a function of the required duration of this accumulation, i.e., the duration of the synchronization system, the convolutions of which are calculated in the receiver. However, as shown above, there are limitations on the duration of the PRS processed in the DCDPRS. Therefore, to ensure the required values in the NLS synchronization parameter p_{cd} and p_{fa} coarse estimate device for any signal-to-noise ratio at the receiver input, the use of an energy accumulator at the output of the convolution unit can be considered. The probability of false detection-discrimination of orthogonal signals against a background of white Gaussian noise can be written as follows [7]:

$$p_{\text{лт}} = 1 - (1 - p_{\text{лт0}})^m \tag{1}$$

where

$$p_{\text{лт0}} = \int_{bq}^{\infty} z \exp(-z^2 / 2) dz = \exp(-b^2 q^2 / 2) \approx m p_{\text{лт0}} \tag{2}$$

is the probability of false detection of a signal that is actually absent at the receiver input during incoherent reception;

$$m = 2 N m_{\text{ч}} \tag{3}$$

and in this case is proportional to the number of two-dimensional intervals of the uncertainty region of the NLS in time and frequency, the sizes of each of which correspond to the sizes of the projection of the main peak of its AF onto the frequency-time plane (N – the length (period) of the PRS, $m_{ch} = F / 2F_s$ is the number of reference frequencies generated at the input of the DCDPRS, and are the width of the uncertainty region in frequency and the width of the spectrum of the NLS, respectively)); d – is the threshold level, normalized relative to the maximum value of the signal component at the output of the DCDPRS, q^2 – Is the signal-to-noise ratio in power at the input of the receiver DM.

As follows from (2),

$$bq = \sqrt{2 \ln(\frac{m}{P_{\text{ЛТ}}})} \tag{4}$$

that is, the signal-to-noise ratio required to ensure a given p_{fa}, is proportional to the square root of $\ln m$.

The probability of a correct rough estimate of the synchronization parameters of the NLS [1]:

$$p_{\text{обн}} = \int_{bq}^{\infty} z \exp(-\frac{z^2 + q^2}{2}) I_0(zq) [1 - \exp(-\frac{z^2}{2})]^{m-1} dz \tag{5}$$

where $I_0(\cdot)$ is the modified zero-order Bessel function.

Note that if the function $[1 - \exp(-\frac{z^2}{2})]^{m-1}$ is approximated by a unit jump, i.e., its values are assumed to be zero for $z < z_0$ and equal to one for $z \geq z_0$, then for $q \geq z_0$, the probability of a correct rough estimate of the synchronization parameters is approximately equal to one, where $z_0 = \sqrt{2(\ln(m-1)}$. In practice, this is impossible, since in this case, bq should be less than q. However, since the threshold value bq is greater than z_0, the probability of a correct rough estimate of the synchronization parameters tends to one when

$$q^2 > 2 \ln(\frac{m}{p_{\text{ЛТ}}}) \tag{6}$$

From (6), it follows that to increase the probability of a correct estimate of the synchronization parameters, it is necessary to increase the signal-to-noise ratio at the receiver input.

For given p_{cd} and p_{fa}, the required signal-to-noise ratio at the receiver input, i.e., q^2, is determined by the noise-to-signal ratio at its input $[\frac{P_n}{P_s}]_{in}$ and the duration of the periodic signal energy accumulation time in it, i.e., by kN, where k – Is the fraction of the PRS period or the number of its periods, on the basis of which the SRS is formed, the energy of which is accumulated in the receiver. Thus, at the output of the NLS convolution device, the maximum value of the signal-to-noise ratio will be $q^2 = kN / ([\frac{P_n}{P_s}]_{in} + \sigma^2)$, where σ^2 is the variance of the side peaks of the normalized autocorrelation function (ACF) of the PRS of length kN [4]. In this case, a Gaussian approximation of the side peaks of the ACF is considered, the values σ^2 of which for typical types of PRS used to form the NLS have been studied and are given in Table 3.2.7 of [4]. Then, according to [9]

$$p_{\text{обн}} = \int_{bq}^{\infty} z \exp(-\frac{z^2+q^2}{2}) I_0(zq) dz \qquad (7)$$

Note that, for $k < 1$, the so-called aperiodic autocorrelation function (APACF) of the PRS segment is calculated in the DCDPRS, for $k = 1$, its periodic autocorrelation function (PACF), and for $k > 1$, a combination of these functions.

For the case of NLS formation based on an M-sequence (MS), the calculated dependencies P_d on $[\frac{P_n}{P_s}]_{in}$ for $p_{fa} = 10^{-4}$ and 10^{-6}, $k = 0.1, 0.3, 0.5, 1, 3, 5, 10, 50$, $m_{ch} = 10$ are shown in Figures 2 and 3. The Dolph-Chebyshev window function used in the formation of the NLS [11-14] was taken into account in the calculations.

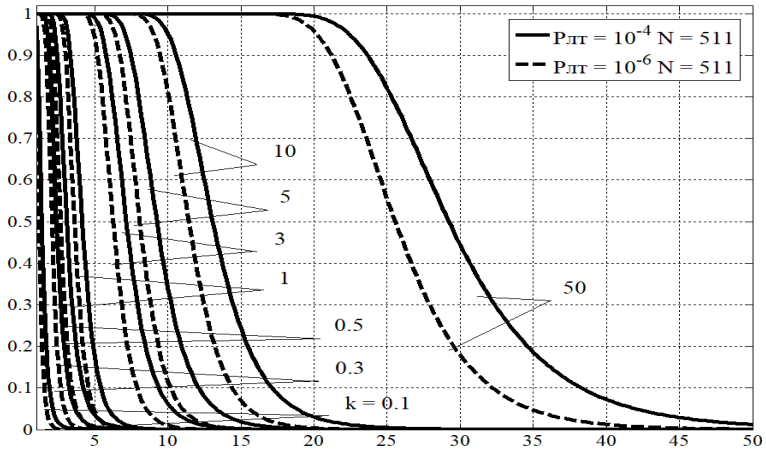


Figure 2. Probabilistic characteristics of the correct rough estimate of the synchronization parameters of the NLS based on MS at $N = 511$ (P_d on $[\frac{P_n}{P_s}]_{in}$).

As follows from the analysis of these figures, the level of the NLS ACF side peaks affects the probability of a correct rough estimate of their synchronization parameters only at low noise-to-signal ratios at the receiver input, less than 10 (i.e., when the noise power exceeds the useful signal by no more than 10 times). For weak signals, when it is necessary to accumulate the energy of several dozen NLS periods, the characteristics of the correlation functions of the used PRS can be ignored, since the noise level at the receiver input has the primary influence on the probability of a correct rough estimate of the synchronization parameters.

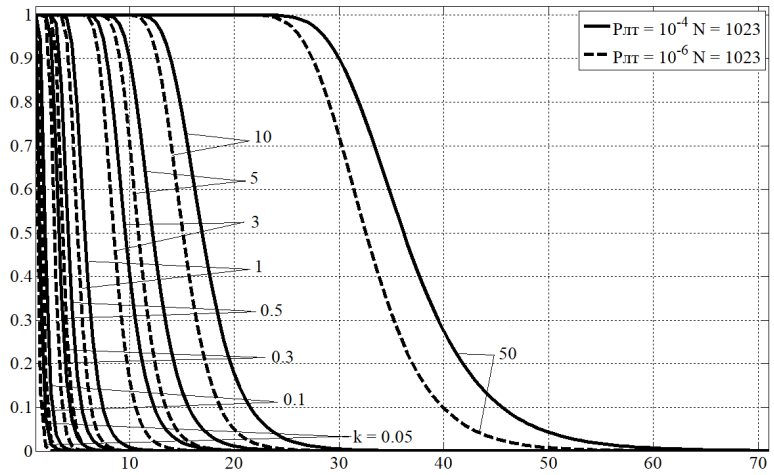


Figure 3. Probabilistic characteristics of the correct rough estimate of the synchronization parameters of the NLS based on MS at N = 1023 (P_d on $[\frac{P_n}{P_s}]_{in}$).

The considered device for rough estimation of the synchronization parameters of the NLS can also be used in the presence of several copies of the same NLS at the receiver input, shifted relative to each other in time by more than T_e, and, possibly, in frequency.

In this case, $q^2 = kN / (\left[\frac{P_{ш}}{P_c}\right]_{вх} + N_c\sigma^2)$, where N_c – is the number of copies of the same NLS simultaneously present at the receiver input. In addition, the probability of a correct rough estimate of the synchronization parameters is $p_{d1} = p_d^{N_c}$. The corresponding probability characteristics in the case of the simultaneous presence of three NLSs at the receiver input, generated based on MP, are shown in Figure 4, and those based on Gold codes – in Figure 5.

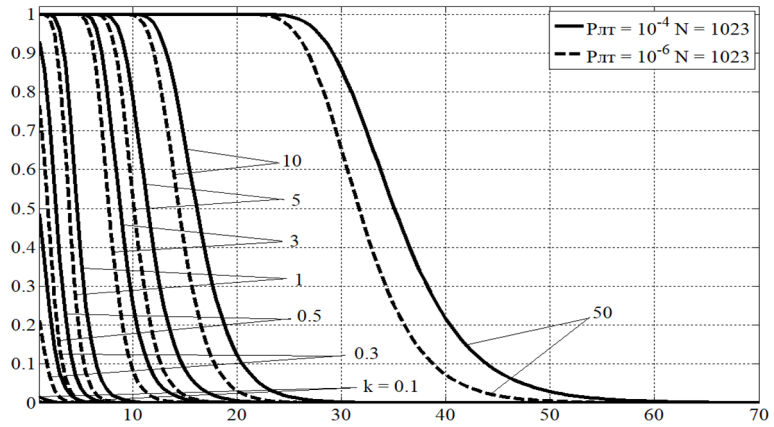


Figure 4. Probabilistic characteristics of the correct rough estimate of the synchronization parameters of three copies of the same NLS, mismatched in time and frequency, when they are formed on the basis of MS with N = 1023 (P_d on $[\frac{P_n}{P_s}]_{in}$)

As can be seen from the analysis of these figures, with increasing N_c efficiency, the estimation of the synchronization parameters of all copies of the NLS, misaligned in time and frequency, simultaneously degrades slightly, compared to the case of estimating the parameters of only one signal. Furthermore, for weak signals, that is, for large values $[\frac{P_n}{P_s}]_{in}$, it does not matter which PRS is used to generate the NLS-MS or Gold codes.

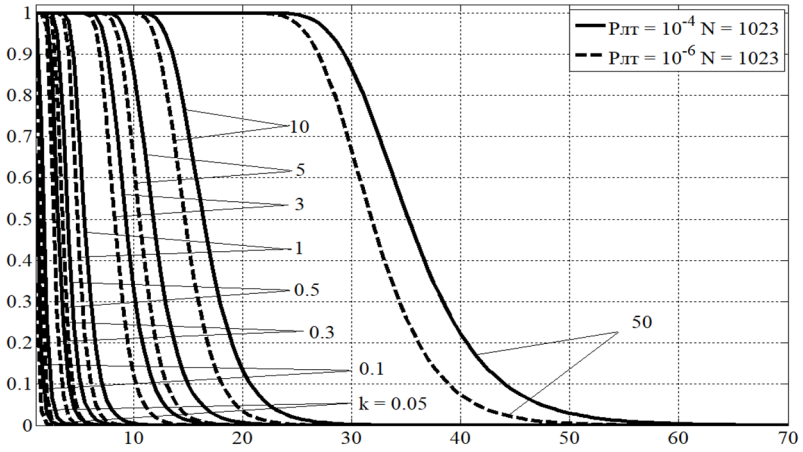


Figure 5. Probability characteristics of the correct rough estimate of the synchronization parameters of three copies of the same NLS, mismatched in time and frequency, when they are formed on the basis of the Gold code with N = 1023 (P_d on $[\frac{P_n}{P_s}]_{in}$)

In addition, it is possible to consider a variant of the DCDPRS containing blocks for calculating the convolutions of several expected NLS at once, formed on the basis of different PRS of the same type. In this case, to calculate the probabilistic characteristics of the correct estimate of the synchronization parameters in the above formulas, it is necessary to use m instead of mN_c, where N_c – is the number of different signals simultaneously present at the input of the receiver. In addition, $q^2 = kN / ([\frac{P_n}{P_s}]_{in} + N_c(\sigma^2 + \sigma_{v1}^2))$, and the resulting probability of correct coarse synchronization is the same as in the previous case $p_{d1} = p_d^{N_c}$, where σ_{v1}^2 is the variance of the cross-correlation functions of the PRS. The values of these variances are also given in [4]. The probabilistic characteristics of the correct coarse estimate of the synchronization parameters of three NLS formed on the basis of different MS, generally mismatched in time and frequency, are shown in Figure 6, and for those based on Gold codes [10] – in Figure 7.

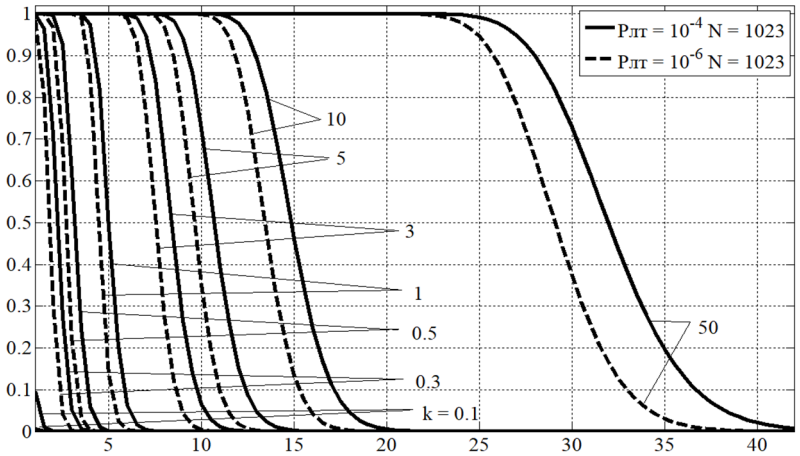


Figure 6. Probabilistic characteristics of the correct rough estimate of the synchronization parameters of three different NLS simultaneously, mismatched in time and frequency, when they are formed on the basis of MP with N = 1023 (P_d on $[\frac{P_n}{P_s}]_{in}$)

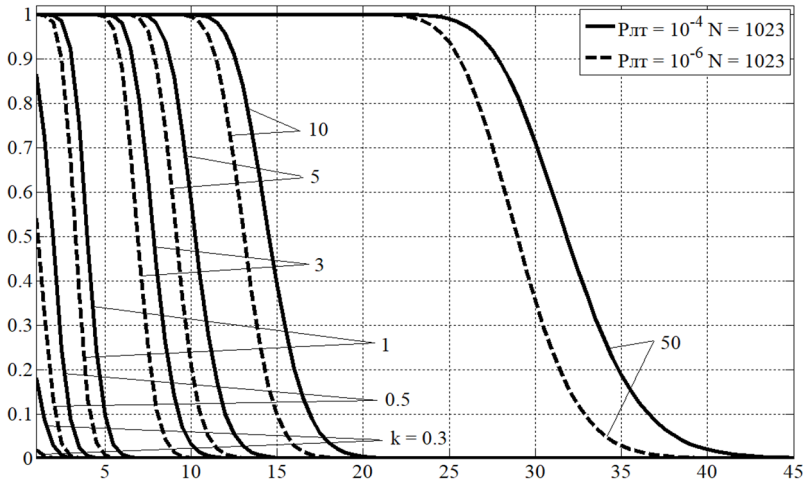


Figure 7. Probabilistic characteristics of the correct rough estimate of the synchronization parameters of three different NLS simultaneously, mismatched in time and frequency, when they are formed on the basis of Gold codes with N = 1023 (P_d on $[\frac{P_n}{P_s}]_{in}$)

As follows from an analysis of these figures, the probabilistic characteristics of a correct rough estimate of the synchronization parameters of several different NLSs simultaneously, misaligned in time and frequency, are somewhat worse than in the case of misaligned copies of the same signal. This is explained by the increased number of two-dimensional intervals of the uncertainty region that must be examined in the DM.

Rough Estimation Time for Synchronization Parameters

The time required for rough estimation of synchronization parameters depends on the time it takes to calculate the convolutions in the DCDPRS. Formally, this time is proportional to the number of blocks shown in Figure 1 and equal to the number of reference frequencies covering part of the frequency uncertainty region of the NLS. Obviously, the minimum time required to achieve synchronization in frequency and time occurs if the generated frequency grid covers the entire frequency uncertainty region at once, while the maximum occurs if the reference frequencies are generated sequentially.

If we consider only one block of the device shown in Figure 1, its operating time is determined by the speed of the digital signal processor implementing the PRS convolution procedure, the length of the processed PRS *kn*, and the convolution calculation algorithm. In the case of a simple correlation algorithm, the computational complexity of the digital convolution procedure is proportional to $(kn)^2$, but accelerated algorithms are known [5].

Conclusion

A methodology has been developed for assessing the efficiency of correctly coarsely estimating the synchronization parameters of noise-like complex signals with a known accuracy, corresponding to the size of the projection of the main peak of their uncertainty function onto the frequency-time plane over which it is plotted. This efficiency corresponds to the duration of the energy accumulation time of the signal-to-noise function required for its detection with predetermined values of their probability characteristics at any signal-to-noise ratio at the receiver input. The methodology is based on a Gaussian approximation of the side peaks of the NLS autocorrelation functions and the peaks of their cross-correlation functions.

REFERENCES

[1] L.E. Varakin, “Communication systems with noise-like signals,” Moscow: Radio and Communications, 1985. 384 p.

[2] S.F. Gorgadze, “Synchronization in infocommunication systems: a tutorial,” MTUCI. Moscow, 2022. 48 p.

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

[4] V.B.v Pestryakov, V.P. Afanasyev, V.N. Gurvits, “Noise-like signals in information transmission systems,” Ed. V.B. Pestryakov. Moscow: Sov. Radio. 1973. 424 p.

[5] Vu Sy Dao, 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.

[6] 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.

[7] S.F. Gorgadze, “Accelerated Digital Algorithm for Synchronization of Noise-Like Signals in Time and Frequency,” *Systems for Synchronization, Generation and Processing of Signals*. 2016. Vol. 7. No. 4, pp. 16-18.

[8] S.F. Gorgadze, V.V. Boykov, “Measuring Signals with Multi-Position Subcarriers for Satellite Radio Navigation Systems,” *Radio Engineering and Electronics*. 2014. Vol. 59. No. 3. P. 264.

[9] V.I. Tikhonov, “Statistical Radio Engineering,” Moscow: Sovetskoe Radio, 1966. 219 p.

[10] 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. Issue No. 96. http://trudymai.ru/

[11] V.P. Dvorkovich, A.V. Dvorkovich, “Window Functions for Harmonic Analysis of Signals,” Moscow: Tekhnosfera, 2014. 105 p.

[12] S.F. Gorgadze, Vu Sy Dao, “Detection and synchronization of weak power spread spectrum 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

[13] S.F. Gorgadze, Vu Sy Dao, A.V. Ermakova, “Synchronization of gold sequences based on fast transform in a truncated basis of walsh-hadamard functions,” *Radio engineering and electronics*. 2024. Vol. 69. No. 2, pp. 137-145. DOI: 10.31857/S0033849424020045

[14] S.F. Gorgadze, Vu Sy Dao, A.V. Ermakova, “Synchronization of m-sequences based on fast hadamard transform,” *Radio Engineering and Electronics*. 2024. Vol. 69. No. 2, pp. 122-136. DOI: 10.31857/S0033849424020031

SYNCHROINFO JOURNAL

www.media-publisher.eu/synchroinfo-journal

GLOBAL BROADBAND DEVELOPMENT: DIGITAL SKILLS

Augustin Vyukusenge [1],

[1] University of Burundi, Bujumbura, Burundi

vyukusengeaugustin@yahoo.fr

ABSTRACT

Regulation have shifted from focusing on basic access to telecommunications and the internet to recognizing different types of digital inequalities and their implications for access to education, healthcare, e-government services, employment opportunities, and participation in the digital economy. This paper presents the first part of a review of global broadband technology development, based on the findings of the ITU report "Status of Broadband Targets." Explore solutions to making broadband policy universal and broadband more accessible. It will also address issues of global internet coverage. It is the second part of the paper "Broadband as key digital infrastructure", continuing this topic, provide an overview, which examines promoting digital skills development, increasing the use of digital financial services, connecting small and medium-sized enterprises to the internet, and bridging the gender digital divide.

DOI: 10.36724/2664-066X-2025-11-4-34-44

Received: 30.06.2025
Accepted: 28.07.2025

Citation: Augustin Vyukusenge, "Global broadband development: digital skills", *Synchroinfo Journal* **2025**, vol. 11, no. 4, pp. 34-44.

KEYWORDS: *ITU; telecommunications; broadband technology development; internet; digital inequalities; digital financial services; gender digital divide*

Introduction

The global broadband market is moving steadily forward, with fiber optics continuing to lead the way. In the first quarter of this year, the number of fixed broadband subscribers reached an impressive 1.45 billion, showing steady growth after a slight decline at the end of last year.

The global broadband market is moving steadily forward, with fiber optics continuing to lead the way. In the first quarter of this year, the number of fixed broadband subscribers reached an impressive 1.45 billion, showing steady growth after a slight decline at the end of last year.

According to Point Topic, 17.6 million new connections were added in the first quarter, with fiber optics accounting for the bulk of the growth, along with wireless technologies to a lesser extent. Satellite, on the other hand, saw a decline in subscribers, but this is likely temporary, and we'll see changes in future reports. The first quarter's growth rate was 1.22%, significantly higher than the previous quarter's growth rate of less than 1%, the lowest since 2019. For the past nine quarters, excluding the most recent, global growth has fluctuated between 1.2% and 1.9%.

The market recovery is largely driven by subscriber growth in East Asia, particularly in China, which accounts for 50.2% of the region's global market share. China is actively developing its space program, recently launching a new batch of LEO satellites as part of the G60 Starlink project, which is designed to compete with SpaceX's Starlink project. By the end of next year, more than 10,000 satellites of the G60 Starlink constellation, also known as Qianfan, are expected to be in orbit.

Meanwhile, home broadband access via fixed wireless access (FWA) is becoming increasingly popular in some global markets, such as the US, Canada, and Italy. Overall, wireless broadband (primarily FWA/5G and fixed LTE) saw connection growth of 8.1% in the first quarter.

Point Topic attributes this growth to demand for connectivity in remote and underserved areas where wired infrastructure is impractical, as well as the desire of some consumers to migrate from traditional broadband services.

Despite impressive growth, wireless broadband still holds a small market share compared to fiber and, to a lesser extent, cable. Fiber remains the clear leader, accounting for over 70% of total connections. The growth in fiber demand is primarily seen in developing countries—six of the ten fastest-growing markets are in emerging economies.

Thus, fiber still leads the global broadband market, but competition is increasing. Satellite communications, FWA and other technologies pose a real threat, and it will be interesting to watch how this competition develops in the future.

The ITU report [1] notes that policymaking has evolved to include new and emerging topics such as digital transformation and artificial intelligence. Significant progress has been made in ensuring accessibility, with the mobile broadband access target achieved globally, while the fixed broadband access target has not yet been met. More than two-thirds of the population regularly uses the internet, and digital skills generally continue to develop as more people become online.

Broadband infrastructure has proven versatile, providing broadband internet access as well as new services and applications, such as distributed computing and artificial intelligence (AI), that rely on broadband infrastructure.

Digital skills

Digital literacy is often identified as one of the main causes of digital exclusion and often among the top answers when people are surveyed about why they do not use the Internet. Digital skills are vital for leveraging ICTs for economic prosperity, human rights, peace and social well-being, as well as acquiring other knowledge and skills (e.g. the use of online platforms such as Duolingo and Babbel for language learning). This Advocacy Target calls for 60% of youth and adults to have achieved at least a minimum level of proficiency in sustainable digital skills by 2025.

This is a target beset with measurement problems. Initial frameworks sought to distinguish between basic, intermediate and advanced skills. More recently, frameworks seek to evaluate ICT skills based on competencies and capabilities and whether individuals can perform certain activities with different types of digital skills: communication & collaboration; problem-solving; safety; content creation; and information & data literacy:

• Communication/collaboration refers to sending messages (e.g. e-mail, messaging service, SMS) with attached files; making calls over the Internet; participating in social networks; and taking part in consultation or voting via the Internet.

• Problem-solving refers to finding, downloading, installing and configuring software; connecting and installing new devices; transferring files or applications between devices; electronic financial transactions; doing an online course; and purchasing or ordering goods or services.

• Safety refers to changing privacy settings and setting up effective security measures.

• Digital content creation refers to using copy and paste tools; creating electronic presentations; using basic arithmetic formulae in a spreadsheet; editing online text, spreadsheets, presentations; and uploading self/user-created content.

• Information/data literacy refers to verifying the reliability of information e.g. getting information about goods or services, reading or browsing newspapers, seeking health-related information.

However, competencies can generally only be measured by in-depth surveys at the local or national level, making comparisons between countries at the international level very difficult. Such local and national surveys are costly and expensive to carry out, meaning that they are mainly confined to high-income countries and regions. Relatively few countries therefore provide data for digital skills, and rarely for all skill areas, due to the cost and difficulty involved.

Further, when digital skills are measured by online surveys, a sample self-selection problem may arise (whereby people without the digital skills to go online or respond to survey are de fact excluded from the survey in the first place). Self-reporting of ICT skills is also very subjective (e.g. some people with strong digital skills may be modest about their achievements, compared to arrogant people who may over-report their paltry digital skills).

Perhaps not surprisingly, communication/collaboration scores the highest across all countries for which data are available, followed by information/data literacy. Upper middle-income countries score lowest for safety and problem-solving.

Another interesting development is the involvement of the private sector in boosting and promoting digital skills in different aspects of life. Insight 5 presents the experience of KT’s AIVLE School in promoting digital skills and pioneering AI education. Another interesting development is the involvement of the private sector in boosting and promoting digital skills in different aspects of life. Insight 5 presents the experience of KT’s AIVLE School in promoting digital skills and pioneering AI education.

Pioneering Inclusive AI Education in Korea

In an era defined by rapid technological advancements, the need for accessible and inclusive education in artificial intelligence (AI) has never been greater. KT’s AIVLE (AIVLE means 'AI + Vision + abLE') School emerged in response to this rising demand, and the program was designed to have participants engage in real-world projects, receive mentorship from industry experts, and gain exposure to AI applications across various domains. It has demonstrated significant impact over the past three years. With approximately 1,800 trainees enrolled, it has a successful employment rate of around 60%, showcasing its effectiveness in preparing participants for the workforce.

The programme aims to be inclusive through its platform-based approach, allowing access to high-quality education from anywhere with Internet and a laptop. It also offers a consultant track, that addresses the market's need for non-IT/humanities majors to participate, and this approach helps ensure individuals from diverse academic backgrounds can contribute to the burgeoning field of AI.

Through collaboration with the government, KT AIVLE School provides free education, ensuring accessibility regardless of income. By bridging the gap in access to AI education and job opportunities, KT's AIVLE School is spearheading a movement towards a more equitable and empowered workforce in the Republic of Korea [1].

Mzansi Digital Learning, an educational platform co-developed by Vodacom and Microsoft, is dedicated to bridging the digital skills gap in South Africa. It offers a broad spectrum of free, zero-rated courses, ranging from basic digital literacy to advanced topics like cybersecurity and generative AI, designed to democratize education and empower all South Africans.

The platform's comprehensive curriculum caters to various levels, ensuring continuous skill advancement in line with individual ambitions. It has made significant strides since its inception, with over 100,000 registered learners, many of whom have successfully completed courses and obtained internationally recognized certifications. This initiative extends its impact beyond individual learners, by fostering a digitally skilled population and contributing to broader societal goals of digital inclusion. A digitally literate society is better equipped to participate in the economy, drive innovation, and address social challenges.

Through Mzansi Digital Learning, Vodacom is contributing to the creation of a digitally proficient and competitive society. The platform's success in advancing digital literacy aligns with the national agenda of reducing unemployment and promoting economic growth through education and skill-building, making it a transformative force in South Africa's journey towards a digitally inclusive future [2].

Digital financial services hold immense potential to transform financial inclusion and allow the most vulnerable within society to access basic financial services including savings accounts, payments, and credit.

The nature of digital financial services continues to evolve –traditional banking services are supplemented and, in some cases, replaced by mobile money services, cryptocurrency transactions and, increasingly, e-wallet services. For example, in China, Chinese residents can now pay for shop transactions by scanning their face, while overseas mobile phone numbers can be used to register Alipay, WeChat Pay, and to make payments either from overseas bank cards, mobile wallets or for some regions, overseas e-wallet for payments by scanning codes.

The GSMA finds international remittances and merchant payments were among the fastest- growing mobile money use cases in 2023, driven in part by the consequences of the COVID-19 pandemic.

Demand for mobile financial services is likely to remain high among unbanked and often marginalized populations. Among registered mobile money account holders, some 1 billion people are still not active regularly on a monthly basis, a big opportunity for the industry to deepen financial inclusion and economic participation.

Beyond infrastructure, increasing use of digital financial services relies on changing people’s attitudes and preferences for these services. It also needs financial literacy and awareness, and successful partnerships among the government, financial institutions, and technology providers to provide the training necessary to use digital financial services effectively and safely.

Digital Skills and Digital Financial Capabilities in the UK

In conjunction with a number of partners, Lloyds Bank (2024) runs an annual survey into digital and financial capabilities of UK consumers. The results provide evidence that financial and digital capabilities have different profiles, although they are linked. For example, financial capabilities remain broadly the same among the UK population, independent of age (prudent and less responsible financial behaviour in terms of spending and/or savings habits are relatively independent of age). However, digital capabilities clearly diminish with age (Figure 1).

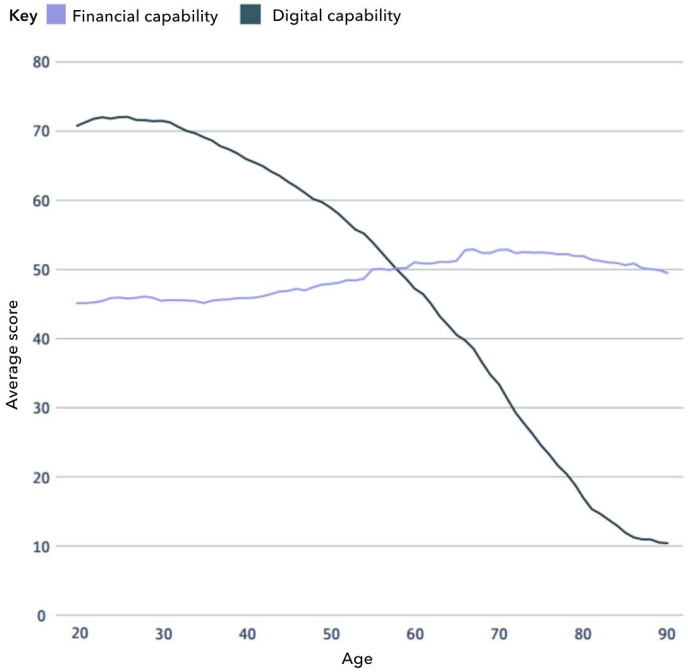


Figure 1. Financial and digital capability in the UK by age, 2023 [1]

Financial and digital capabilities are still linked in some senses, however. Lloyds Bank finds that, for those in the high digital capabilities segment, shopping around for cheaper deals online has helped people to save money during the cost-of-living crisis. The Internet can provide individuals (for 30% of those surveyed) with cheaper deals that can help them with the cost of living. Comparison shopping is not the only way being online can help individuals to save money and manage their finances more effectively. Using budgeting tips (12%) and looking at spending analytics via an app (12%) have also helped people save money. The Internet can enable consumers to manage their finances more effectively.

Along with opportunities come risks, however. People with low digital capabilities might seem more likely targets for some scams, but in fact, time online and exposure are bigger factors in being targeted online. Those with the highest digital capability are more than 11 times more likely to be scammed than those with the lowest digital capability. Looking at victims who have actually been scammed, 50% were in the Very High digital segment, while 4% were in the 'Very Low' segment. Length of exposure to online risks through time online may effectively outweigh any degree of digital capabilities.

Digital Financial Inclusion in Jamaica

There has been a steady increase in the number of individuals and businesses in Jamaica using digital payment platforms, including mobile payments, online banking and electronic payments. According to one survey in 2022, 69% of people had some form of account – 10% had a credit union account, 58% had a bank account, and 1% a mobile money account.

On the supply side, a few pilot platforms were tested prior to 2022, but did not prove successful. In 2022, the Bank of Jamaica introduced the Lynk digital wallet, as well as Jamaica's first digital currency, JAM-DEX. At least two banks and one telecom service provider have developed plans to introduce digital wallets, including one mobile wallet (a type of digital wallet based solely on mobile devices, including phones or smart watches). These developments enabled the Jamaican Ministry of Labour and Social Security (MLSS) and World Food Programme (WFP) to deliver cash transfers to vulnerable populations affected by COVID-19 via a digital payment provider, WiPay.

Through collaboration among the MLSS, WFP and WiPay, adjustments were made to programme delivery, including a dashboard to track distribution and redemption of cash. This dashboard included real-time updates on uptake per location, which then facilitated swift decision-making in deploying mobile payment units in hard-to-reach communities. WiPay also increased its network of agents from 25 agents at the end of 2021 to over one hundred by April 2022.

Problems identified among potential users included a distrust of digital financial services, a fear of being scammed, and a clear age gap in knowledge of and use of digital financial products and services, for both men and women. Among retailers, a digital readiness survey found that retailers had limited knowledge and use of digital payments. 60% of retailers indicated that people in their community do not use digital wallets, while another 34% did not know if their customers used digital wallets.

Micro-, Small- and Medium-sized Enterprises (MSMEs), both formal and informal, make up over 90% of companies worldwide, accounting for 70% of total employment and up to 50% of global Gross Domestic Product (GDP). Broadband connectivity can enable MSMEs to reach new markets, increase their competitiveness and enable them to participate in global market. Broadband connectivity is increasingly vital for accessing digital financial services and e-government services.

The UN Broadband Commission's Advocacy target focuses on improving the sectoral connectivity of MSMEs by 50% over the time period 2018 to 2025, which is relatively ambitious. For example, a sector in which MSMEs are 60% unconnected in 2018, will have only 30% unconnected by 2025. However, data availability for MSMEs globally is very sparse – where data exists, data mostly describes large firms and multinationals, making it difficult to assess this target for SMEs.

MSMEs face considerable and numerous challenges in broadband adoption, including the availability of technologies and suitable apps and services; the ability of SMEs to plan, finance, implement and optimize transformation through digital skills. For a start, adopting digital technologies is often costly. Large firms are generally more resilient, and have greater opportunities to access finance, and can spread these investments over either consumers or different years. In contrast, small businesses may have reduced access to finance, and are less able to pass on the costs to customers.

Many entrepreneurs and firm owners worry about cybersecurity and data privacy, as well as other risks. As a result, MSMEs are less likely to have a strategy to deploy ICT, and are more likely to view ICT training as a 'luxury item' beyond their budget, instead of an investment to save time and costs. Limited budgets, lack of skills and expertise, and concerns about safety and compliance can hinder the ability of small firms to fully embrace digital transformation.

As a result, small businesses may risk falling behind their larger counterparts, and face difficulties in competing effectively in an increasingly digital and an increasingly global marketplace. Digital technologies are often cited as opening up access by firms to foreign markets, but this is a two-way street, and depending on local regulation, digital technologies may also permit foreign firms to enter previously relatively protected markets.

To address these challenges, as well as data availability, the Broadband Commission Working Group on Connectivity for MSMEs, co-chaired by the GSMA and the International Trade Centre (ITC), researched and released the Making Digital Connectivity Work for MSMEs report [3], which outlines barriers and opportunities to MSME connectivity.

Connectivity data disaggregated by enterprise size is generally available for high-income nations, although not always for micro-enterprises. For most low- and middle-income countries, aggregated data on enterprises with Internet access is rarely available. The nature of Internet connectivity also matters – a single person micro-enterprise might find having a smartphone with wireless access sufficient to carry out most operations.

Europe has good SME data availability, due to Eurostat's regular surveys. In 2023, a vast majority (94%) of all EU enterprises6 used a fixed broadband Internet connection, while 78% had a website, 61% used social media, 50% used e-business applications and 22% made e-commerce sales. These broadband connectivity stats were sharply defined by business size, however (Figure 2, top graph). For example, in 2023, 99% used a fixed broadband connection, including 93% of small enterprises and 97% of medium-sized enterprises with broadband access.

In 2023, 45% of all EU enterprises used cloud computing services and 61% used social media. Large enterprises enjoyed significant advantages over all other sizes of firms in terms of access to cloud computing (between 10 and 20 percentage points higher), use of social media, e-commerce and AI (between 1 and 15 percentage points higher) – Figure 2, bottom graph.

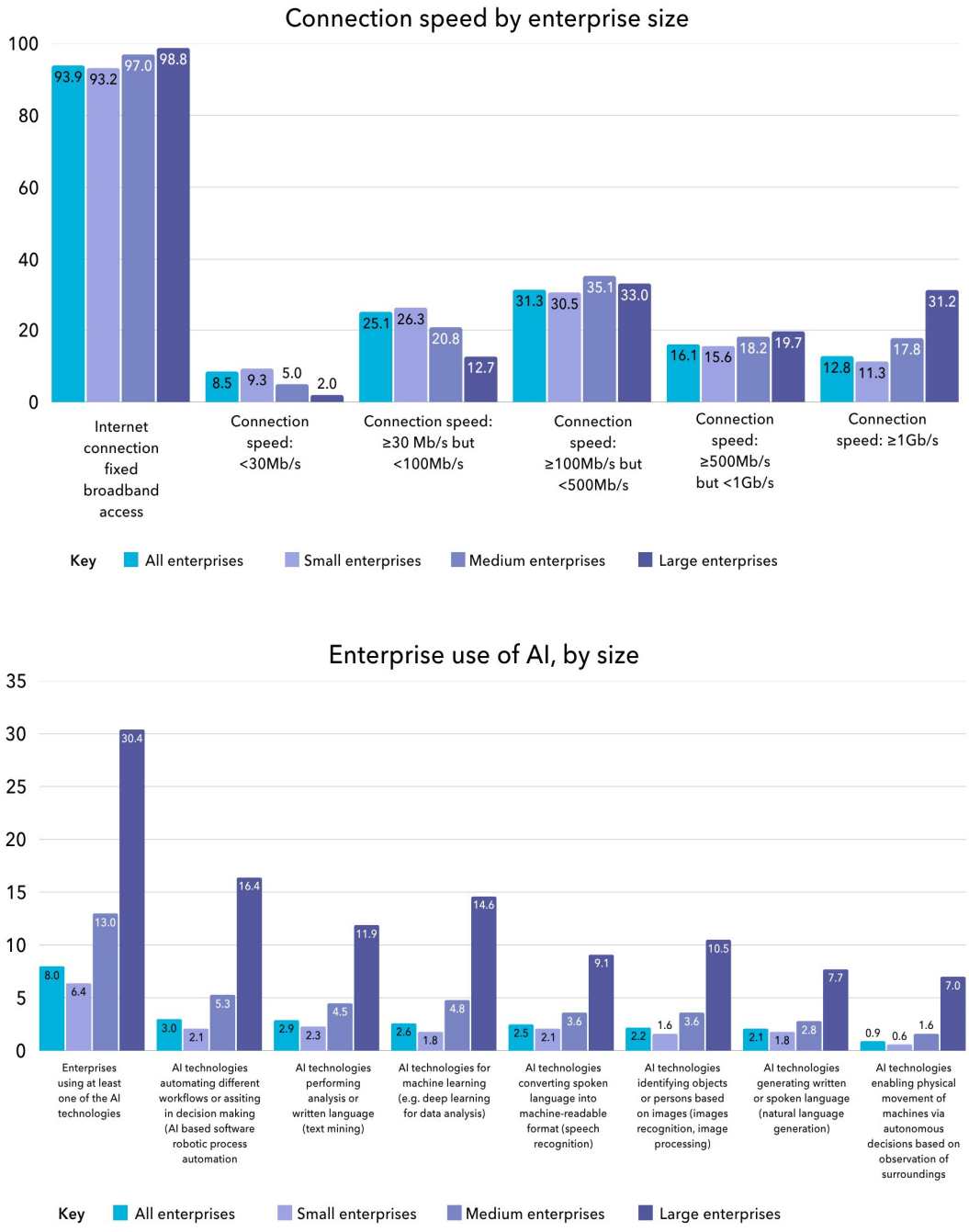


Figure 2. Enterprises with fixed broadband connection in the EU and using AI technologies, 2023 (% enterprises) [1]

By comparison, an IFC/World Bank survey of 3,325 microenterprises enterprises in seven African countries found low levels of smartphone and computer use. Use of the Internet for business purposes was around 7% on average, ranging from 24% in South Africa to 1% in Rwanda. Computer ownership is also low with over 90% of businesses surveyed in Ghana, Kenya, Mozambique, Nigeria, Rwanda, Tanzania and Uganda reporting not having one. Most cited not having a need for Internet access or computers in their business. A UNDP survey focusing on MSMEs in Kenya revealed that they were adversely affected by the pandemic, with one out of every 10 enterprises surveyed indicating a shutdown of their businesses due to the pandemic.

Bridge the gender digital divide aims to ensure that the benefits of broadband Internet can reach everyone, regardless of gender.

According to the latest ITU estimates, in 2024, 70% of all men used the Internet in 2024, compared to 65% of all women (Figure 3). These proportions have increased marginally from 2022, when 69% of all men were using the Internet, compared to 63% of all women.

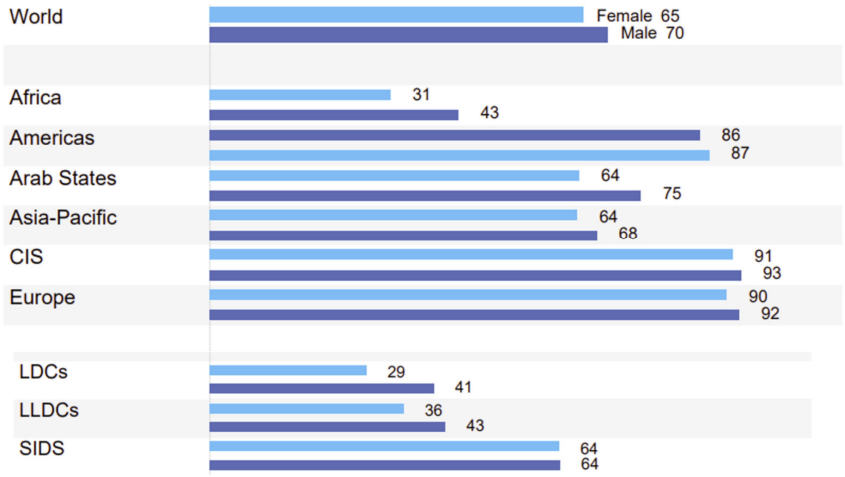


Figure 3. Percentage of female and male population using the Internet, 2024 [1]

Globally, 189 million more men than women used the Internet regularly in 2024 (compared with 244 million in 2023 and 277 million in 2021). The number of women online is therefore 'catching up' with the number of men online. Gender parity increased from 0.90 in 2019 to 0.92 in 2023, and 0.94 in 2024 indicating that the gender digital divide is narrowing overall. This improvement is also reflected at the level of regions and country groups, with one notable exception – in the group of LDCs, gender parity actually decreased from 0.74 in 2019 to 0.70 in 2024.

Generally, the regions and income groups with the highest Internet use also have the highest gender parity scores (Figure 4, left graph), including high-income countries, SIDS, the Americas, CIS countries and Upper Middle-Income Countries (UMICs). In contrast, in the group of Least Developing Countries (LDCs), gender parity has actually decreased, from 0.74 in 2019 to 0.70 in 2024 (shown as diverging gradient between the male and female increases in Figure 4, left graph). Meanwhile, LLDCs have shown only limited progress towards gender parity since 2019.

Gender parity scores are generally lower in terms of mobile phone ownership with larger and more persistent gender disparities in terms of ownership.

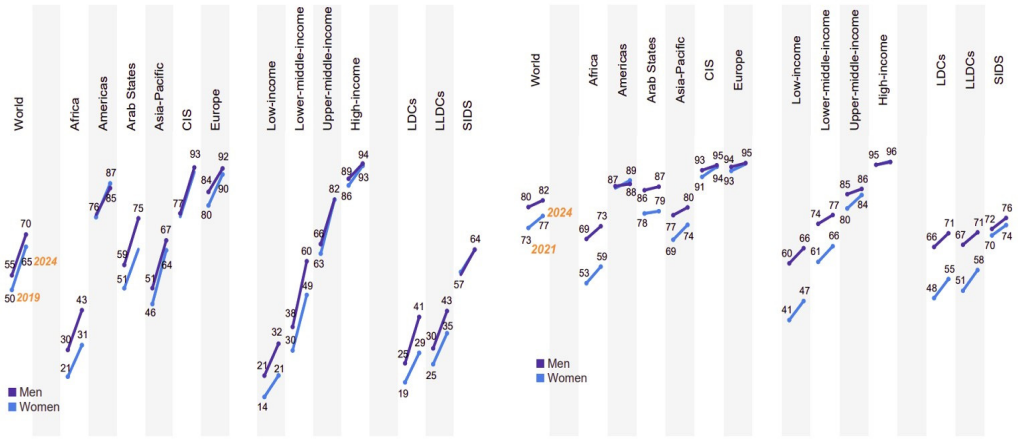


Figure 4. Percentage of individuals using the Internet by gender, 2019 and 2024, and percentage of individuals owning a mobile phone by gender, 2021 and 2024 [1]

Notable gender gaps in mobile Internet access persist in LMICs. The GSMA's Mobile Gender Gap Report 2024 [15] found more women in LMICs are using mobile Internet than ever before, but adoption is slowing and a significant gender gap remains. In 2024, women are 15% less likely than men to use mobile Internet (Figure 5, left graph), compared to 19% in 2023, which means there were 265 million fewer women than men using mobile Internet in these countries.

Mobile gender gaps are widest in Sub-Saharan Africa and South Asia, where over 60% of the 785 million unconnected women in LMICs live. Although the gender gap was widest in South Asia, this gender gap has been reducing fastest (Figure 5, right graph), from 41% to 31%, driven primarily by India where women's adoption increased while men's remained unchanged. The gender gap in mobile Internet narrowed slightly in Sub-Saharan Africa between 2022 and 2023 (from 36% to 32%), but Sub-Saharan Africa's gender gap is still stubbornly similar to what it was in 2017 (34%). The report offers detailed recommendations for operators, Internet companies, policy-makers and regulators and the development community, concluding that concerted action is needed by all stakeholders to close the mobile gender gap.

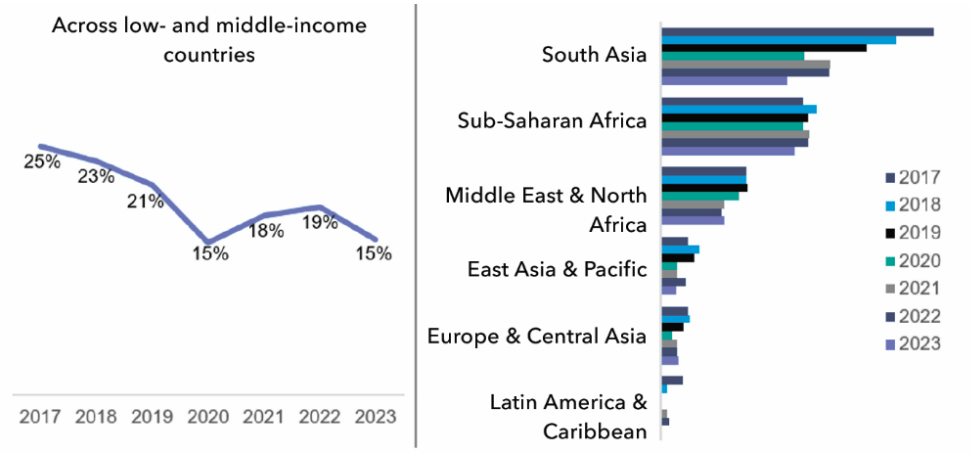


Figure 5. Gender gap in mobile internet adoption across LMICs, and by region, 2017-2023 [1]

Today, gender equality debates are becoming more nuanced and have moved far beyond device ownership and access and towards female participation in Science, Technology, Engineering, Arts and Mathematics (STEAM). Some argue that digital technologies may be less relevant, less functional and ultimately, less helpful for women and girls, unless women are actively involved in designing, developing and deploying technologies.

UNICEF's Game Changers Coalition programme specifically promotes digital skills development and bridging the gender digital divide in seven countries (Armenia, Brazil, Cambodia, India, Kazakhstan, Morocco and South Africa), reaching 100,000 girls and teachers to date.

Supported by the Ministry of Foreign Affairs in Sweden, and co-designed with leading gaming industry partners, the programme infuses innovation into traditional Science, Technology, Engineering, Arts, Maths (STEAM) programming through game development, with a specific purpose of closing gender gaps in STEAM learning and experiences. Adolescent girls participating in this programme learn how to design, code and present their own games, learning digital and tech skills that are essential in the 21st century economy, including high-growth and high-income jobs in gaming and wider tech industries. On average, a participant receives 100+ hours of hybrid instruction to learn coding, design, storytelling for game creation, she will work in a team of peers to develop a game using her imagination and creativity, and participate in a 2-day game creation hackathon "Game Jam.

In Cambodia, the Ministry of Education, Youth and Sport have scaled the teacher curriculum on the national teacher training platform; in Armenia, the regional government of Syunik opened three Innovation Labs, where game creation is taught along with other digital skills; in Kazakhstan, IT Hubs from all over the country are embedding some programme components to attract more females to STEAM careers and further grow the tech industry in the country.

In addition to skills building and experiences for girls, the Game Changers Coalition aims to convene a bold and transformative industry movement in alignment with like-minded companies in the gaming and tech industry, and other shared-purpose public and private partners. Partners who have been engaged in the process to date include the likes of Electronic Arts, Microsoft, Sony Entertainment, Roblox, Ubisoft and Lego Group. Activities include joint co-creation of policies and practices for the industry to enhance Diversity Equity and Inclusion (DEI) efforts and thought leadership demonstrating what the future of tech looks like, as an empowering, inclusive and safe space for all children and adolescents.

And gender-based discrimination may not just be about entry and access to STEM jobs. In September 2024, the IMF published a report about how women may lose out on STEM jobs, while the European Social Survey found that tech may create additional work for women, in addition to their jobs, as they take on more of the tasks involved in 'social connectedness', compared with male patents, guardians or care-givers.

The Vodacom Code Like a Girl Programme, initiated in South Africa in 2017, aims to bridge the gender gap in ICT by equipping underprivileged young girls with STEM skills through a structured ICT training. The programme fosters problem-solving, sequential thinking, creativity, and design skills via coding. Open to females aged 14-18, it requires no prior school subject knowledge. Offered in a hybrid format, the programme includes:

- A virtual self-paced learning environment for those with computer and Internet access, spanning a month with IT support.
- A weeklong boot-camp for those without such access, hosted at universities, Vodacom Foundation computer labs, and schools nationwide.

The curriculum spans Level 1 to Level 5, starting with basic ICT and programming skills, such as web-page design, and advancing to more complex topics. Accredited by the Sector Education and Training Authority, the programme has benefited over 6000 South African students in enhancing their coding and ICT skills. Internationally, the programme has been implemented across Voda- com's markets in Lesotho, Mozambique, DRC, Tanzania, Vodafone Egypt, and Safaricom's markets in Kenya and Ethiopia, with over 16,000 girls having now graduated from the programme.

Conclusions

Importance of broadband Internet for sustainable development remains clear, as our societies continue to grow and develop, and more and more key services either move online or embed digital services.

Targets can play a key role in informing, influencing and shaping policy priorities at the national, regional and global levels. Despite progress in some areas, the number of countries with national broadband plans has stabilized, but Plans continue to become more comprehensive and extend beyond broadband and connectivity issues into holistic Digital Agendas.

Promising new applications in digital financial services are being developed, but data at the global level are relatively outdated.

There has been some progress in digital skills and getting MSMEs online, but problems with data availability mean that progress at the global level is difficult to measure.

Target for gender equality in access to broadband has been achieved by a few individual countries, although this target has not been achieved at the global level.

Broadband stakeholders are well-positioned to deliver on the promise and opportunities of broadband for improving development outcomes.

REFERENCES

[1] The State of Broadband Advocacy Targets 2025. https://www.itu.int/hub/publication/s-pol-broadband-30-2025. Date of access: 10.07.2025.

[2] A. Vyukusenge "Increasing the capacity of fiber-optical transmission systems due to decreasing distances between bearing," Synchroinfo journal. Vol. 6, No. 6. pp. 21-23. 2020. DOI: 10.36724/2664-066X-2020-6-6-21-23.

[3] G. Kundimana and A. Vyukusenge, "Implementation Possibilities of Elastic Optical Networks Technology in Burundi Backbone Network," 2021 International Conference on Engineering Management of Communication and Technology (EMCTECH), Vienna, Austria, 2021, pp. 1-6, doi: 10.1109/EMCTECH53459.2021.9619177.