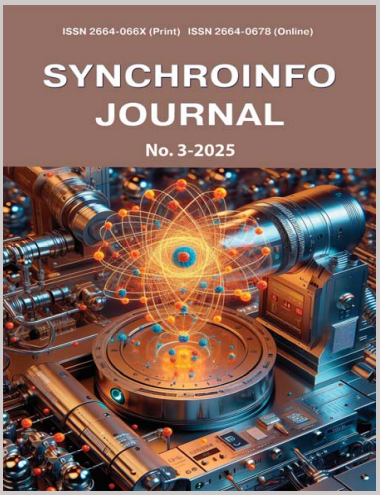
CONTENT

Vol. 11. No. 3-2025



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

A STUDY OF MINIMUM VISIBILITY ROADS CONDITIONS IN RAINY WEATHER

Elchin B. Iskenderzade [1], **Elshan R. Rahimov** [2], **Jeyhun R. Rahimov** [3]

[1] National Aerospace Agency, Baku, Azerbaijan;
[2] Baku Higher Oil School, Baku, Azerbaijan;
[3] Azerbaijan Technical University, Baku, Azerbaijan

ABSTRACT

This article examines the conditions for minimum visibility on roads during rainy weather. Problems of finding a semi-empirical relationship between meteorological visibility on roads and the visibility range for drivers in rainy weather are discussed and solved. Problems of determining the conditions for minimum visibility range for drivers in rainy weather are also solved. A semi-empirical expression linking meteorological visibility and the visibility range for drivers during rain is derived. It is determined that in rainy weather, with a positive regression relationship between background illumination and rain intensity, the visibility range for drivers is reduced to a minimum.

DOI: 10.36724/2664-066X-2025-11-3-2-6

Received: 20.05.2025
Accepted: 21.07.2025

KEYWORDS: *rain intensity,* background illumination*, meteorological visibility, regression relationship, optimization*

Citation: Elchin B. Iskenderzade, Elshan R. Rahimov, Jeyhun R. Rahimov, "A study of minimum visibility roads conditions in rainy weather", *Synchroinfo Journal* **2025**, vol. 11, no. 3, pp. 2-6.

Introduction

As noted in [1], the deterioration of visibility directly due to rain is usually small. For example, if meteorological visibility is within 400 m, then the rain intensity that could cause such low visibility would be 300 mm/hour. However, rains with such intensity occur quite rarely. At the same time, visibility of the road is significantly affected by rainwater accumulated on the car windshield. In [2], the effect of raindrops falling on the car windshield on visibility on the road in rainy weather was studied. In [3, 4], the conditions for deterioration of visibility were investigated using physical modeling of rain as applied to stationary vehicles. In [5-7], it was shown that an increase in rain intensity leads to a decrease in visibility for the driver. In [5], it was shown that visibility decreases with a decrease in background illumination. Moreover, for moving vehicles, visibility was further deteriorated due to the accumulation of water on the windshield. Based on the obtained experimental results, the following model of the dependence of visibility range on the condition of the windshield of a car in rainy weather was proposed.

$$D = C_0(Rt)^{-C_1}\exp(C_2 L_b) \quad (1)$$

where C_0, C_1, C_2 are positive constants; R is the rain intensity; t is the windshield wiper operating period; L_b is the background illumination.

According to [1], the following relationship exists between the rain intensity R and the attenuation coefficient:

$$k = aR^{\gamma} \quad (2)$$

where k is the attenuation coefficient; α and γ are coefficients depending on the experimental conditions.

The optical thickness of the rain factor at a distance L is determined as:

$$\tau = \int_0^L k\,dr \quad (3)$$

As noted above, rain itself has little direct effect on road visibility.

This has been repeatedly verified in practice, and at a rainfall intensity of 45 mm/hour, the attenuation coefficient did not exceed 4 x 10^{-3} (Fig. 1) [1].

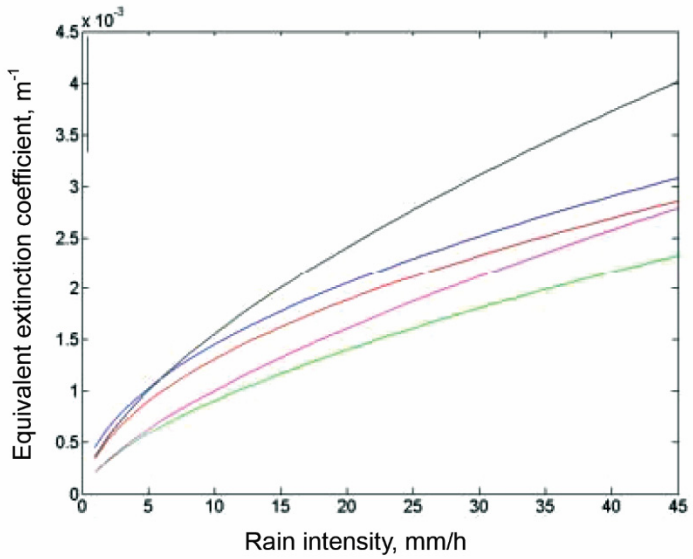


Figure 1. Experimentally obtained curves of dependence of the attenuation coefficient on rain intensity during 1985-2000 [1] by different researchers

However, it should be noted that the driver's workplace is located behind the windshield, and when determining visibility on the road in rainy weather, the effect of the windshield on visibility must be taken into account.

This article further examines the effect of raindrops accumulated on the windshield on the apparent meteorological visibility for drivers driving in rainy weather.

Materials and methods

As indicated in the work [1], meteorological visibility V_{met} is defined as

$$V_{met} = \frac{3}{k} \tag{4}$$

Taking into account expressions (2) and (4), we obtain

$$V_{met} = \frac{3}{aR^{\gamma}} \tag{5}$$

From expression (5) we find

$$R = \sqrt[\gamma]{\frac{3}{aV_{met}}} \tag{6}$$

Taking into account expressions (1) and (6), we have

$$D = C_0 t^{-C_1} \left[\left(\sqrt[\gamma]{\frac{3}{aV_{met,k}}} \right)^{-C_1} \exp(C_2 L_b) \right] = C_0 t^{-C_1} \left[\left(\frac{3}{aV_{met,k}} \right)^{\frac{-C_1}{\gamma}} \exp(C_2 L_b) \right] =$$

$$C_0 t^{-C_1} \left(\frac{3}{aV_{met,k}} \right)^{C_0/\gamma} \exp(C_2 L_b) \tag{7}$$

Where $V_{(met,\,k)}$ is the apparent meteorological visibility for the driver.

As can be seen from expression (7), the indicators D and V_{met} are functionally related. Given t, L_b = const, an increase in D will mean an increase in V_{met}. Consequently, the apparent meteorological visibility $V_{(met,\,k)}$ for the driver, if D is extreme, will also have an extreme property.

Next, let's consider the extreme properties of the indicator D. To do this, we use expression (1). In this expression, we assume t = const. We rewrite expression (1) as

$$D = C_{01} R^{-C_1} \exp(C_2 L_b) \tag{8}$$

where

$$C_{01} = C_0 \cdot t^{-C_1} \tag{9}$$

Next, in expression (8) we introduce for consideration the function

$$L_b = \psi(R) \tag{10}$$

The physical meaning of (10) is that the background glow should have a regressive relationship with the rain intensity as the vehicle moves along the road. Logically, along the road, one can expect both an increasing and a decreasing regressive relationship between *L* and *R*. In the first case, one can assume that an increase in *R* indicates a concentration of rain clouds in the area where the road passes, and in the second case, one can assume that rain clouds are large-scale, also covering background areas. Given the above assumptions, the following restrictive condition can be imposed on the function ψ(*R*).

$$\int_0^{R_{max}} \psi(R)dR = C_3;\ C_3 = const \tag{11}$$

Next, taking into account expression (10) and based on expression (8), we form the following target functional F_1, where

$$F_1 = \int_0^{R_{max}} C_{01}R^{-C_1} \exp\big(C_0\psi(R)\big)\, dR \tag{12}$$

A graphical representation of the hypothetical dual version of function (10) is shown in Figure 2.

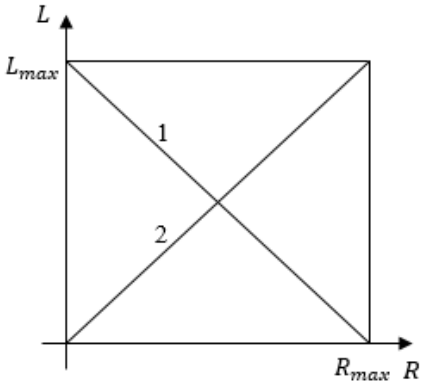


Figure 2. Expected regression curves for L versus R. Numbers indicate:
1 – presence of negative regression; 2 – presence of positive regression

Taking into account expressions (11) and (12), we construct the objective functional F2 for unconditional variational optimization.

$$F_2 = \int_0^{R_{max}} C_{01}R^{-C_1} \exp\big(C_0\psi(R)\big)\, dR - \lambda\left[\int_0^{R_{max}} \psi(R)dR - C_3\right] \tag{13}$$

The solution of the optimization problem (13) according to [8] satisfies the following condition

$$\frac{d\{C_{01}R^{-C_1} \exp\big(C_0\psi(R)\big) - \lambda\psi(R)\}}{d\psi(R)} = 0 \tag{14}$$

From condition (14) we find:

$$C_0C_{01}R^{-C_1} \exp\big(C_0\psi(R)\big) - \lambda = 0 \tag{15}$$

From expression (15) we find

$$\exp\big(C_0\psi(R)\big) = \frac{\lambda R^{C_1}}{C_0C_{01}} \tag{16}$$

Taking the logarithm of expression (16) we obtain

$$\psi(R) = \frac{1}{C_0} \ln \left[\frac{\lambda R^{C_1}}{C_0 C_{01}} \right] \quad (17)$$

When solving (17), F_2 reaches a minimum, therefore, with a functionally (logarithmically) direct dependence of L on R, i.e. if an increase in rain intensity is accompanied by an increase in illumination from the background according to law (17), the visibility distance for the driver can reach a minimum.

Discussion

Thus, the conditions for minimum road visibility for drivers in rainy weather were investigated. The following problems were discussed and solved:

1) Finding a semi-empirical relationship between meteorological visibility on roads and the visibility range for drivers in rainy weather.
2) Determining the conditions for minimum visibility for drivers in rainy weather.

A variational optimization problem was developed to find a possible regression relationship between L (background illumination) and rain intensity (R) while driving on a highway at which the visibility range for drivers in rainy weather reaches a minimum. The possibility of a dual nature for this regression relationship was also considered, i.e., both an increase and a decrease in background illumination with increasing rain intensity are allowed.

Conclusion

The following key findings were obtained as a result of a study examining the impact of rain on road visibility:

1. A semi-empirical expression was derived linking meteorological visibility and the visibility range during rain for drivers, taking into account the accumulation of raindrops on the windshield.

2. It was determined that in rainy weather, with a positive regression relationship between background illumination and rain intensity, the visibility range for drivers is reduced to a minimum.

REFERENCES

[1] N. Hautiere, E. Dumont, R. Bremond, V. Ledoux, “Review of the mechanisms of visibility reduction by rain and wet road”.

[2] K. Garg and S. Nayar, “Vision and rain,” *International Journal of Computer Vision*, no. 75(1), pp. 3-27, October 2007.

[3] T. Kurahashi, Y. Fukatsu, and K. Matsui, “Method of evaluating visibility provided by windshield wipers in rainy conditions,” *In SAE Technical Paper Series*, number 851636, 1985.

[4] R. Morris, J. Mounce, J. Button, and N. Walton, “Visual performance of drivers during rainfall,” *Transportation Research Record*, no. 628, pp. 19-25, 1977.

[5] V. Bhise, J. Meldrum, L. Forbes, T. Rockwell, and E. McDowell, “Predicting driver seeing distance in natural rainfall,” *Human Factors*, no. 23(6), pp. 667-682, 1981.

[6] D. Ivey, E. Lehtipuu, and J. Button, “Rainfall and visibility – the view from behind the wheel,” Technical Report 135-2, College Station, TX: Texas Transportation Institute, 1975.

[7] R. Morris, J. Mounce, J. Button, and N. Walton, “Field study of driver visual performance during rainfall,” Technical Report DOT-HS-5-01172, College Station, TX: Texas Transportation Institute, 1977.

[8] L. E. Elsgolts, “Differential equations and the calculus of variations,” Moscow: Nauka. 1974. 432 p.

SYNCHROINFO JOURNAL

www.media-publisher.eu/synchroinfo-journal

OPTIMIZATION OF THE INFORMATION COLLECTION MODE USING UAVS ON DISTRIBUTED GROUND NETWORKS OF MEASURING SENSORS

Emil M. Akhmedov [1]

[1] National Aerospace Agency, Baku, Azerbaijan

ABSTRACT

This article is devoted to optimizing the data collection mode using UAVs from ground-based measurement network sensors. The problem of optimizing data collection from clustered ground-based sensors using a UAV swarm is formulated and solved. It is shown that the data collection rate can be maximized when there is a direct linear relationship between the bandwidth of the UAV data reception channel and the intensity of white Gaussian noise in the receiving channel.

KEYWORDS: *measuring sensors, data collection, UAVs, data collection speed*

DOI: 10.36724/2664-066X-2025-11-3-7-12

Received: 15.05.2025
Accepted: 18.07.2025

Citation: Emil M. Akhmedov, "Optimization of the information collection mode using UAVS on distributed ground networks of measuring sensors", *Synchroinfo Journal* **2025**, vol. 11, no. 3, pp. 7-12.

Licensee IRIS, Vienna, Austria.

Introduction

As noted in [1], UAVs are designed to perform a wide range of tasks in areas such as aerial reconnaissance, military applications, target detection, pipeline and power line monitoring, georeconnaissance, agriculture, and goods delivery. One such application is forest fire hazard monitoring [2]. Functionally, in many UAV monitoring applications, the unmanned devices collect information from sensors within a distributed network of measuring transducers located throughout the facility's condition monitoring field. As noted in [3], the number of sensors worldwide is projected to reach hundreds of billions by 2030. Consequently, collecting and processing such a large volume of information requires improvements to data collection and preprocessing systems.

According to [4], the use of UAVs for collecting data for the Internet of Things will provide the following advantages:

– High efficiency and flexibility in data collection: UAVs can significantly reduce data collection time, as the flight trajectory can be optimized [5-7];

– Low power consumption and the ability to supply sensors wirelessly [8, 9];

– Wide field of view. At high UAV flight altitudes, it is possible to cover a large area of objects where sensors are located. [10, 11]

However, the specific arrangement of sensors within an area dictates the need to select a special flight trajectory, as well as increased efficiency in collecting information from ground-based sensors.

A model representation of a network in which a group of UAVs collects and transmits information to a base station is shown in Figure 1.

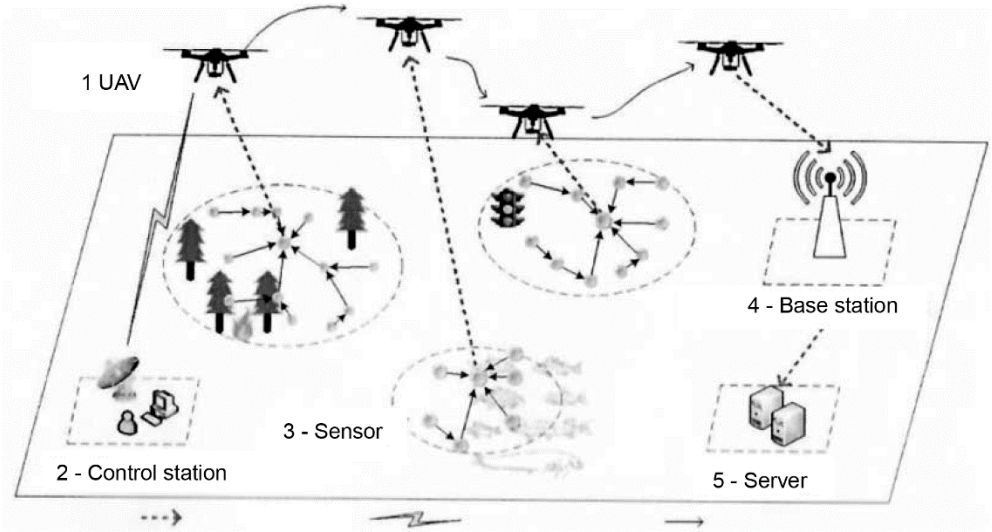


Figure 1. Model representation of information by a group of UAVs from ground sensors and the transmission of information to the base center [4]

As noted in [4], the system uses a LoS (line-of-sight) communication channel. The probability of successful data transmission over such a communication line is calculated using the formula

$$\mathrm{P}_{\mathrm{LOS}}\left(S_{m,U}\right)=\frac{1}{1+a\exp\left[-b\left(A\left(S_{m,U}\right)-a\right)\right]} \quad (1)$$

where $A\left(S_{m,U}\right)$ is the angle between the sensors S_m and m, $m \in M$, α and b are environmental parameters that primarily depend on the density of buildings in the area, as well as the height of the buildings.

The data transfer rate from the UAV sensor S_m is determined as [18]

$$\mathrm{R}\left(S_m, U\right) = B \cdot \log_2\left(\frac{1+\left|h\left|S_{m,U}\right)\right|^2 P_m}{N_0}\right) \quad (2)$$

where B is the channel bandwidth;
$h(S_m,U)$ is the channel gain between the UAV and the sensor;
P_m is the power of the transmitted signal from the sensor to the UAV;
N_0 is the additive Gaussian noise power.
The objective of this study is to analyze the possibility of increasing R by optimizing the UAV operating mode.

Materials and methods

Let us assume that the data collection and transmission system shown in Figure 1 is clustered and brought into the form shown in Figure 2.

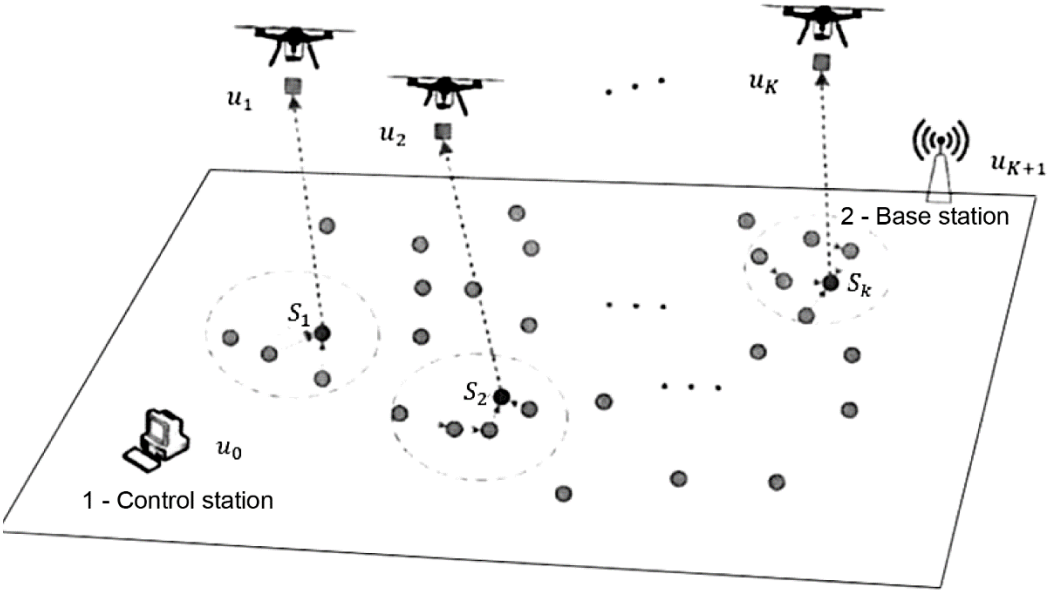


Figure 2. A system for collecting and transmitting data from clustered sensors using UAVs [4]

Let's assume that the communication channel of the i-th UAV contains white noise with intensity N_{0i}. Moreover, $i = \overline{1,n}$.

Let's adopt the following model N_{0i}

$$N_{0i} = N_{0i-1} + \Delta N_0$$

Where $\Delta N_0 = const$

$$N_{0,0} = 0. \tag{3}$$

Note that condition (3) implies the existence of an ordered set.

$$N_0 = \{N_{0i}\} \tag{4}$$

We also adopt the following model of the multiplier *B*

$B_j = B_{j-1} + \Delta B$ where $\Delta B = const$

at $B_0 = 0$; $j = \overline{1,n}$.

The existence of an ordered set is also assumed.

$$B = \{B_j\} \tag{5}$$

Next, we introduce the following possible connection function for consideration.

$$N_i = \varphi(B_j) \tag{6}$$

Taking into account (2), (5), and (6), we construct the following discrete sum.

$$\mathrm{R}_\Sigma = \sum_{j=1}^{n} B_j \cdot \log_2 \left(\frac{1 + \left| h(S_{m,U}) \right|^2 \cdot P_m}{\varphi(B_j)} \right) \tag{7}$$

We write the discrete functional (7) in a conventional analog form.

$$\mathrm{R}_\Sigma = \int_0^{B_{\max}} B \cdot \log_2 \left[\frac{1 + \left| h(S_{m,U}) \right|^2 \cdot P_m}{\varphi(B)} \right] dB \tag{8}$$

To find the optimal form the function $\varphi(B)$, we impose the following constraint on this function.

$$\int_0^{B_{\max}} \varphi(B) dB = C; \quad C = const \tag{9}$$

Taking into account expressions (8) and (9), we construct the objective optimization functional *F*.

$$F = \int_0^{B_{\max}} B \cdot \log_2 \left[\frac{1 + \left| h(S_{m,U}) \right|^2 \cdot P_m}{\varphi(B)} \right] dB + \lambda \left[+ \int_1^{B_{\max}} \varphi(B) dB - C \right] \tag{10}$$

where λ is the Lagrange multiplier.

The solution to optimization problem (10) according to the Euler-Lagrange method satisfies the condition

$$\frac{d\left\{B\cdot\log_2\left[\frac{1+\left|h\left(S_{m,U}\right)\right|^2\cdot P_m}{\varphi(B)}\right]dB+\lambda\cdot\varphi(B)\right\}}{d\varphi(B)}=0 \tag{11}$$

From condition (11), we obtain

$$-\frac{B}{\varphi(B)}+\lambda=0 \tag{12}$$

From expression (12), we find

$$\varphi(B)=\frac{B}{\lambda} \tag{13}$$

Let's calculate the Lagrange multiplier. To do this, using expressions (9) and (13), we obtain

$$\int_0^{B_{\max}}\frac{B}{\lambda}dB=C \tag{14}$$

From expression (14), we find

$$\lambda=\frac{B_{\max}^2}{2C} \tag{15}$$

Taking into account expressions (13) and (15), we obtain

$$\varphi(B)=\frac{2BC}{B_{\max}^2} \tag{16}$$

We will show that when solving (13), R_Σ reaches a maximum, i.e., the data transmission rate from the sensors to the UAV reaches a maximum. To do this, according to the Lagrange criterion, it is sufficient to calculate the second derivative of the integrand in (14) and verify that it is always negative.

Discussion

Thus, the problem of optimizing data collection from clustered ground sensors using a UAV swarm has been formulated and solved. An assumption has been made regarding the existence of a dependence between the intensity of Gaussian white noise in the UAV receiving channel and the bandwidth of the same channel. An integral constraint is applied to this dependence, significantly limiting the choice of the optimal function from the space of continuous and twice-differentiable functions.

An objective functional for optimizing the data collection system has been constructed. Application of the unconstrained variational optimization method and Euler's method to solve the optimization problem enabled the optimal form of the desired function to be obtained, for which the selected objective functional reaches its maximum.

Conclusion

The optimization of data collection using UAVs from clustered ground-based sensors is considered. It is shown that the data collection rate can be maximized when there is a direct linear relationship between the UAV data reception channel bandwidth and the intensity of white Gaussian noise in the receiving channel.

REFERENCES

[1] H. Ahmed, N. Nasir, “Drone patrolling applications, challenges and its future: a review,” Vol. XX. 2017.

[2] X. Chen, B. Hopkins, H. Wang, L. Oneill, F. Afghah, A. Razi, P. Fule, “Wildland fire detection and monitoring using a drone-collected RGB/IR image dataset,” *IEEE Access*. Vol. 10. 2022.

[3] Ehret and Michael, “The zero marginal cost society: The internet of things, the collaborative commons, and the eclipse of capitalism,” *The Journal of Sustainable Mobility*, vol. 2, no. 2, pp. 67-70, 2015.

[4] Z. Wei, M. Zhu, N. Zhang, L. Wang, Y. Zou, Z. Meng, Z. Feng, “UAV assisted data collection for internet of things: A survey,” Nov. 2022.

[5] P. Tong, J. Liu, X. Wang, B. Bai, and H. Dai, “UAV-enabled age-optimal data collection in wireless sensor networks,” *IEEE International Conference on Communications Workshops (ICC Workshops)*, pp. 1-6, 2019.

[6] J. Zong, C. Shen, J. Cheng, J. Gong, T.-H. Chang, L. Chen, and B. Ai, “Flight time minimization via UAVS trajectory design for ground sensor data collection,”*16th International Symposium on Wireless Communication Systems (ISWCS)*, pp. 255-259, 2019.

[7] Z. Wei, X. Liu, C. Han, and Z. Feng, “Neighbor discovery for unmanned aerial vehicle networks,” *IEEE Access*, vol. 6, pp. 68 288-68 301, 2018.

[8] S. Poudel and S. Moh, “Medium access control protocols for unmanned aerial vehicle-aided wireless sensor networks: A survey,” *IEEE Access*, vol. 7, pp. 65 728-65 744, 2019.

[9] J. Baek, S. I. Han, and Y. Han, “Optimal UAV route in wireless charging sensor networks,” *IEEE Internet of Things Journal*, vol. 7, no. 2, pp. 1327-1335, 2020.

[10] C. M. de A. Lima, E. A. da Silva, and P. B. Velloso, “Performance evaluation of 802.11 IoT devices for data collection in the forest with drones,” *IEEE Global Communications Conference (GLOBECOM)*, pp. 1-7,2018.

[11] Z. Wei, H. Wu, S. Huang, and Z. Feng, “Scaling laws of 21unmanned aerial vehicle network with mobility pattern information,” *IEEE Communications Letters*, vol. 21, no. 6, pp. 1389-1392, 2017.

[12] J. Grigulo and L. B. Becker, “Experimenting sensor nodes localization in WSN with UAV acting as mobile agent,” *IEEE 23rd International Conference on E-merging Technologies and Factory Automation (ETFA)*, vol. 1, pp. 808-815, 2018.

[13] A. Filippone, “Flight performance of fixed and rotary wing aircraft,” CA, 2006.

[14] J. Wang, C. Jiang, Z. Wei, C. Pan, H. Zhang, and Y. Ren, “Joint UAV hovering altitude and power control for space-air-ground IoT networks,” *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1741-1753, 2019.

[15] M. B. Ghorbel, D. Rodrguez-Duarte, H. Ghazzai, M. J.Hossain, and H. Menouar, “Joint position and travelpath optimization for energy efficient wireless datagathering using unmanned aerial vehicles,” *IEEE Transactions on Vehicular Technology*, vol. 68, no. 3, pp. 2165-2175, 2019.

[16] C. Zhan and Y. Zeng, “Completion time minimization for multi-UAV-enabled data collection,” *IEEE Transactions on Wireless Communications*, vol. 18, no. 10, pp.4859-4872, 2019.

SYNCHROINFO JOURNAL

www.media-publisher.eu/synchroinfo-journal

PROBABILISTIC CHARACTERISTICS OF ACCELERATED SEARCH SPREAD SPECTRUM SIGNALS

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 reasons for limiting the duration of a spread spectrum signal processed in a digital device for its accelerated search are considered, which are associated both with the instability of the frequencies of clock generators on the receiving and transmitting sides in the absence of preliminary clock synchronization, and with the conditional complexity and response speed of this device. A technique has been developed for analyzing the probabilistic characteristics of an accelerated search (detection) of a signal, which makes it possible to relate the allowable duration of its processing time and the signal-to-noise ratio at the receiver input.

DOI: 10.36724/2664-066X-2025-11-3-13-21

Received: 28.05.2025
Accepted: 22.07.2025

KEYWORDS: *spread spectrum signals, synchronization parameters, frequency and delay uncertainty regions, search, accelerated search, probabilistic characteristics of detection*

Citation: Vu Sy Dao, Svetlana F. Gorgadze, "Probabilistic characteristics of accelerated search spread spectrum signals", *Synchroinfo Journal* **2025**, vol. 11, no. 3, pp. 13-21.

Introduction

Binary noise-like complex signals (NLCs), generated from binary pseudorandom sequences (PRS), are currently widely used in various digital communication systems, including satellite radio navigation systems [1, 2]. Synchronization problems are typically solved using special periodically repeating pilot signals emitted directly at the carrier frequency or at one of its quadrature components.

The main problem is the precise synchronization of NLCs in time, and less often in frequency. However, a necessary condition for the successful operation of the radio system is synchronization by the pilot signal repetition period and the clock frequency of the pseudorandom code in order to generate a reference signal at the receiving end of the NLC, synchronous in time with the received signal. This problem can be solved using a multi-stage signal search procedure, the first stage of which is performed in a special accelerated search device, where rough synchronization of the received NLC is carried out, primarily in time [3, 4].

The signal search device is a device for its combined detection and time delay parameter estimation. Therefore, the primary performance indicator is the probability of correctly detecting a signal with a certain time delay relative to a signal with a conditionally zero delay, given the false alarm probability [7, 8].

The aim of this research is to develop a method for analyzing the probabilistic characteristics of noise-like signal detection in an accelerated signal search device, taking into account the limitations on signal processing time associated with the lack of clock synchronization.

Finding sync settings

The search involves detecting a signal and measuring its parameters, typically frequency and delay time, with an accuracy corresponding to the cross-sectional dimensions of the main peak of the signal's uncertainty function (UF) [5-8]. That is, two adjacent values of any parameter can be considered indistinguishable if the difference between them is less than the cross-sectional width of the UF's central peak.

As a result, any of the synchronization parameters under consideration can be considered discrete, with the signal delay τ varying from 0 to the signal duration (repetition period), of the signal T, and ΔT from 0 to F, where is the width of the uncertainty region in frequency.

If we assume that $\Delta\tau$ and Δf_i are, respectively, the width of the interval of the delay time and frequency uncertainty region within which the values of any parameter are indistinguishable from the point of view of its evaluation, then the number of discrete values of the parameter τ is determined as $n_v = T/\Delta\tau$, and the number of values Δf of the parameter is determined as $n_{ch} = F/\Delta f_i$. But in reality, when sampling the processed signal, the values $\Delta\tau$ and Δf_i must be selected in accordance with Kotelnikov's theorem. That is, in this case, when selecting the signal sampling intervals in time and frequency in accordance with the size of the main peak of the functional class, they will be twice the signal sampling interval recommended by this theorem. Then, if the signal spectrum width is equal to ΔF_s, then $\Delta\tau \approx 1/\Delta F_s$, and $\Delta f_i \approx 1/T$.

Considering that in the case of the pseudorandom code $\Delta F_s \approx N/T$, we obtain that the total number of unknown parameters is $n_{\text{v,ch}}(\text{NLC}) = n_v n_{ch} = FT\Delta F_s T = FTN$, where N is the length (period) of the pseudorandom code [9].

Figure 1 shows a time-frequency plane in which the uncertainty regions of the pseudorandom code synchronization parameters – delay time and frequency – are bounded by a rectangle.

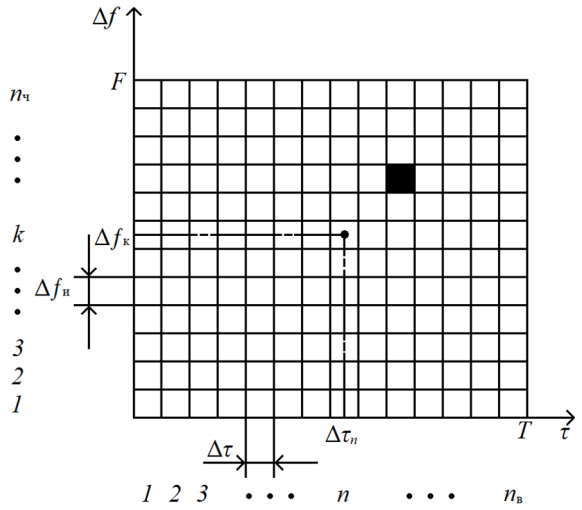


Figure 1. The uncertainty region of synchronization parameters

The parameter uncertainty region is divided by a grid into rectangular cells with sides of $\Delta\tau$ and Δf_i. The total number of cells is $n_{v,ch}$. The area of each cell is approximately equal to the area of the central peak of the FN; that is, each cell can accommodate only one of its central peaks. Therefore, the grid defines the boundaries between recognizable parameter values, and the parameters themselves correspond to the centers of the uncertainty intervals and can take any value from their total number of n_v and n_{ch}.

Thus, the discrete values of the synchronization parameters can be numbered and designated as τ_n, $n=1,\ldots,n_v$ and $\triangle f_k$, $k=1,\ldots,n_{ch}$.

In Figure 1, the shaded cell corresponding to the received NLS is highlighted. This is the cell that must be found during the search, after which its center must be found. However, the latter is no longer relevant to the search task.

The construction of an estimator can be based on the use of τ and Δf a set of correlators (Cor), whose reference signals are copies of the signal with discrete values of the synchronization parameters, i.e., taking into account the recommendation of Kotelnikov's theorem, $\mathrm{Re}[\dot{S}(t-\tau_n)\exp(j(2\pi(f_0+\triangle f_k)t+\phi))]$, $n=1,\ldots,2n_v$, $k=1,\ldots,2n_{ch}$, $\dot{S}(t)$, is the complex envelope of the received signal. The total number of correlators should be $4n_v n_{ch}$.

The block diagram of a device implementing the maximum likelihood estimate of the signal frequency and delay time, consisting of a set of correlators, is shown in Figure 2. The output signal of the correlators, after calculating the absolute values of their responses, will be the absolute value of the periodic autocorrelation function (PACF) $|\dot{\chi}(\tau,\triangle f)|$ (accurate to a factor corresponding to the signal energy and the additive noise component), whose values for discrete values τ_n and $\triangle f_k$ will appear simultaneously at the correlators' output. A decision unit (DU), which is a maximum selector, is then used. In the latter, the values of the correlator responses are compared and the maximum one is selected. The parameters of the reference signal of the correlator with the largest output response are given as the maximum plausible estimate of the frequency and delay time of the signal.

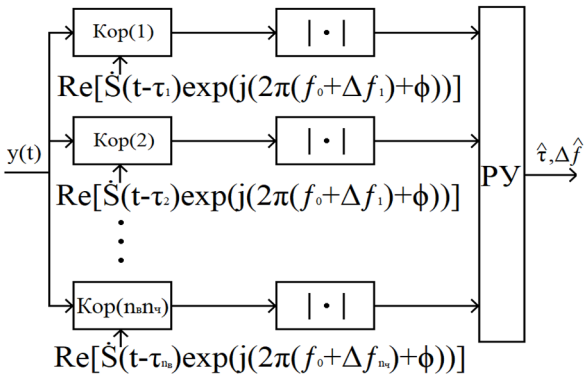


Figure 2. Device for maximum likelihood estimation of frequency and delay time based on a set of correlators

If the signal frequency is known and equal to $f_0(\triangle f = 0)$, the circuit in Figure 2 uses only $2n_v$ correlators to estimate the signal's time delay, but all of them can be replaced by a single matched filter (MF).

The latter is a linear device with an impulse response that is a mirror image of the useful signal, i.e., $h(t) = s(T-t)$, where *T* is the signal duration. The MF maximizes the output signal-to-noise ratio when exposed to additive white Gaussian noise, but in this context, its ability to reproduce the signal's autocorrelation function in real time is important. Indeed, the MF response is:

$$r(t) = \int_{-\infty}^{\infty} y(x)h(t-x)dx = \int_{-\infty}^{\infty} y(x)s(T-t+x)dx = \frac{1}{2}\mathrm{Re}[\int_0^T \dot{y}(x)\dot{s}(T-t+x)dx] =$$
$$= \mathrm{Re}[\{\frac{1}{2}\int_0^T \dot{Y}(x)\dot{S}(T-t+x)dx \cdot \exp(-j2\pi f_0 T)\} \cdot \exp(j2\pi f_0 t)] \cdot \quad (1)$$

As can be seen, the curly brackets in the last formula represent the complex envelope of the signal at the MF output, and:

$$|\frac{1}{2}\int_0^T \dot{Y}(x)\dot{S}(T-t+x)dx| = \frac{1}{2}|\dot{\chi}(t-T,0) + \xi_n|, \quad (2)$$

where ξ_n is the additive interference component at the MF output.

However, it is important to note that (1) assumed that the AF was matched to the input signal with an accuracy of up to the initial phase shift of its high-frequency carrier.

Thus, the AF's real-time response replicates the real part of the input signal's autocorrelation function with a factor of ½, shifted in time by the signal duration *T*.

This circumstance allows the device, to be used for the most realistic estimate of the signal's time delay.

The input signal *y*(*t*) is first processed in the SF, from whose output the signal is fed to the envelope detector (ED). In the final block, which is the decision unit (DU), the instant in time t_m when the signal at the ED output reaches its maximum value is recorded, with the estimated signal delay being equal to $\hat{\tau} = t_m - T$. The values $|\mathrm{Re}\{\dot{\chi}(t-T,0)\}|$ at the DU input appear sequentially.

In practice, a signal processor (SP) is typically a digital device whose input extracts the complex envelope of the received signal (for a signal processor generated based on a binary sequence reference sequence, this is a real function), after which it is sampled in time at a clock frequency of $f_c \approx 1/2\Delta\tau$.

Two samples are taken over the duration $T_e = T / N$ of an elementary pulse of the SP, shifted relative to each other in time by $T_e/2$. These two groups of signal samples, each taken at time intervals of duration T_e, must be processed separately – each in its own device, and a signal detection decision must be made upon its detection in either device. We will refer to them as SP1 and SP2.

It should be noted that the doubled signal sampling frequency does not exactly correspond to the clock frequency of the received signal, theoretically equal to $2f_T$, due to the instabilities of the master oscillators on both the transmitting and receiving sides. Furthermore, at the search stage, the received signal is not yet clocked. As a result, after a certain period of time, a slip will inevitably occur; that is, two SLC samples, when sampled over a time interval T_e, will fall on the same elementary pulse, or one such pulse will be missed.

Due to the shift in SLC samples at the inputs of SF1 and SF2 on T_e, a slip will never occur simultaneously at the inputs of these devices. However, the SLC processing time in these devices should not exceed the time between two consecutive slips, which can be easily estimated given the instability of the master clock frequencies on the transmitting and receiving sides.

For example, if $\frac{\Delta f_T}{f_T} = 10^{-4}$, then it is easy to calculate that the duration of the pseudorandom code that can be processed in SF1 and SF2 should not exceed approximately 5000. Therefore, it is important to be able to evaluate the efficiency of SLC search depending on the length of the PRS processed in the corresponding device.

Efficiency of Accelerated Search for SLC

The problem of searching for SLC synchronization parameters, i.e., its joint detection and parameter estimation with an accuracy corresponding to the cross-sectional dimensions of the main FC peak, is reduced to the problem of recognizing $n_{\text{v,ch}} = n_v n_{ch}$ quasi-orthogonal signals.

Indeed, each pair of parameters $\triangle f_k$ and τ_n corresponds to a signal $s(t, \tau_n, \triangle f_k)$, $n = 1, \ldots, n_v$, $k = 1, \ldots, n_{ch}$ and the FC of all these signals have non-coincident central peaks. Their mutual FCs take small values corresponding to the FC side peaks. If we assume that the FC signal shape is approximately button-shaped and the statistical characteristics of its side peaks are known, then the problem of searching for synchronization parameters is reduced to the problem of recognizing $n_{\text{v,ch}}$ quasi-orthogonal signals [9-13]. In this case $n_{\text{v,ch}} = n_v = N$.

Furthermore, a variant with a conditionally coherent signal accumulation of SLC over the duration of several repetition periods from the output of each SF was considered. In this case, the SLC can be processed in the SF over the duration of the signal repetition period, and at the input of the RA, the PACF samples are summed in parallel. The signal detection characteristics were also studied in the case where the SF can only process a portion of the NLS period.

A distinctive feature of the developed method for studying the effectiveness of the search device is the ability to construct graphs taking into account the ratio of the noise power to the signal power at the receiver input $[\frac{P_n}{P_s}]_{in}$, as well as the length of the processed pseudorandom code.

Figure 3 shows graphs of the dependence of the probabilities of correct NLS detection P_d from $[\frac{P_n}{P_s}]_{in}$ on the false alarm probability $P_{fa} = 10^{-4} \text{and } 10^{-6}$.

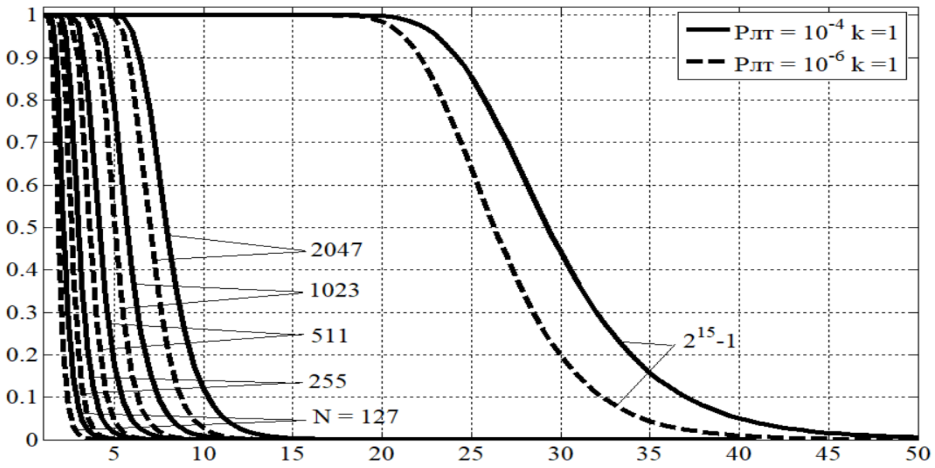


Figure 3. Dependencies on P_d from $[\frac{P_n}{P_s}]_{in}$ when forming a NLS based on MS and given $P_{fa} = 10^{-4}$ and 10^{-6} for $N = 127, 255, 511, 1023, 2047, 2^{15} - 1$

It was assumed that the signal was generated based on an M-sequence (MS) of length *N*, and the SF processes one (*k* = 1) full period of its repetition. Similar graphs, but for the case where the SF can process either a portion of the NLS period (*k* = 0.1, 0.3,…), where *k* is its portion, or a single period (*k* = 2,…, 10,…, 50) with conditionally coherent accumulation of several periods, are shown in Figures 4-9 when generating a NLS based on an MS, and in Figure 10 when generating a NLS based on a Gold code.

The developed technique allows for the analysis of the probability of error $[\frac{P_n}{P_s}]_{in}$ in the presence of several time-shifted copies of the same signal at the receiver input due to its multipath propagation.

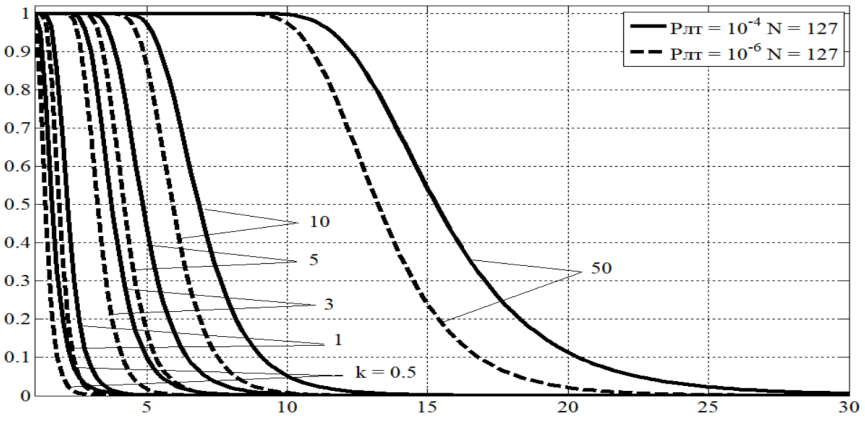


Figure 4. Dependencies on P_d from $[\frac{P_n}{P_s}]_{in}$ when forming the NLS based on MS for $N = 127$ when $k = 0.5, ..., 50$

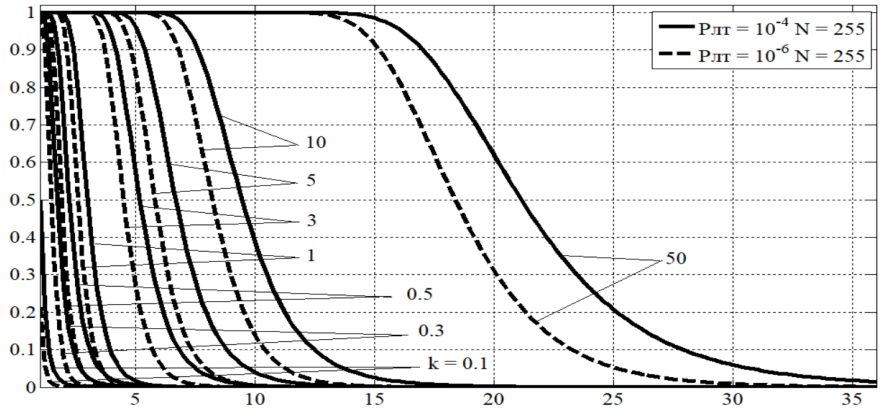


Figure 5. Dependencies on P_d from $[\frac{P_n}{P_s}]_{in}$ when forming the NLS based on MS for $N = 255$

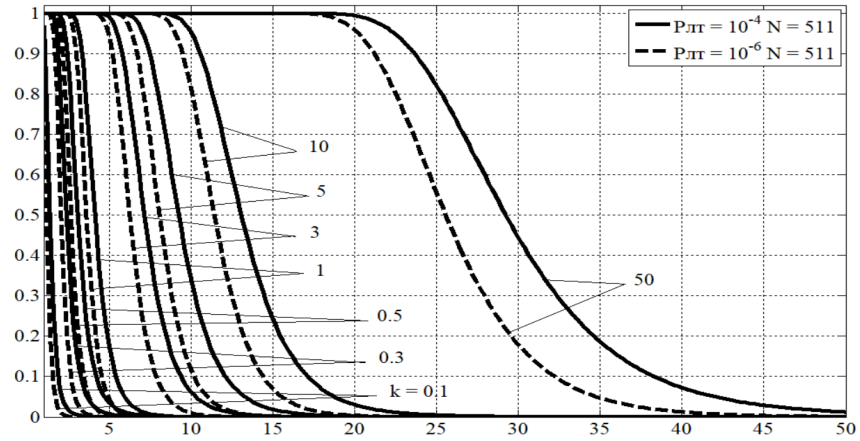


Figure 6. Dependencies on P_d from $[\frac{P_n}{P_s}]_{in}$ when forming the NLS based on MS for $N = 511$

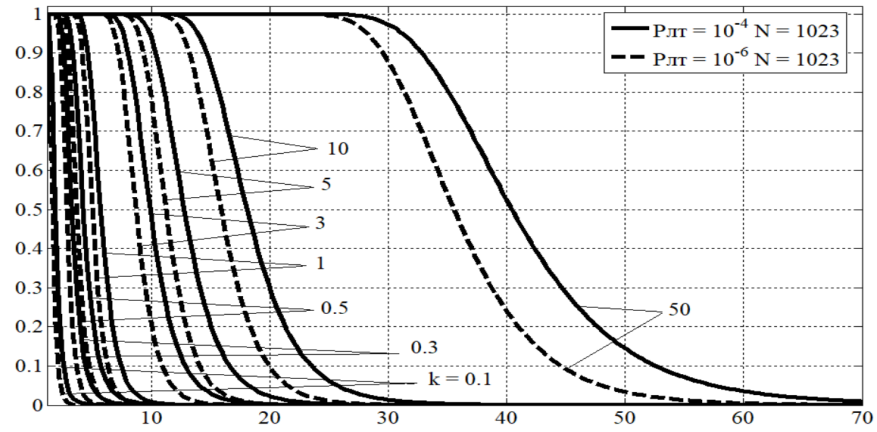


Figure 7. Dependencies on P_d from $[\frac{P_n}{P_s}]_{in}$ when forming the NLS based on MS for $N = 1023$

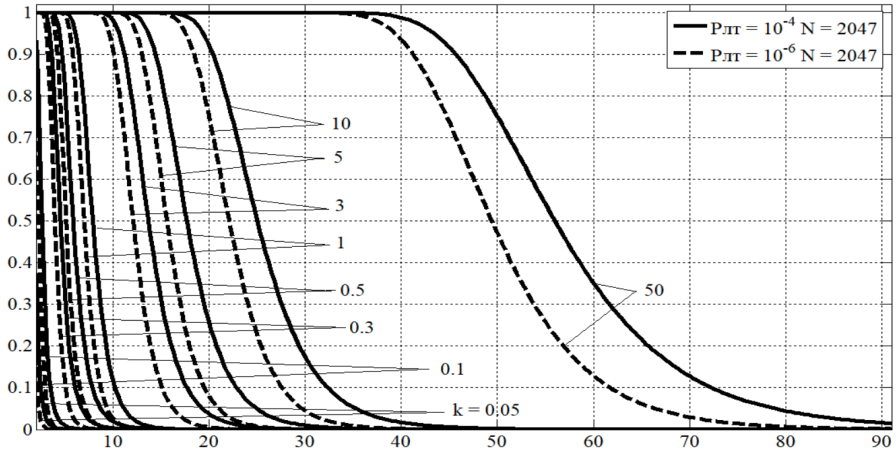


Figure 8. Dependencies on P_d from $[\frac{P_n}{P_s}]_{in}$ when forming the NLS based on MS for $N = 2047$

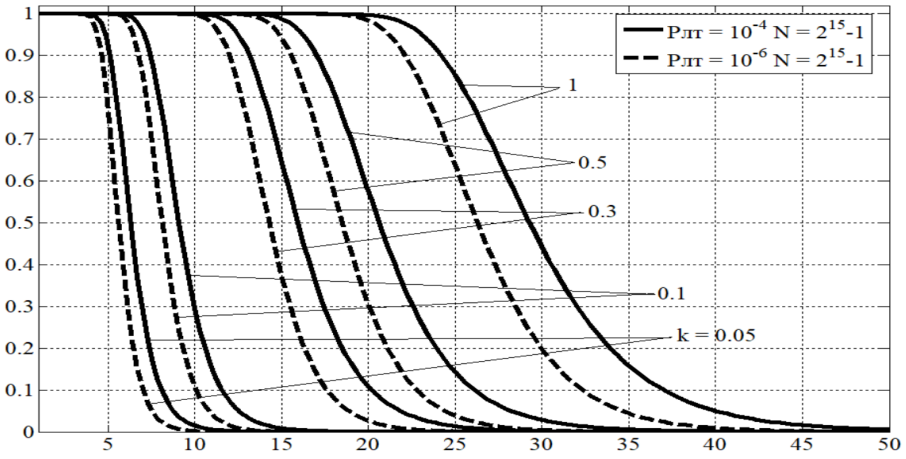


Figure 9. Dependencies on P_d from $[\frac{P_n}{P_s}]_{in}$ when forming the NLS based on MS for $N = 2^{15} - 1$

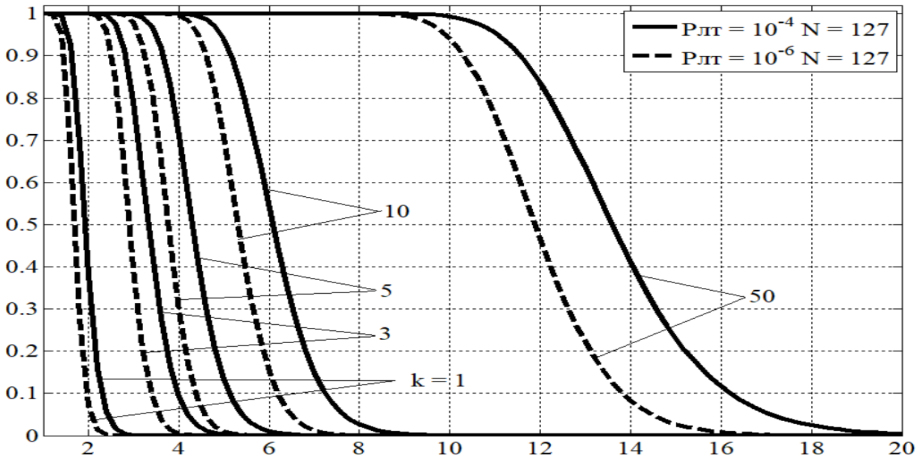


Figure 10. Dependencies on P_d from $[\frac{P_n}{P_s}]_{in}$ when forming the NLS based on the Gold code for *N* = 127

Conclusion

This article presents a developed methodology for analyzing the efficiency of a digital device for accelerated search for the time delay parameter of a complex noise-like signal, taking into account the limited processing time associated with the instability of the master clock generators on the transmitting and receiving sides.

Another factor that necessitates processing relatively short signal segments is the relative complexity of the search device and its speed. Consequently, the basic parameter for analyzing the efficiency of a noise-like signal search device is the duration of the pseudorandom code, which can be directly processed in a matched filter or correlator, as well as the permissible number of signal periods whose energy can accumulate conditionally coherently from the filter or correlator output.

Thus, the developed methodology for analyzing the efficiency of the search device allows one to evaluate its effectiveness given a priori information about the instability of the master clock generators and the noise-to-signal power ratio at the receiver input.

REFERENCES

[1] V.P. Ipatov, “Broadband systems and code division of signals,” Moscow: Mir Svyazi, 2007.

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

[3] Vu Sy Dao, S.F. Gorgadze, “A device for accelerated search of a noise-like signal,” *Information Society Technologies. Proceedings of the XVI International Industry Scientific and Technical Conference.* Moscow, 2022, pp. 88-90.

[4] S.F. Gorgadze, T.M. Gut, “Accelerated evaluation of spread spectrum signals synchronization parameters,” *2020 Systems of Signals Generating and Processing in the Field of on-Board Communications,* 2020. P. 9078627.

[5] 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.

[6] 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.

[7] 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.

[8] S.F. Gorgadze, A.S. Vovk, “Estimation of Parameters of a Noise-Like Signal on a Non-harmonic Subcarrier,” *Fundamental Problems of Radioelectronic Instrument-Making*. 2014. Vol. 14. No. 5, pp. 182-185.

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

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

[11] 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

[12] 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

[13] 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

AUTHENTICATION ALGORITHM FOR SMART POWER GRID 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

The paper describes an authentication algorithm structure and key stages of its application for smart power grid systems, its advantages over traditional solutions, and practical application scenarios. An authentication algorithm based on a combination of verifiable encryption and one-time keys, designed to ensure high cryptographic strength in demanding security environments. Particular attention is paid to adapting the algorithm to critical infrastructures such as energy grids, where delays and data compromise can lead to catastrophic consequences.

DOI: 10.36724/2664-066X-2025-11-3-22-28

Received: 12.06.2025
Accepted: 25.07.2025

KEYWORDS: *smart power; authentication; verifiable encryption; one-time keys; security; smart grid; energy systems*

Citation: V.A. Dokuchaev, I.A. Safonov, J. Rahmani, "Authentication algorithm for smart power grid systems", *Synchroinfo Journal* **2025**, vol. 11, no. 3, pp. 22-28.

Introduction

Modern authentication systems face numerous challenges related to increasing security and user experience requirements [1, 2]. Communication networks continue to evolve, and with the support of comprehensive long-term development programs, quality standards can be expected to improve [3-5]. These issues are particularly pressing in the context of critical infrastructures such as energy grids. Energy systems, the backbone of the economy and everyday life, are increasingly becoming targets for sophisticated cyberattacks capable of causing large-scale outages, financial losses, and threats to national security [6]. Protecting such systems requires not only resilience to external threats but also ensuring uninterrupted operation, which challenges developers to combine high security with minimal delays in authentication processes.

With the growing number of cyberattacks and the increasing sophistication of hacking methods, traditional approaches such as passwords and static keys are becoming increasingly less reliable. Passwords are often vulnerable to phishing, brute-force attacks, and data leaks, while static keys, while providing a higher level of security, are vulnerable to compromise over long periods of use—especially in systems where regularly changing keys is difficult, as is the case with distributed power grid nodes. These issues are driving the search for new solutions that can provide both a high level of security and the operational efficiency critical to energy facilities.

One of the most promising areas in this area is the use of one-time keys in combination with verifiable encryption. One-time keys, generated dynamically for each session or transaction, minimize the risks associated with their interception or reuse by attackers, which is especially relevant for power grids with their vast number of devices. However, one-time keys alone do not solve all problems, such as verifying the integrity of authentication processes in real time. Verifiable encryption comes to the rescue, ensuring that all authentication stages are completed correctly without malicious intervention, which is critical for preventing man-in-the-middle attacks in power facility control systems [7, 8].

The purpose of this article is to present an authentication algorithm based on these technologies and demonstrate its advantages in the context of protecting energy infrastructures. The proposed solution is aimed not only at increasing cryptographic strength but also at optimizing computing resources, making it applicable even in power system networks with limited network bandwidth.

The concept of verifiable encryption

Verifiable encryption is a cryptographic method that encrypts a message in such a way that a verifier can verify that certain conditions for the encrypted data are met without decrypting it. This approach is based on the use of zero-knowledge proofs and cryptographic protocols that guarantee data integrity.

One of the key properties of verifiable encryption is transparency. This means that an encrypted message can be verified against specified parameters without having to disclose it. For example, it can be verified that a message was signed by a specific user or contains certain attributes while remaining encrypted.

Preserving confidentiality is also an important aspect. The message content remains protected, which is achieved through the use of strong cryptographic algorithms such as RSA, elliptic curve algorithms, or homomorphic encryption [9]. Data integrity is ensured by digital signature mechanisms or hash functions.

One-time keys, as their name suggests, are used only for a single operation or session. One-time keys minimize the risks associated with compromise, as even if leaked, the key cannot be reused. These keys are generated for each client-server interaction and are then destroyed.

One-time keys play an important role in preventing replay attacks, in which an attacker intercepts data and attempts to reuse it [10]. The temporary nature of the keys and their uniqueness make these attacks ineffective. Using one-time keys also reduces the risk of leaking long-term keys, as compromising one temporary key does not reveal information about other sessions.

Using verifiable encryption with one-time keys offers a number of advantages. First and foremost, it offers a high level of security. One-time keys eliminate the possibility of reusing compromised data, and verifiable encryption guarantees the confidentiality of the information. The algorithm's flexibility allows it to be adapted to various tasks and conditions. Verification parameters can be configured to meet the requirements of a

specific system or organization. Another important aspect is user convenience, as the method can be integrated with other authentication methods, including biometric technologies and token devices [11]. A comparison with other authentication methods is presented in Table 1.

Table 1

Comparison with other authentication methods

Method	Security level	Usability	Resilience to attacks
Passwords	Low [12]	Medium (requires memorization)	Low (vulnerable to phishing, brute force, and dictionary attacks) [13]
Multi-factor authentication (MFA)	High (combination of factors) [14]	Low (requires additional devices/actions)	High (complicates attacks, but vulnerable to SIM-swap) [15]
Magic Link	Average (depending on the security of the delivery channel) [16]	High (no password required)	Medium (vulnerable to email/SMS interception)
Verifiable encryption	Very high (one-time keys + cryptography) [17]	High (automatic key generation)	Very high (non-reuse by design, protection against MITM) [18]

Authentication algorithm based on verifiable encryption using one-time keys

Authentication algorithm based on verifiable encryption using one-time keys The complexity of attacks aimed at compromising user data is growing, requiring developers to create innovative approaches to ensure the confidentiality and integrity of information. Algorithms based on a combination of verifiable encryption and one-time keys represent one of the most promising technologies. One of the algorithms is presented below:

Registration:

The user sends their digital identity p_1 to the device.

The device generates two keys:

Primary key k_1 for encryption.

Auxiliary key k_2 for hashing.

The device calculates the hash of p_1 using GOST 34.11-20181: $h_2 = H(p_2)$.

The device encrypts the hash h_1 using the key k_1 and the block cipher:

$$c_1 = E_{k_1}(h_1) = h_1 \oplus k_1.$$

The device calculates the hash from the key k_2 and adds it to the encrypted hash h_1:

$$c_1^{'} = c_1 \oplus H(k_2).$$

The device sends $c_1^{'}$ to the server, which stores it in the database.

Verification:

The user sends their digital identity p_1 to the device.

The device generates two one-time keys:

Primary key $k_1^{'}$ for encryption.

Secondary key $k_2^{'}$ for hashing.

The device calculates the hash of p_2 using GOST 34.11-2018:

$$h_2 = H(p_2).$$

The device encrypts the hash h_2 using key $k_1^{'}$ and the block cipher:

$$c_2 = E_{k_1^{'}}(h_2) = h_2 \oplus k_1^{'}.$$

The device calculates the hash of key $k_2^{'}$ and adds it to the encrypted hash h_2:

$$c_2^{'} = c_2 \oplus H(k_2^{'}).$$

The device sends $c_2^{'}$ to the server.

The server calculates the encrypted distance between $c_1^{'}$ and $c_2^{'}$ using function *F*:

$$F(c_1^{'}, c_2^{'}) = c_1^{'} \oplus c_2^{'} = c_d.$$

The server sends the encrypted distance c_d back to the device.

The device decrypts c_d using keys k_1, $k_1^{'}$, k_2 and $k_2^{'}$:

$$D_{k_1,k_1^{'},k_2,k_2^{'}}(c_d) = (c_1 \oplus H(k_2)) \oplus (c_2 \oplus H(k_2^{'})) \oplus (k_1 \oplus k_1^{'}) =$$
$$= (h_1 \oplus H(k_2)) \oplus (h_2 \oplus H(k_2^{'})) \oplus (k_1 \oplus k_1^{'}).$$

The device calculates the final value:

$$h_1 \oplus h_2 = D_{k_1,k_1^{'},k_2,k_2^{'}}(c_d) \oplus H(k_2) \oplus H(k_2^{'}).$$

The device compares $h_1 \oplus h_2$ with the threshold value *s*. If $h_1 \oplus h_2 \le s$, the device returns "OK", otherwise "NG".

Authentication algorithm based on verifiable encryption using one-time keys

In the era of digital transformation, smart technologies are increasingly being implemented in various industries [19]. In recent years, the development of grid technologies has received a strong boost during the pandemic, affecting virtually all industries, including industrial and manufacturing sectors [20]. The energy sector is a critical element of the infrastructure of any country. The operational efficiency of an energy company depends largely on the reliability of corporate information and communication systems and networks. However, these systems also create new data security risks [21].

Modern energy systems, such as smart grids and power generation networks, require a high level of security and reliability [22]. These systems integrate complex infrastructure, including control centers, generators, distribution nodes, smart meters, sensors, and control devices. Interaction between these elements occurs through digital communication channels, which creates risks of cyberattacks, ranging from data interception to command spoofing [23]. The implementation of Smart Grid technology in the electric power industry increases economic efficiency, its use significantly reduces the costs of production, distribution and consumption of electricity [24].

To protect such systems, an authentication algorithm based on verifiable encryption with one-time keys is proposed, ensuring the integrity and confidentiality of critical information [25]. Such tools help mitigate emerging risks in the information and communication systems of energy generating companies
[26, 27].

Power systems are based on data transmission networks controlled by SCADA (Supervisory Control and Data Acquisition) systems. These systems are responsible for collecting information, remotely controlling equipment, and monitoring parameters in real time [28]. Smart Grid SCADA controls smart meters, transformers, and circuit breakers, and in large energy companies, it regulates generator operating modes, balances loads, and monitors the status of power lines [29]. Data is transmitted between field devices such as RTUs (Remote Terminal Units) and PLCs (Programmable Logic Controllers), servers, and dispatch interfaces via wired and wireless channels.

However, many communication protocols, including Modbus and DNP3, are not designed to protect against modern cyberthreats, making them vulnerable to attack. The implementation of verifiable encryption is particularly relevant for IEC-61850, which is used in digital substations, and IEEE C37.118, where data integrity is critical for real-time network management [30, 31].

The proposed method is adapted not only for classic SCADA systems but also for new architectures, including distributed substations, where the method protects control commands during high-voltage line switching; hybrid microgrids (Microgrids), ensuring data authentication between solar farms, wind turbines, and energy storage systems in standalone mode; and automatic load shedding (ALS) systems, verifying the authenticity of load balancing commands during power grid failures [32]. For decentralized networks with intermittent connections to the control center, such as remote wind farms, the algorithm implements local verification via pre-established keychains, minimizing dependence on centralized infrastructure and maintaining security even under limited connectivity.

The main problem with such systems is the lack of guarantees of the authenticity of transmitted commands. An attacker can infiltrate the communication channel, spoof parameters, or resend an intercepted command, causing equipment to malfunction. This can lead to accidents, consumer outages, or infrastructure damage. Traditional encryption methods are not always effective: long sessions with persistent keys facilitate replay attacks, and the lack of verification mechanisms allows data manipulation [33].

Each command, such as "disable overloaded section" or "adjust generator frequency," is encrypted with a unique key that is destroyed after use. This eliminates the possibility of reusing intercepted data. Verifiable encryption simultaneously ensures that the command has not been altered during transmission: any attempt to tamper with it results in automatic message rejection. When sending an instruction to shut down a transformer, the system generates a one-time key, encrypts the command, and transmits it to the recipient. Even if the communication channel is compromised, an attacker will be unable to inject false instructions or reproduce previously sent data.

With the growing number of IoT devices, the issue of compatibility with resource-intensive algorithms arises. The proposed method is optimized for low-power processors. Key generation requires less than 5% of the computing power of a typical protection and automation device [34]. The authentication latency does not exceed 2 ms, which meets the requirements of GOST R IEC 61850-5-2011222 for critical commands. To minimize the load, messages are grouped with a single verification key.

Special attention is paid to the protection of emergency notification systems. Messages about overloads, power line failures, or abnormal voltage surges require instant delivery and absolute reliability. The algorithm ensures their integrity through verifiable encryption, and one-time keys prevent blocking or delays of notifications. Upon detecting generator overheating, the system generates a key, encrypts the message, and sends it to the control center. The recipient verifies the authenticity of the data and the validity of the key, eliminating false alarms or the concealment of an emergency.

Thus, the authentication algorithm based on verifiable encryption with one-time keys offers a universal solution for power systems. It protects control commands, monitoring data, and emergency messages, minimizing the risk of cyberattacks. Implementing this approach increases the resilience of Smart Grids and power networks, ensuring the security of critical infrastructure in the face of growing digital threats.

Conclusion

The proposed authentication algorithm, based on verifiable encryption and one-time keys, represents a significant advance in security and usability for modern systems. In an era of increasingly sophisticated cyberthreats and ever-increasing data protection requirements, this approach offers a reliable solution capable of minimizing the risks associated with information leaks and key compromise.

An important aspect of the proposed algorithm is its versatility. Its adaptability to various application areas, including financial services, corporate networks, government platforms, and even the Internet of Things (IoT), opens up new possibilities. In each of these areas, the algorithm is capable of providing a high level of security while maintaining simplicity and user convenience. This is especially important in an environment where users increasingly prefer systems that are not only secure but also intuitive to use. However, despite all its advantages, the algorithm requires further development and optimization.

One area for future research could be improving its performance, especially when working with large data volumes or in systems with high loads. Furthermore, it is important to explore the possibilities of integrating the algorithm with other technologies.

REFERENCES

[1] S. V. Pavlov, E. V. Leonovich, V. V. Maklachkova, V. A. Dokuchaev, “Networks 2030: prospects and challenges,” *REDS: Telecommunications Devices and Systems*, 2022, vol. 12, no. 2, pp. 17-23.

[2] V. A. Dokuchaev, S. S. Mytenkov, D. D. Rakhmani, I. A. Safonov, “Analysis of vulnerabilities and risks of traditional password systems in the context of corporate distributed systems and critical infrastructures,” *Economics and quality of communication systems*. 2025. No. 2 (36), pp. 135-147.

[3] R. Jahed, “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.

[4] V. A. Dokuchaev, “Digital twins: new opportunities, new risks,” *Innovations for building a digital future: Proceedings of the XXIX International Forum IAS' 2025*, Moscow, April 25, 2025. Moscow: State University of Education, 2025, pp. 82-89.

[5] V. A. Dokuchaev, Yu. I. Vedeneeva, “Security and trust in digital twin technologies,” *Theory and practice of economics and entrepreneurship: Proceedings of the XXII International scientific and practical conference*, Simferopol – Gurzuf, April 24-26, 2025. Simferopol: IP Zueva TV, 2025, pp. 269-271.

[6] V. A. Dokuchaev, “Artificial Intelligence and Energy: New Drivers, New Risks,” *Trends in the Development of the Internet and Digital Economy: Proceedings of the VIII International Scientific and Practical Conference*, Simferopol-Alushta, May 29-31, 2025. Simferopol: IP Zueva T.V., 2025, pp. 16-17.

[7] R. L. Rivest, A. Shamir, L. Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,” *Communications of the ACM*, 1978, vol. 21, no. 2, pp. 120-126.

[8] S. Goldwasser, S. Micali, “Probabilistic Encryption,” *Journal of Computer and System Sciences*, 1984, vol. 28, no. 2, pp. 270-299.

[9] A. J. Menezes, P. C. van Oorschot, S. A. Vanstone, “Handbook of Applied Cryptography,” Boca Raton: CRC Press, 1996, p. 816.

[10] D. Boneh, M. Franklin, “Identity-Based Encryption from the Weil Pairing,” *Advances in Cryptology – CRYPTO 2001*. Berlin: Springer, 2001, pp. 213-229.

[11] M. Kihara, S. Iriyama, “New Authentication Algorithm Based on Verifiable Encryption with Digital Identity,” *2019 International Conference on Information Security*, Tokyo, 2019, pp. 1-8.

[12] Verizon. Data Breach Investigations Report [Electronic resource]. Mode of access: https://www.verizon.com/business/resources/reports/dbir (Date of access: 20.10.2025)

[13] OWASP. Authentication Cheat Sheet [Electronic resource]. Mode of access: https://cheatsheetseries.owasp.org (Date of access: 20.10.2025).

[14] Google Security Blog [Electronic resource]. Mode of access: https://security.googleblog.com (Date of access: 20.10.2025).
[15] NIST. Special Publication 800-63B. Digital Identity Guidelines: Authentication and Lifecycle Management [Electronic resource]. Mode of access: https://doi.org/10.6028/NIST.SP.800-63b (Date of access: 20.10.2025).
[16] FIDO Alliance. Whitepaper [Electronic resource]. Mode of access: https://fidoalliance.org (Date of access: 20.10.2025).
[17] IETF. RFC 6238: Time-Based One-Time Password Algorithm [Electronic resource]. Mode of access: https://tools.ietf.org/html/rfc6238 (Date of access: 20.10.2025).
[18] Forrester Research. Zero-Trust Network Architecture [Electronic resource]. Mode of access: https://www.forrester.com (Date of access: 20.10.2025).
[19] 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: IEEE, 2020, p. 9261544. DOI: 10.1109/EMCTECH49634.2020.9261544.
[20] J. Rahmani, "Trends in the development of network technologies in 2022," *Information Society Technologies: Proceedings of the XVI International Industry Scientific and Technical Conference*, Moscow, March 2-3, 2022. Moscow: Media Publisher, 2022, pp. 30-31.
[21] V. A. Dokuchaev, "Typical structure of a corporate infocommunication system of an energy-producing company of the 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: KNRTU-KAI, 2019, pp. 298-299.
[22] NIST. Special Publication 1108R3. Framework for Improving Critical Infrastructure Cybersecurity. Gaithersburg: NIST, 2020.
[23] G. Liang, et al., "Cybersecurity for Power Grids: Challenges and Solutions," *IEEE Transactions on Smart Grid*, 2017, vol. 8, no. 5, pp. 2446-2455.
[24] M. S. Kozhanov, "Analysis of the economic efficiency of Smart Grid implementation in the electric power industry and its impact on electricity prices," *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: V. I. Vernadsky Crimean Federal University, 2023, pp. 318-322.
[25] M. Bellare, V. T. Hoang, P. Rogaway, "Foundations of garbled circuits," *CRYPTO 2013: Proceedings of the 33rd Annual Cryptology Conference*, Santa Barbara, 2013, pp. 784-807.
[26] 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.
[27] J. Rahmani, "The main approaches to evaluating the effectiveness of applying the risk analysis and management methodology at an energy company," *T-Comm*, 2022, vol. 16, no. 9, pp. 46-55. DOI: 10.36724/2072-8735-2022-16-9-46-55.
[28] IEEE. IEEE Std C37.1-2007. IEEE Standard for SCADA and Automation Systems. New York: IEEE, 2007.
[29] IEC. IEC 61850-7-420:2021. Communication networks and systems for power utility automation – Part 7-420: Basic communication structure — Distributed energy resources logical nodes. Geneva: IEC, 2021.
[30] IEC. IEC 61850-5:2020. Communication networks and systems for power utility automation – Part 5: Communication requirements for functions and device models. Geneva: IEC, 2020.
[31] IEEE. IEEE C37.118.2-2011. IEEE Standard for Synchrophasor Data Transfer for Power Systems. New York: IEEE, 2011.
[32] A. Ulbig, et al., "Impact of Grid Integration of Wind Power on Power System Stability," *Applied Energy*, 2014, vol. 123, pp. 145-153.
[33] ENISA. Report on ICS Security [Electronic resource]. Mode of access: https://www.enisa.europa.eu (Date of access: 10.01.2025).
[34] M. Usman, et al., "IoT-Based Secure Energy Management for Smart Grids," *IEEE Internet of Things Journal*, 2021, vol. 8, no. 10, pp. 7892-7905.

CHINA TO HOST ITU WORLD RADIOCOMMUNICATION CONFERENCE 2027 IN SHANGHAI

The International Telecommunication Union (ITU) is pleased to announce that the next Radiocommunication Assembly (RA-27) and World Radiocommunication Conference (WRC-27) will take place in Shanghai, China, from 11 October to 12 November 2027.

Held every four years, the World Radiocommunication Conference (WRC) reviews and revises the ITU Radio Regulations, the international treaty governing the use of the radio frequency spectrum and associated satellite orbits.

During the four-week conference, ITU Member States will consider the results of technical studies and adopt decisions that shape the future use of spectrum for a wide range of radiocommunication services and applications, including mobile, satellite, radiolocation, radio astronomy, and space research services that support lunar communications.

"WRC-27 will be a defining moment in making universal, meaningful connectivity a reality," said ITU Secretary-General Doreen Bogdan-Martin. "The conference will make critical decisions about sharing spectrum and satellite orbit resources efficiently and equitably, on Earth and in space, in ways that benefit all of humanity."

Over 4,000 delegates are expected to attend the WRC-27 and RA-27 meetings. In addition to ITU's 194 Member States, representatives from sister United Nations agencies, Regional Telecommunication Organizations, and ITU Radiocommunication Sector Members will participate as observers.

"As the first country in the Asia-Pacific region to host the WRC, China highly anticipates the successful convening of this grand event," said Li Lecheng, Minister of Industry and Information Technology (MIIT) of China. "We will fulfill our obligations as the host country in accordance with ITU's rules and regulations, provide comprehensive services and support for the Conference, and work together with all ITU member states to present to the world a radiocommunication event that fosters win-win cooperation and yields fruitful outcomes. We hereby extend a cordial invitation to all delegates to the event and wish them all a pleasant stay in Shanghai."

The WRC preparatory process spans a four-year study cycle, involving extensive studies and technical discussions among governments, regulators, equipment manufacturers, telecommunication operators, and industry forums at national, regional, and global levels.

"World Radiocommunication Conferences are essential to shaping the future of global communications," said Mario Maniewicz, Director of the ITU Radiocommunication Bureau. "WRC-27 in Shanghai will guide the evolution of radiocommunication services on Earth and in space – for broadband connectivity, safety of life, and space and Earth observation. It is where the international community comes together to ensure that spectrum regulations keep pace with rapid technological innovation and respond to global, regional, and national needs."

WRC's inclusive and collaborative approach enables consensus-building among all stakeholders. It ensures that the Radio Regulations remain a stable, predictable, and universally applied framework – fostering an interference-free environment that supports continued investment in radiocommunication services.

The Radiocommunication Assembly 2027 (RA-27) will take place from 11 to 15 October 2027.
The World Radiocommunication Conference 2027 (WRC-27) will take place from 18 October to 12 November 2027.

SYNCHROINFO JOURNAL

www.media-publisher.eu/synchroinfo-journal

BROADBAND AS KEY DIGITAL INFRASTRUCTURE

Augustin Vyukusenge [1],

[1] University of Burundi, Bujumbura, Burundi

vyukusengeaugustin@yahoo.fr

ABSTRACT

The digital divide is taking on new forms, even as access gaps narrow. Digital technologies are expanding in scale, reach, and impact. Policymaking and 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." The article will explore solutions to making broadband policy universal and broadband more accessible. It will also address issues of global internet coverage.

KEYWORDS: *ITU; telecommunications; broadband technology development;* internet; digital inequalities; digital technologies

DOI: 10.36724/2664-066X-2025-11-3-30-40

Received: 30.06.2025
Accepted: 28.07.2025

Citation: Augustin Vyukusenge, "Broadband as key digital infrastructure", *Synchroinfo Journal* **2025**, vol. 11, no. 3, pp. 30-40.

Introduction

Digital technologies are expanding in scale, reach, and impact. Policymaking and 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.

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.

Digital financial inclusion is growing among some online populations, particularly youth, globally. Among firms and enterprises, connectivity and digital capabilities vary significantly by size, although significant data limitations make it difficult to assess enterprise connectivity in some regions of the world. Available survey data suggest that internet access and digital capabilities among micro, small, and medium-sized enterprises (SMEs) are generally improving over time. The gender digital divide is narrowing in absolute terms in the number of internet users.

The ITU/UNESCO Broadband Commission for Sustainable Development was established in 2010 following the 2007/2008 financial crisis. Governments were convinced that broadband could play a vital role in economic recovery and in promoting citizen-centered services to achieve development goals and economic progress.

After fifteen years of focused policy and statistical analysis, the ITU/UNESCO Broadband Commission for Sustainable Development continues to believe that broadband stakeholders are well-positioned to realize the potential and opportunities of broadband for improved development outcomes. Telecommunications services, infrastructure providers, and operators have enabled and contributed to fifteen years of relatively stable economic growth across various countries and economies. Many of the world's largest companies (by revenue and market capitalization) are now digital, technology, or semiconductor companies. 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.

Overview of developments in mobile communications and broadband access

The digital economy is continuing to expand, entering into all aspects of our lives. Growth in the number of Internet users needed to achieve digital inclusion continues, with the online population adding an additional 280 million people over 2023 to reach 5.5 billion people regularly online by end-2024, equivalent to just over two-thirds or 68% of the total global population (Figure 1).

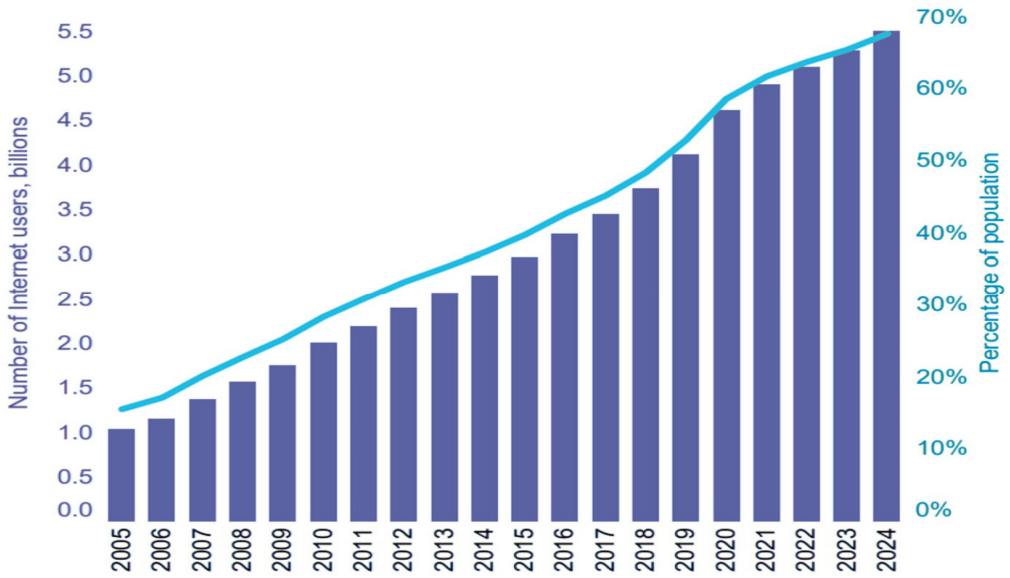


Figure 1. Individuals using the Internet, 2005-2024 [1]

However, this still leaves some 2.6 billion people offline, around 32% or one- third of the global population [2]. This gap in the number of Internet users can be distinguished from the "usage gap" of people living within mobile broadband coverage but not using it (estimated at 38% of the global population in 2022), as well as the coverage gap (estimated at around 5% of people, living in areas still not covered by mobile broadband [3]). Today, offline populations and communities risk being excluded from opportunities created by the digital economy, as well as many citizen services (e.g. in e-government, health and education). Indeed, the expansion of mobile broadband across different verticals such as manufacturing, finance, construction and communications is a bedrock for fresh growth in the digital economy.

Mobile communications is also continuing to grow steadily. The GSMA estimates that globally, there were 8.87 billion mobile connections by the end of 2024, projected to reach 9.99 billion mobile connections in 2030 (Figure 2).

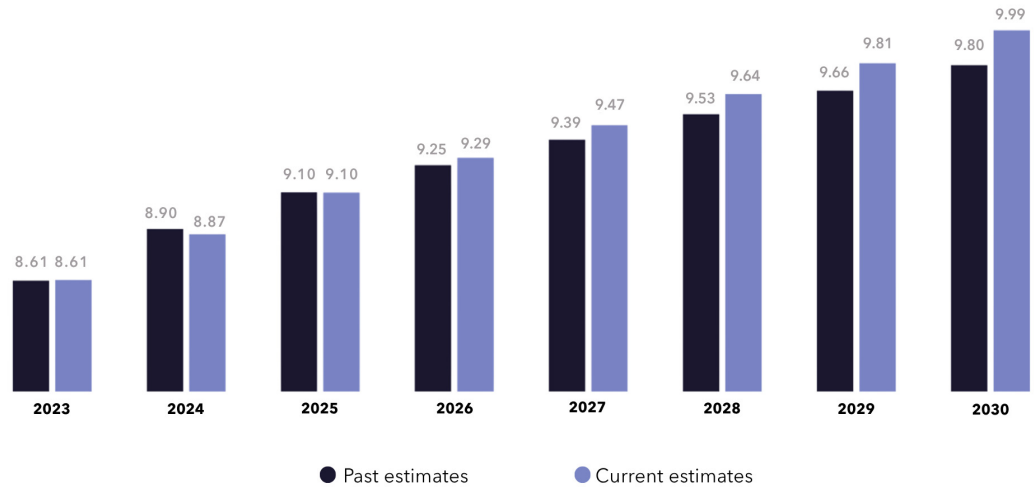


Figure 2. Growth in Global Mobile Connections, 2023-2030 [1]

The number of 5G base stations in China amounted to 3.92 million by June 2024, equivalent to a third or 33% of the total number of mobile base stations in China [4]. The number of 5G mobile subscribers exceeded 927 million in June 2024 (52.4% of total mobile subscribers in China). The Ericsson Mobility Report estimated that 5G subscriptions in India reach around 970 million by the end of 2030, accounting for 74% of mobile subscriptions [5].

Meanwhile, growth in connected devices and demands on networks (including from fixed wireless access solutions) is fuelling massive traffic growth. Total mobile data traffic is estimated to treble between 2023 and 2029. At the same time, the nature of the expectations and demands placed on networks, by users, applications, and use cases is changing. In 5G's programmable networks, developers using network APIs, are dynamically calling or leverage individual network capabilities, such as high peak data rates, or ultra-low latencies, into a new generation of applications and use cases. This both unlocks fresh innovation across private and public sectors, whilst also adding a further dimension to the digital divide.

According to ITU's most recent data (Figure 3), four out of five individuals aged 10 years-old or over own a mobile phone. In terms of where these subscribers are located, phone ownership exceeds 90% of the population in high-income countries (96%), Europe (95%) and CIS (94%). The lowest phone ownership rates are in low-income countries (56%), LDCs (63%) and LLDCs (65%).

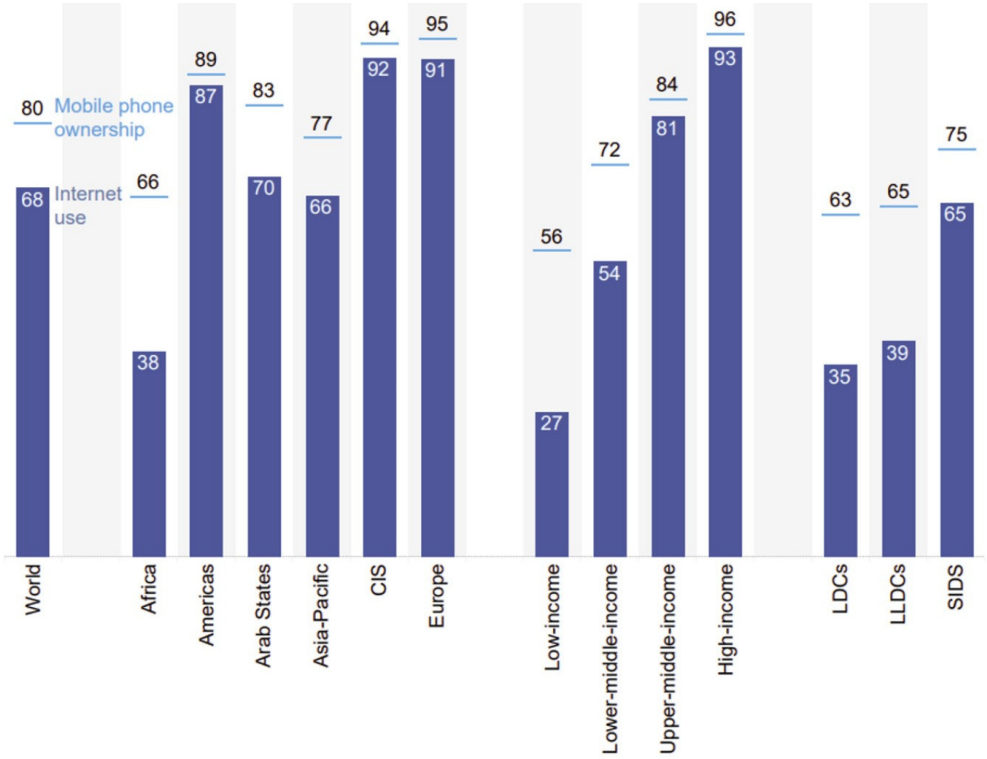


Figure 3. Percentage of individuals owning a mobile phone and using the Internet, 2024 [1]

In the meantime, digital technologies are evolving and diversifying, and encompassing developments such as Artificial Intelligence (AI). AI is no single technology, but instead comprises multiple different services, types of models, and the connection of "many different data sources", often distributed across hybrid IT infrastructure [6]. AI is increasingly managing network complexity and orchestrating network demands, which is essential in the new era of programmable networks. In turn, AI-infused networks are better able to meet the diverse demands of AI use cases that enterprises, governments and consumers place on networks.

We stand on the brink of a future that will be significantly shaped by AI, which holds immense potential to accelerate progress across the SDGs. However, such benefits risk being distributed unevenly – most notably, in the Global South – if our global community does not immediately and concertedly shape its trajectory at this critical stage, focusing on four key components.

First, from advancing access to healthcare and education to driving climate action, AI is already transforming lives. However, to ensure that these benefits reach everyone, it is crucial to strengthen countries' Digital Public Infrastructure (DPI), which will lay the groundwork for AI's positive impact to flow widely and equitably.

Second, AI must be developed and deployed inclusively. AI systems are often trained on datasets sourced mainly from the Global North, creating information asymmetry and an imbalance in data representation. This often results in AI models with low local relevance and benefit. AI must be specifically designed to reflect the needs, challenges, and opportunities of developing countries.

Third, tailored support at the country-level is needed to ensure that AI is harnessed to its maximum potential for inclusive development.

Accelerating digitalization with AI is crucial to improving of meeting the Sustainable Development Goals (SDGs). Modern connectivity plays a foundational role in digitalization: AI makes that role greater. For instance, 5G acts as a platform for connected technologies and solutions to flourish, enabling societal benefits that contribute to the SDGs. Today's AI enhancements, including in network performance and operational efficiency, give more potency to the 5G platform.

Looking ahead, new technologies are being architected to enable networks to self-heal, self-organize, and self-configure, helping them manage the increasingly complex demands of digitalization. The pace of AI-infused innovation within and on top of the network is rapid and necessary to close the gap toward the SDGs. Rapid advancement requires regulation which enables innovation.

A broad approach to regulating AI technology should be avoided, otherwise it risks stifling needed investment and innovation. As always, continuous dialogue between industry, policy-makers, and other stakeholders is essential. Building trust around AI usage and development is key. No less important is the need to safeguard interoperability to help provide affordable, scalable, and modern connectivity.

Emerging technologies present significant opportunities for the telecom sector. AI can dramatically improve network management through predictive analytics, enabling more efficient traffic handling and fault management. However, the integration of these technologies also introduces complex challenges and risks. The financial implications of adopting high-end AI solutions pose considerable challenges, particularly for operators in developing regions where investment in such technologies may not be feasible without supportive regulatory frameworks and financial models. Cybersecurity remains a paramount concern, as more intelligent networks are potentially more vulnerable to sophisticated cyber-attacks. Ensuring the security of these systems is critical, especially as they become integral to delivering essential services, including healthcare.

The deployment of AI could inadvertently exacerbate the digital divide, with less developed regions struggling to keep pace with the rapid technological advancements seen in more developed markets. This necessitates a balanced approach in regulatory frameworks that not only encourages innovation but also ensures equitable access to technology.

Adopting human-centric and responsible AI and GenAI-based tools is vital to boost the global digital economy. AI-driven predictive maintenance can enhance broadband infrastructure, improve broadband customers experience by ensuring more reliable and widespread access while AI-powered virtual assistants and chatbots can provide 24/7 support, helping users navigate digital services and access vital information.

The risks associated with GenAI, such as increased inequality, non-availability of complete, and quality data, copyright infringements, and embedded biases, highlights the need for careful monitoring and iterative improvements. Ensuring GenAI systems are trained on diverse and representative quality datasets is crucial to mitigating these risks.

In fact, the Digital Cooperation Organization (DCO) Member States have demonstrated their commitment to responsible AI adoption by signing the Riyadh AI Call for Action Declaration (RAICA), reaffirming their shared desire to harness AI's potential to improve lives worldwide. The DCO is developing several AI initiatives, including an AI toolkit to assist Member States in assessing AI readiness and integrating AI, including GenAI, into business systems to enhance productivity, service quality, and efficiency. This includes creating controlled testing environments with flexible AI regulatory frameworks, enhancing global cooperation on AI governance, and encouraging investments in AI digital skills and requisite infrastructure.

By promoting cooperation through joint research and shared service platforms, stakeholders can balance AI innovation with regulatory measures. While GenAI offers many opportunities to enhance connectivity and sustainable development, the DCO recognizes the importance of addressing associated challenges and risks through collaboration and comprehensive co-created digital strategies. By leveraging GenAI responsibly, we can make significant strides toward achieving the Broadband Commission's Advocacy Targets and building a more inclusive, sustainable and connected global digital economy.

Broadband as key Digital Infrastructure

By 2025, all countries was planned to have a funded National Broadband Plan (NBP) or strategy in place or include broadband in their Universal Access and Service (UAS) Definition. A sound policy approach should also promote action to enhance broadband access and/or when broadband is included in countries' Universal Access/Service (UAS) definitions.

Research suggests that this target is not achieved. Despite increases in broadband coverage globally, a number of National Plans have expired and not been renewed (ITU, 2023). In 2024, 167 countries had a national broadband plan or other strategic document emphasizing broadband, marginally down from 170 in 2022. Figure 4 depicts the national strategy planning process.

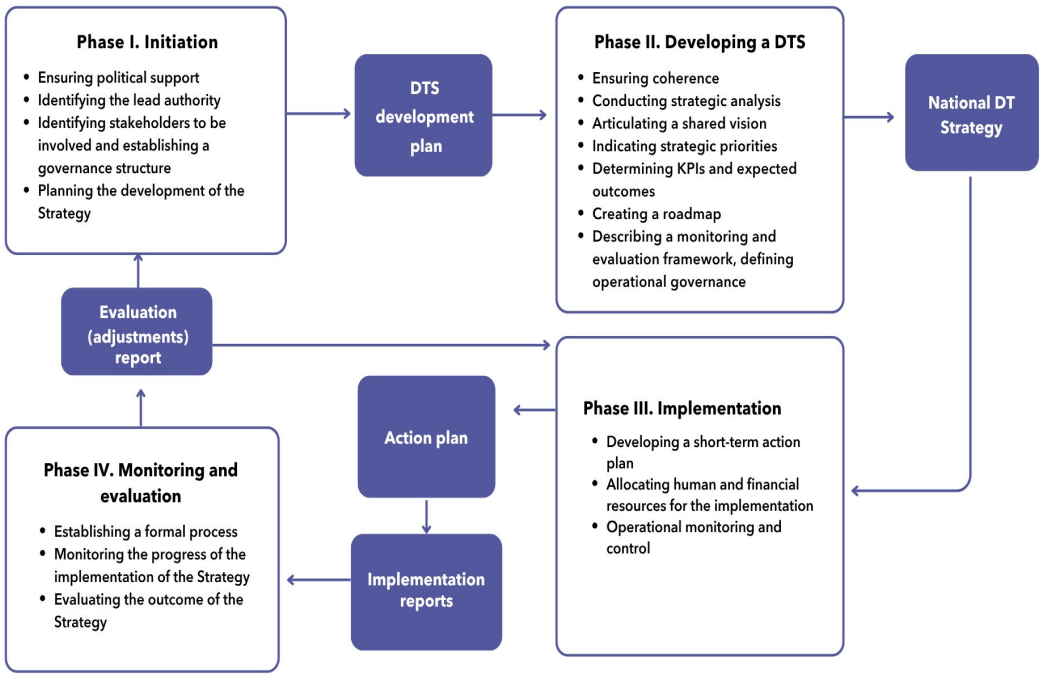


Figure 4. The national strategy planning process [1]

Today, digital transformation is the new focus of policy-making, as countries seek to address the far-reaching ramifications of digital policy. National digital infrastructure is recognized as just one building block of strategies for digital transformation. The era of discrete Plans for the telecom or broadband sector are broadly over. Today, Digital Agendas, National Visions or National Strategies on AI are increasingly the focus of policy-makers' attention.

Broadband infrastructure planning is expensive, complex and needs constant revision (Figure 4). Governments need to work in conjunction with the private sector, where much of the investment capital and expertise in relation to broadband and digital services now resides.

Further, it is now necessary to integrate and include the impact of AI on health sectors (e-Health strategies), transport and housing (Smart City Plans), Education (e-learning and edtech, school strategies) and security (cybersecurity and national defence). Important regional and sectoral strategies are being developed – for example, Europe's General Data Protection Regulation (GDPR) or the African Union's AI Strategy Roadmap or in Europe's Digital Health Action Plan [7], coordinated by the World Health Organization (WHO). For example, Figure 5 shows all the areas that Australia is taking into account in planning its digital economy strategy, which builds on and incorporates its Data Strategy, Cybersecurity Strategy, Blueprint for Critical Technologies, Digital Government Strategy and National Blockchain Roadmap.

Figure 5. Putting Australia's Digital Economy Strategy into Context [1]

Recent examples of Digital Strategies include Belize's National Digital Agenda for 2022-2025, Qatar's Digital Agenda 2030 adopted in March 2024, Guyana's efforts to advance its national digital agenda and Uganda's National Digital Agenda Strategy, launched in August 2024.

In 2025, entry-level broadband services should be made more affordable in low- and middle-income countries (LMICs). Making broadband more affordable is key to achieving universal and meaningful connectivity. This target specifies that prices for entry-level broadband services should be below 2% of monthly GNI per capita in developing countries by 2025. It is important that the total cost of ownership and use of broadband devices and connectivity is considered.

According to ITU's 2024 Facts and Figures report [8], fixed and mobile-broadband services continued to become more affordable in 2024, costing less as a proportion of income per capita in 2024, than in 2023. The data-only mobile-broadband basket and the fixed- broadband basket became more affordable in all regions and for all income groups.

Globally, the world has achieved the affordability target for mobile data-only broadband. For mobile data-only broadband, Latin America achieved the 2% target in 2024, meaning that all world regions have now achieved this target, except the African region. However, the fixed data-only broadband target has not yet been achieved, where Europe is the only region to have achieved the affordability target, although Asia-Pacific and the CIS region are approaching the target.

Similarly, in terms of income levels, a wide gap persists between high-income economies and the rest of the world. High-income countries are the only group of countries to have achieved the affordability target in both mobile and fixed broadband. Upper middle-income countries have achieved the affordability target in terms of mobile-broadband, but not fixed broadband.

In 2024, 114 economies out of 188 met the affordability target for at least the data-only mobile broadband or the fixed broadband basket, nine economies more than in 2023. However, among the low-income and middle-income economies, only 65 or around one-half of countries have met the Broadband Commission's affordability target for at least one of the two baskets. Given recent trends in ICT prices and income levels, it looks increasingly inevitable that most of the remaining 66 economies in that income group will miss the 2025 objective, even for entry-level broadband access.

In 2020, nearly 2.5 billion people lived in countries where the cost of the cheapest available smartphone was a quarter or more of the average monthly income, according to a 2020 survey of 70 countries by the Alliance for Affordable Internet (A4AI), equivalent to the share of monthly income that a typical European household spends on housing & utilities.

In some countries, devices were even less affordable still. In Sierra Leone, the average person needs to save six months' salary to buy the cheapest available smartphone. In India, where almost 18% of the global population now lives, the price of the cheapest smartphone from leading operator Jio was 206% of average monthly income. This is striking in a country that has some of the lowest-priced Internet data in the world.

There is a stark divide between countries for handset affordability. Botswana topped the survey for most-affordable devices, with a low-cost smartphone priced at just 4% of average monthly income, with Jamaica (5%), Mexico (5.7%) and Costa Rica (6%) following closely behind. While these countries are outliers at either end of the price spectrum, there is also wide disparity among regions. In Africa, devices were least affordable at 62.8% of average monthly income compared with 11.7% in the Americas and 16.2% in Asia-Pacific (excluding India). With India included, the Asia-Pacific figure jumps to 87.4% owing to India's role as an outlier with a very large population and relatively high costs.

A4AI makes the following recommendations:

1) duce taxes on low-cost handsets.

2) Support the use of Universal Service & Access Funds (USAFs) to subsidize devices.

3) Support fina ing plans to help low-income consumers spread the cost of devices over time.

Broadband-Internet user penetration should reach: 75% worldwide; 65% in low- and middle-income countries; and 35% in least developed countries, in 2025. Internet access is a priority because access to broadband Internet is fundamental to inclusive and sustainable development. Today, the Internet and broadband are increasingly vital for work, education, business, entertainment and global connection [12, 13].

In 2024, there was around 5.5 billion people online (approximately 2.8 billion male and 2.7 billion female Internet users), with another 2.6 billion offline. Internet use grew to an estimated 68% of the total global population in 2024 (Figure 6), up from 53% in 2019. There is still much to be done to achieve universal and meaningful connectivity. In 2024, Internet use was 93% in high-income countries, 54% in LMICs but just 35% in the LDCs (according to the most recent ITU estimates [9]).

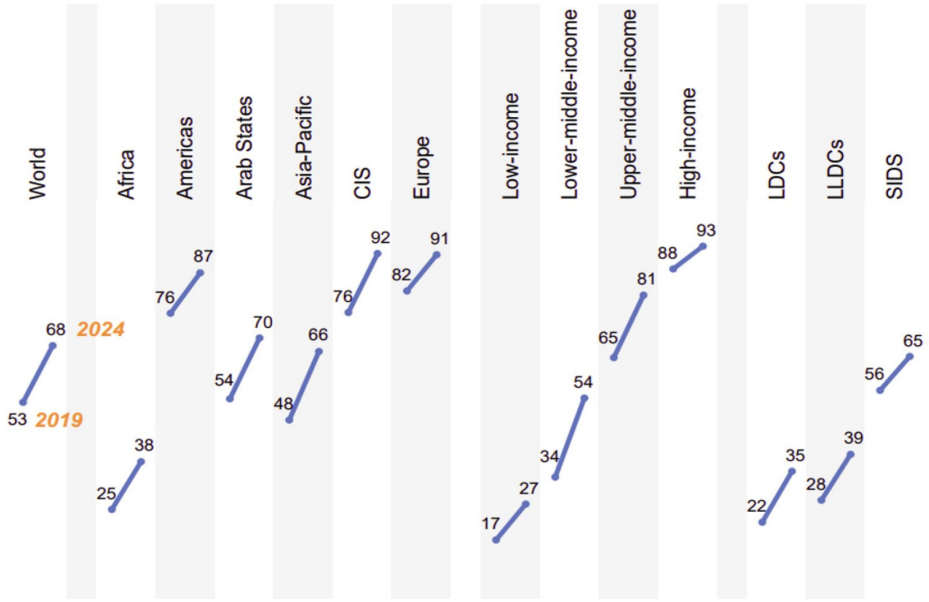


Figure 6. Percentage of individuals using the Internet by region, 2019 and 2024 [1]

However, there are also the first indications of 'digital disconnection'. For example, one survey suggests that the penetration of Internet users online in the UK actually fell for the first time [10]. The causes of this 'digital disconnection' are as yet poorly understood, but they may include factors as diverse as increases in the cost-of-living, disenchantment with the digital world (e.g. some parents are now giving children feature phones, rather than smartphones to try and limit screentime) and ageing populations in a growing number of countries. Separately, there are attempts by either parents or regulators and schools to deal with digital addiction or digital harms – for example, the recent ban on social media enacted for under 16 year-olds in Australia, or attempts by schools to limit, reduce or ban mobile phones in Australia, France and Switzerland.

As an example, the experience of Vodacom, which is using AI to expand its services in African countries, is interesting. Vodacom Group is a leading pan-African telco that provides an array of services from traditional products to financial services to over 200 million people in Africa. In addition to deploying various cloud-based digital platforms, products and tools across its footprint, Vodacom has deployed various AI tools (including machine learning and big data) to provide better services to customers in line with their needs, including mobile financial services products and loans.

One example of customers benefitting from AI is through an offer deployed in South Africa in 2017 and in the Democratic Rep. of Congo, Lesotho, Mozambique and Tanzania as of 2019, called 'Just 4 You'. It provides affordable, tailor-made bundles, created using machine learning and big data to design bespoke deals for each customer. Today, this package delivers great value to over 40 million customers in Africa, and it has evolved to offer smart discounts on fintech services and third-party offerings, as well as regional offers on voice and data bundles and some third-party services. In particular, it has become popular among customers on low incomes, as a best value deal.

Vodacom has also deployed various health and IoT solutions across Africa, and implemented process improvements across numerous areas, including in its call centres. Vodacom implements these innovations ethically and responsibly, taking various factors into account including each country's specific consumer protection laws and human rights laws.

Looking beyond the international digital divide, various digital divides persist at the national level, including in high-income countries. While overall Internet use is increasing, some marginalized groups are being left behind, such as the elderly, women & girls, people living in rural areas and people with disabilities.

In terms of new markets where Internet users are being added, China added 7.4 million new Internet users over 2024. In China, communication with family is still the main reason why offline individuals wish to go online, followed by the availability of Internet devices and free training in how to use the Internet.

Elderly individuals aged 60+ accounted for 62% of the total offline non-user population in China in June 2024. Lack of knowledge about how to use the Internet is perceived as the biggest barrier (49% of non-netizens), followed by lack of literacy in Pinyin or other literacy limitations (27.6%). Digital accessibility for the elderly and disabled groups is a significant driver in helping bridge the digital divide. By the end of June 2024, 2,792 websites and apps closely related to the lives of the elderly and people with disabilities were updated for accessibility. People aged 60+ accounted for 20.8% of new Internet users in the first half of 2024.

Singapore is another country facing a significant digital divide among older adults. The example below illustrates how Singapore is promoting digital inclusion for older adults.

Singapore regularly monitors Internet access and digital skills. Due to its urbanization and technologically savvy population, Internet access is available at home to 99% of all households. Senior-only households of people aged 60 years+ have:

• A 7% percentage point gap in terms of households with Internet access (93%) due to a perceived lack of need, skills, knowledge and confidence of seniors to use the Internet (up from 55% in 2017).

• Only 64% of senior households own a computer, due to a perceived lack of need or interest to own or learn to use computers (compared to 90% of all households and 98% of households with children).

• 89% of seniors aged 60+ own a smartphone (compared with 100% for all resident households).

With more time spent online, it is vital to ensure that citizens have the necessary knowledge and skills to protect themselves from online risks (e.g., scams, misinformation, harmful online content). The Government is building on existing efforts to:

• Highlight the need for all residents to keep their digital devices up-to-date (e.g., downloading and installing software patches, or upgrades) to reduce exposure to online risks.

• Help Singaporeans stay safe and alert online by teaching important cybersecurity skills, such as enabling two-factor authentication (2FA) and security checks when transacting online.

• Improve Singaporeans' information literacy. As the Internet has become the primary source of information for many people, we will continue efforts to help Singaporeans be informed and discerning consumers of information via initiatives such as the National Library Board (NLB)'s Source, Understand, Research, Evaluate (S.U.R.E) programme [11].

• Provide people with a better understanding of online harms that they may be exposed while connected. There are encouraging improvements in seniors' digital skills in various areas (e.g., communicating online, searching for information, transacting online).

The Infocomm Media Development Authority (IMDA) regularly monitors statistics for Internet connectivity by age. In 2023, only 45% of seniors are generally willing to try out new technologies, compared with 65% of Singaporeans aged 15 to 59 (IMDA, 2023). IMDA's Seniors Go Digital programme was launched in 2020 to help seniors embrace the benefits of going digital and equip them with knowledge and digital skills. Notably, seniors are becoming more comfortable with digital transactions. For instance, the percentage of seniors using online payments has more than doubled from 38% in 2018 to 78% in 2022. Also, more seniors are using the Singpass app in 2022 (67%), compared to 2020 (41%).

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.

Target is close to being achieved for mobile broadband affordability, but not for fixed broadband.

There has been strong progress in access to the Internet, but Internet access is often concentrated in urban areas, and is far from universal. The age digital divide is now a divide prevalent in many high-income countries (e.g. the UK, Singapore) or among the unconnected, offline populations (e.g. China).

After fifteen years of dedicated policy and statistical analysis, the ITU/UNESCO Broadband Commission for Sustainable Development continues to believe that broadband stakeholders are well-positioned to deliver on the promise and opportunities of broadband for improving development outcomes.

In the next part of this paper, continuing this topic, will 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.

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] ITU Facts & Figures 2024, available at: www.itu.int/hub/publication/D-IND-ICT_MDD-2024-4/

[3] https://www.gsma.com/r/wp-content/uploads/2023/10/The-State-of-Mobile-Internet-Connectivity-Report-2023.pdf

[4] https://english.www.gov.cn/archive/statistics/202407/23/content_WS669f8be0c6d0868f4e8e9625.html

[5] https://economictimes.indiatimes.com/industry/telecom/telecom-news/number-of-5g-subscribers-in-india-may-triple-to-970-mn-by-2030-report/articleshow/115691585.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

[6] Feature: Nvidia, HPE chiefs address A... – Mobile World Live.

[7] WHO Press Release, 13 September 2022, www.who.int/europe/news/item/13-09-2022-countries-in-the-european-region-adopt-first-ever-digital-health-action-plan.

[8] ITU's 2024 Facts and Figures report. https://www.itu.int/hub/publication/D-IND-ICT_MDD-2024-4/

[9] 2Measuring digital development – Facts and Figures 2024 – ITU.

[10] Lloyds Consumer Digital Index 2023 report, available at: 231122-lloyds-consumer-digital-index-2023-report.pdf.

[11] singapore-digital-society-report-2023.pdf; www.channelnewsasia.com/commentary/singapore-elderly-tech-digital-isolation-social-lonely-4694131

[12] 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.

[13] 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.