Simulation of the cloud IoT-based monitoring system for critical infrastructures

Oleksii Smirnov [1], Viktoriia Sydorenko [2], Marek Aleksander [3], Oksana Zhyharevych [4] and Serhii Yenchev [2]

[1] *Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine*
[2] *National Aviation University, Kyiv, Ukraine*
[3] *Panstwowa Wyzsza Szkoła Zawodowa w Nowym Saczu, Nowy Sacz, Poland*
[4] *Lesya Ukrainka Volyn National University, Lutsk, Ukraine*

Abstract

IoT is one of the most developing ICT technology during the last 15 years. There are many cases of IoT implementation in various spheres including critical infrastructures (transport, banks, ICT, etc.). In the paper IoT concepts and requirements were analyzed, advantages and disadvantages were defined as well as benefits for companies were declared. Main standards and best practices in different aspects of IoT implementation were analyzed in this study. Based on the developed mathematical models of WSN, model studies were conducted to verify the theoretical dependences of the collision probability basis of the collision probability modeling, which allowed to verification of the proposed models. Cloud-based monitoring information technology was further developed, which allowed to development of software and hardware monitoring of real-time environmental parameters in the real-time IoT concept. It can be effectively implemented in various critical infrastructures for both cybersecurity and physical security parameters monitoring. The next steps will be related to software realization of the proposed models for cloud IoT-based monitoring system realization in critical infrastructures.

Keywords

IoT, cloud technology, monitoring, critical infrastructure, simulation, ICT, WSN, security

1. Introduction

The Internet of Things is a global infrastructure for the information society that connects (physical and virtual) objects using emerging, interoperable information and communication technologies to enable improved services. The Internet of Things (IoT) fully utilizes objects to provide services to a variety of applications while meeting security and privacy needs by utilizing identification, data collecting, processing, and communication capabilities. The IoT may be seen as a vision having both technological and societal ramifications when seen from a wider angle [1].

Devices can interact with each other in one of three ways (see Fig. 1): directly (case c), over a communication network without a gateway (case a), or through a communication network with a gateway (case b). Additionally, combinations of cases are possible; for instance, devices can communicate with one another directly through a local network (case c), which is a network that provides local connectivity between devices and between devices and a gateway, such as an ad-hoc network, and then indirectly through a local network gateway (case a). For IoT systems, the security considerations [2–3] are pertinent and crucial.

CMiGIN 2022: 2nd International Conference on Conflict Management in Global Information Networks, November 30, 2022, Kyiv, Ukraine
EMAIL: o.smirnov@gmail.com (O. Smirnov); v.sydorenko@ukr.net (V. Sydorenko); marek.aleksander@gmail.com (M. Aleksander); o.zhyharevych@gmai.com (O. Zhyharevych); esw@ukr.net (S. Yenchev)
ORCID: 0000-0001-9543-874X (O. Smirnov); 0000-0002-5910-0837 (V. Sydorenko); 0000-0003-2619-1063 (M. Aleksander); 0000-0002-1979-4168 (O. Zhyharevych); 0000-0001-6994-9378 (S. Yenchev)

Information security (IoT Security), scaling up the expanding amount of technological devices and data (IoT Scalability), and solving IoT Technical Solutions and Low-Power Consumption have been highlighted as the three connected fundamental concerns for the IoT idea. Protocols for completing IoT activities were also examined.

MQTT is a protocol for data collection from devices and transmission to their servers (D2S); XMPP is a protocol for establishing connections between devices and people, which is a subset of the D2S-scheme; DDS is a quick bus for the fusion of intelligent devices (D2D); and AMQP is a queuing system for establishing connections between servers (S2S).

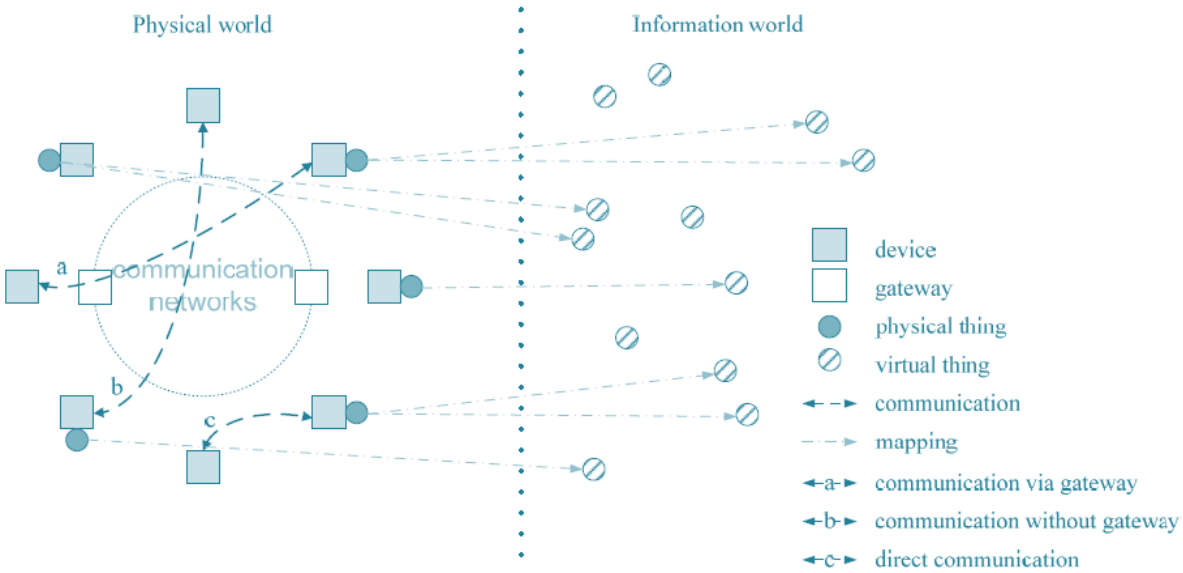

Figure1: Technical overview of the IoT

IoT combines devices, getaway, communication, physical and virtual things, etc (Fig. 1).

2. Analysis of IoT features and requirements for simulation and construction

The following are the IoT's core characteristics:

- *Things-related services:* Within the limitations of things, such as privacy protection and semantic coherence between physical things and their associated virtual things, the IoT is capable of offering thing-related services. Both the technology in the physical world and the information world will alter in order to deliver thing-related services within the limitations of things.
- *Enormous scale:* At least a factor of ten more devices than those currently linked to the Internet will need to be controlled and be able to communicate with one another. There will be a discernible change in favor of device-triggered communication in the ratio of communication prompted by devices to communication caused by people. The management of the produced data and its interpretation for application purposes will be even more crucial. This has to do with both the semantics of data and effective data processing.
- *Heterogeneity:* As they are based on many hardware platforms and networks, IoT devices are heterogeneous in nature. Through multiple networks, they may communicate with other gadgets or service platforms.
- *Interconnectivity:* Anything may be connected to the global information and communication infrastructure in terms of the Internet of Things.
- *Dynamic changes:* Device context, such as location and speed, as well as the states of devices, such as sleeping and waking up, connected and/or disconnected, also alter dynamically. Additionally, the quantity of devices may fluctuate.

Analysis of up-to-date papers [4-8] gives a possibility to define both the main advantages and disadvantages of the IoT in the context of simulation and practical implementation of this technology for critical infrastructures (with high-security requirements).

Today Critical Infrastructure (Fig. 2) contains the following sectors (in the USA for example): Chemical, Commercial Facilities, Communications, Critical Manufacturing, Dams, Defense Industrial Base, Emergency Services, Energy, Transportation Systems, and other sectors are among them.

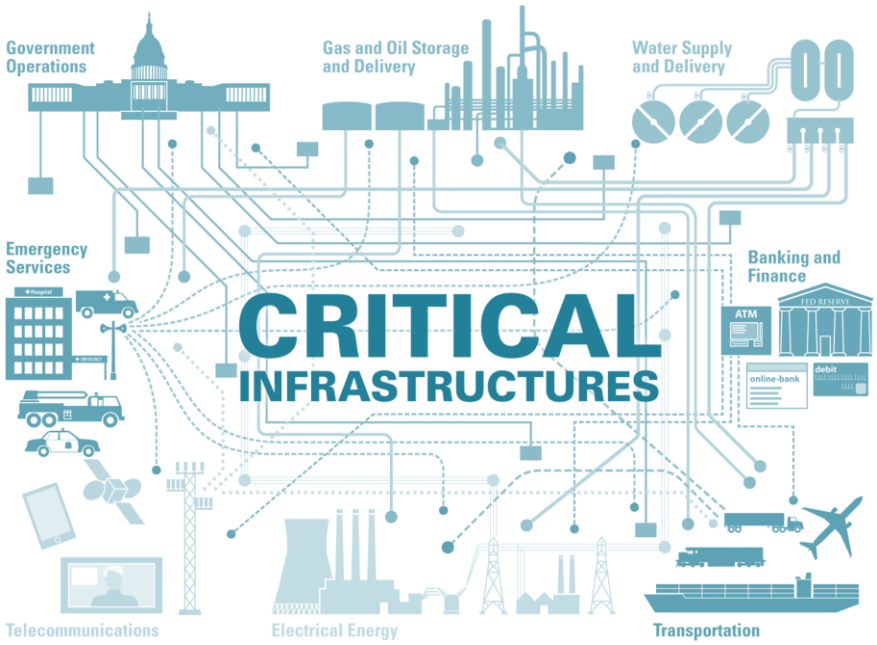

Figure 2: Critical infrastructures sectors

One of the most effective way of IoT use in critical infrastructure is monitoring – it can include cybersecurity parameters monitoring as well as physical parameters monitoring.

3. The security and other IoT requirements for critical applications

In Fig. 3 shows the ecosystem of a typical IoT architecture according to the mentioned international standard [1]. These shortcomings of IoT negatively affect its basic functions, in particular, its application for monitoring, in addition to security problems, faces the problem of collisions during scaling, as well as the high energy needs of known solutions, most of which are deterministic.

Today it is necessary to create a new class of wireless networks (WSN) that allow to fill certain gaps in the development of WSN networks related to solving problems such as:

- obtaining low financial costs in terms of network nodes equipped with sensors for general and simple applications,
- ease of operation, in particular, sensor algorithms and ease of connecting and disconnecting new components,
- significant limitation of the occupied band of radio frequencies in the context of the growing deficit of the radio frequency spectrum,
- significant energy savings at the nodes (reduction of nodes for data processing, no receiver signal, autonomous operation of nodes in the intervals of very short activity and short-term radio radiation), especially due to lack of energy replenishment directly related to node operation time,
- complete independence of the nodes from each other.

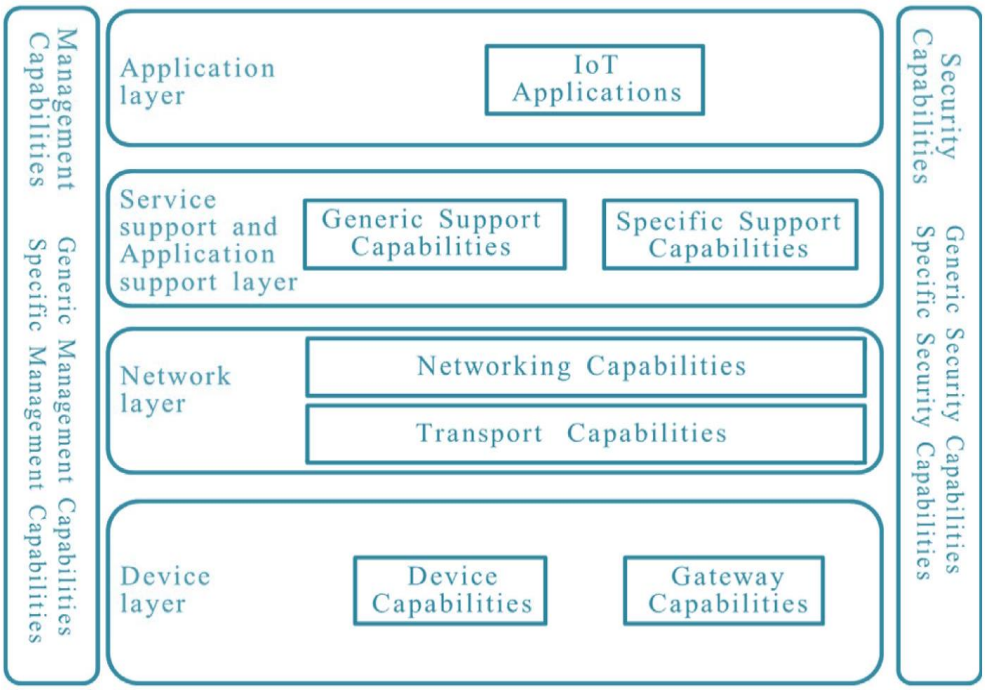

Figure 3. IoT Architecture in accordance to ITU-T Y. 2060 [1]

Thus, the first section identifies the shortcomings of the known approaches and proves the need for mathematical models, methods, and communication protocols of WSN networks with random access and appropriate monitoring information technology to ensure high performance, quality and survivability of their operation. Fig. 4 presents basic security requirements that must be implemented for risk identification and mitigation in context of cyber incident realization.

Identify and understand risks	Entities will have a responsibility to take an all-hazards approach when identifying and understanding risks. This will consider both natural and human induced hazards. This may include understanding how these risks might accumulate throughout the supply chain, understanding the way systems are interacting, and outlining which of these risks may have a significant consequence to core service provision.
Mitigate risks to prevent incidents	Entities will be required to have appropriate risk mitigations in place to manage identified risks applicable to their sector. Risk mitigation should consider both proactive risk management as well as having processes in place: to detect and respond to threats as they are being realised; and plan for disasters and have a way to lessen the negative impact were it to actually occur.
Minimise the impact of realised incidents	The regulated entity will be responsible for engaging with the regulator to ensure that identified risks and proposed mitigations are proportionate to the risks, while also considering the business, societal and economic impacts. Entities will be required to have robust procedures in place to recover as quickly as possible in the event a threat has been realised. This may include ensuring plans are in place for a variety of incidents, such as having back-ups of key systems, adequate stock on hand (such as medicines), redundancies for key inputs, out-of-hours processes and procedures, and the ability to communicate with affected customers.

Figure 4: Security requirements [9]

4. WSN models for IoT-based monitoring

WSN stochastic models were developed to assess the probability of signal collision in the system.

Let's mark A_s' as event, that means collision absence in the interval $[0, s]$ $(s > 0)$. Also let's mark $P(A_s')$ as the probability of collision absence in the interval $[0, s]$. Let's consider $[0, s]$, where $s > t_p$. Suppose that $N(s) = j$, that is quantity of transmissions in the interval $[0, s]$ equals j $(j \geq 1)$. Random vector $(U_1, \dots, U_j)$ of the time between transmissions is even distributed in the set $\Omega_t^* = \{(u_1, \dots, u_j): u_1 + \cdots + u_j \leq s\}$ with conditional density $f(u_1, \dots, u_j | N(s) = j) = j!/s^j$ for $(u_1, \dots, u_j) \in \Omega_t^*$, and also 0 beyond that. In this way conditional density of collision absence in the interval $[0, s]$, supposing $N(s) = j$, is equal:

$$P(A_s'/N(s) = j) = P(U_1 > t_p, \dots, U_j > t_p) = \left(1 - \frac{jt_p}{s}\right)_+^j ,$$

where expression x_+ determines as $x_+ = x$ for $x \geq 0$ and $x_+ = 0$ for $x < 0$.

Conditional probability of collision in the length interval s, where $s > t_p$, by condition $N(s) = j$, forms by the following expression:

$$P(A_s/N(s) = j) = 1 - \left(1 - \frac{jt_p}{s}\right)_+^j \quad (1)$$

The probability of collision in the length interval s, where $s > t_p$, determines by the following expression:

$$P(A_s) = \sum_{j=2}^{\infty} e^{-n\frac{s}{T}} \frac{(n\frac{s}{T})^j}{j!} [\, 1 - (1 - j\frac{t_p}{s})_+^j], \quad (2)$$

where n is number of nodes, T is the average time between node transmissions, t_p is the time of protocol transmission.

The question of the number of nodes that remain in collision in the length interval s is also analyzed for $s > t_p$. The probability of collision in the length interval s is investigated for $s > t_p$. Below are models that characterize the lower and upper estimates of the conditional probability of the number of gears that remain in conflict, in the length interval s, assuming that the number of gears in the transmission interval is in the length interval s $(s > t_p)$ equals j.

Let's mark Y_s as number of transmissions in collision in the length interval s. In this case we will have expression:

$$(j\frac{t_p}{s})^{\kappa-1}(1 - j\frac{t_p}{s})^{j-\kappa} \leq P(Y_s = \kappa/N(s) = j) \leq (j\frac{t_p}{s})^{\left[\frac{\kappa+1}{2}\right]}(1 - \frac{t_p}{s})^{j-\left[\frac{\kappa+1}{2}\right]},$$

$$\sum_{j=2}^{\infty} e^{-n\frac{s}{T}} \cdot \frac{\left(n\frac{s}{T}\right)^j}{j!} (j\frac{t_p}{s})^{\kappa-1}(1 - j\frac{t_p}{s})_+^{j-\kappa} \leq P(Y_s = \kappa)$$

$$\leq \sum_{j=2}^{\infty} e^{-n\frac{s}{T}} \cdot \frac{\left(n\frac{s}{T}\right)^j}{j!} (j\frac{t_p}{s})^{\left[\frac{\kappa+1}{2}\right]}(1 - \frac{t_p}{s})_+^{j-\left[\frac{\kappa+1}{2}\right]} .$$

Models that characterize the lower and upper estimates of the expected number of gears in conflict and the variance of the number of gears in conflict in the length interval S $(EY_s, D^2(Y_s))$. Let's suppose $s > t_p$.

Then

$$\sum_{\kappa=2}^{\infty} \kappa \sum_{j=2}^{\infty} e^{-n\frac{s}{T}} \cdot \frac{\left(n\frac{s}{T}\right)^j}{j!} (j\frac{t_p}{s})^{\kappa-1}(1 - j\frac{t_p}{s})_+^{j-\kappa} \leq EY_s$$

$$\leq \sum_{\kappa=2}^{\infty} \kappa \sum_{j=2}^{\infty} e^{-n\frac{s}{T}} \cdot \frac{\left(n\frac{s}{T}\right)^j}{j!} (j\frac{t_p}{s})^{\left[\frac{\kappa+1}{2}\right]}(1 - j\frac{t_p}{s})_+^{j-\left[\frac{\kappa+1}{2}\right]} ,$$

$$\sum_{\kappa=2}^{\infty}\kappa^2\sum_{j=2}^{\infty}e^{-n\frac{s}{T}}\cdot\frac{\left(n\frac{s}{T}\right)^j}{j!}(^j(\bar{}_1-\left[\sum_{\kappa=2}^{\infty}\kappa\sum_{j=2}^{\infty}e^{-n\frac{s}{T}}\cdot\frac{\left(n\frac{s}{T}\right)^j}{j!}(j\frac{t_p}{s})^{\left[\frac{\kappa+1}{2}\right]}(1-j\frac{t_p}{s})_+^{j-\left[\frac{\kappa+1}{2}\right]}\right]^2$$

$$\leq D^2(Y_s)\leq$$

$$\sum_{\kappa=2}^{\infty}\kappa^2\sum_{j=2}^{\infty}e^{-n\frac{s}{T}}\cdot\frac{\left(n\frac{s}{T}\right)^j}{j!}(^j(\bar{}_1-\left[\sum_{\kappa=2}^{\infty}\kappa\sum_{j=2}^{\infty}e^{-n\frac{s}{T}}\cdot\frac{\left(n\frac{s}{T}\right)^j}{j!}(j\frac{t_p}{s})^{\kappa-1}(1-j\frac{t_p}{s})_+^{j-\kappa}\right]^2 .$$

Thus, two dependences are obtained for the probability of collision (Fig. 5). The first expression (1) describes the probability of collision in the short time tp of providing the protocol, determining the probability of intact provision of the protocol. The second expression (2) is derived using other properties of the Poisson process with respect to the probability of collision over a sufficiently long transmission time.

The graphs illustrate the probability of collision depending on the number of nodes (sensors) for the set average time between messages (Fig. 5), and also shows the dependence on the average time of protocol transmission, if the number of nodes is set (Fig. 6). For the average time between transmissions of a node equal to 10 s, the maximum number of nodes, which ensures the quality of transmission at a probability level not exceeding 10^{-2}, is 10, and for the average time between transmissions of a node equal to 30 s, the maximum number of nodes is 50. Further increase in the average time between node transmissions allows you to increase the maximum number of nodes. For a given number of nodes, increasing the average time between collisions causes a decrease in the probability of collision.

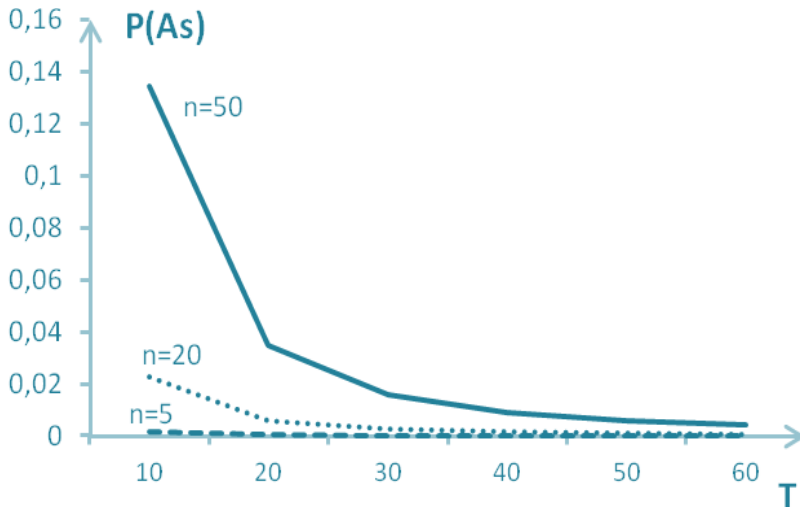

Figure 5: Collision probability in the interval s, where $s > t_p$ depending on observation time $s = 180$ s. and average time between transmissions of a node for $n = 5, 20, 50$

Using graphs, you can find the optimal values of the parameters that affect the correctness of the transfer (n, T, t_p). Graphs make it possible to determine in which range the transmission quality is provided at a given level or for which values (n, T, t_p) the probability of collision increases sharply. You can determine the order of collision probability values for arbitrarily selected parameters: for example, for $t_p = 3.2 \times 10^{-5}$, the number of transducer sensors equal to 10, and providing each sensor with an average transmission time every $T = 60$ s the collision probability is 1.65×10^{-4}.

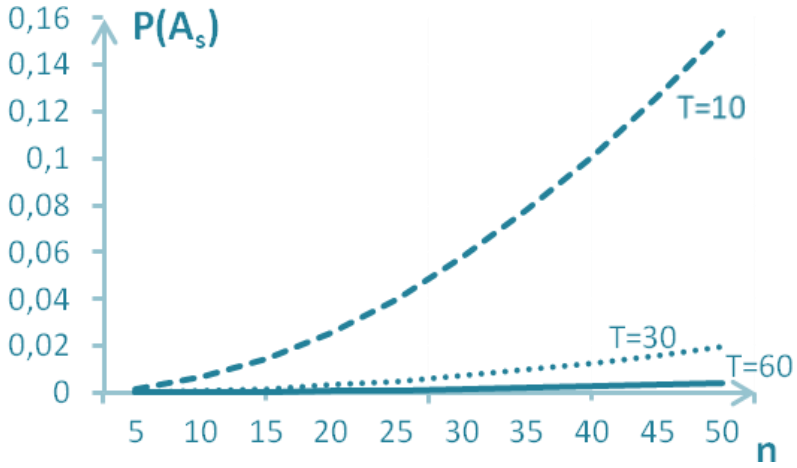

Figure 6: Collision probability in the interval s, where $s > t_p$ depending on observation time $s = 180$ s. and nodes number where $T = 10$ s., 30 s., 60 s.

The three-dimensional coordinate system (Fig. 7) shows a set of end devices $A = \{a_1, \ldots, a_m\}$ and a set of end points of the system $B = \{b_1, \ldots, b_m\}$ from the begin of a set of coordinators of network $K = \{k_1, \ldots, k_m\}$ (for begin $n = 1$).

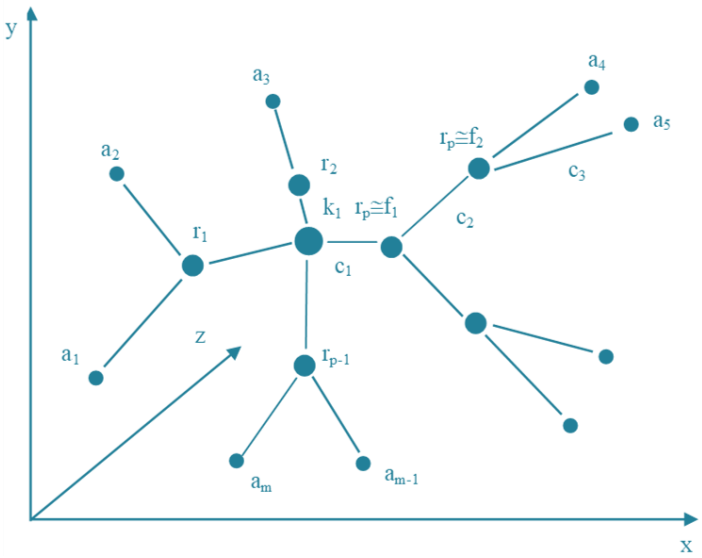

Figure 7: Model of end topology WSN (primary information sources)

Distance between points $a(x_i, y_i, z_i)$ and $b(x_j, y_j, z_j)$ equals:

$$c_{ij} = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2 + (z_i - z_j)^2}.$$

There are a set of such distances $C = \{c_{11}, \ldots, c_{m1}, \ldots, c_{1n}, \ldots, c_{mn}\}$. The distance between the nodes should not exceed the maximum data transmission range. We will assume that the maximum transmission range between any WSN nodes is the same and equal to $c_{\max}$.

5. Simulation and benefits

The monitoring system based on this approach and developed software technical complex can be switched in following four operation modes in critical infrastructures (based on cybersecurity requirements [10-12] from international standards and best practices):

Normal (standard operation, normal operation). The tasks of normal operation consist of emergency planning, the main purpose of which is to gather information to predict the possible occurrence and development of the crisis regime and control its consequences, determine the resources of telecommunications networks and tools needed to resolve crises, develop special forecasts to respond effectively in anticipation of the problem, taking into account all the forces and means to implement the objectives. In this mode, regulatory, legislative and other mechanisms aimed at minimizing the risk and damage from the crisis are identified and created.

Increased preparedness (non-standard operation, active preparation, and practical implementation of several preventive/precautionary measures). To do this, collect and use in the monitoring system data on the state of internal and external structure, data for current and retrospective analysis with the possibility of preventive planning of trends in the current situation, as well as planning resources, forces, and means necessary to neutralize, stabilize and reduce the severity of the consequences of the crisis. Lack of necessary information often becomes a major obstacle to the functioning of the monitoring system to prevent possible consequences. In many cases, this is due to untimely provision of data, detection, and use of the necessary resources of interconnected, sensory means and telecommunications networks of different operators.

Crisis (actions in a crisis situation). In a crisis mode, the monitoring system should provide a real-time operational mode. Tasks must be implemented on a limited time interval quickly and continuously. In the event of crisis situations in the monitoring system, there may be problems of peak load on all elements, in connection with which they may significantly exceed the functional limitations for their use.

Post-crisis (elimination of long-term consequences of the crisis regime). The post-crisis regime is transitional to the usual and includes analysis of the crisis situation, features for its elimination, modification of the content of databases and knowledge bases, and restoration of normal modes of operation of the components of the monitoring system [13].

Utilizing IoT performance monitoring solutions, businesses may get observable outcomes [14], like:

- Gain a thorough grasp of all IoT ecosystem components and real-time data. You will be able to enhance the standard of customer service, address issues, and other things.
- Recognize the data transmission rate, the locations of the delays, and the locations of these bottlenecks.
- Data gathering and analysis. Analyze a wide range of Internet-based IoT data from linked devices, customers, and applications.
- Filling up performance gaps. Enhance the functionality of several apps, APIs, networks, and protocols.
- A real-time warning system. Receive warnings of issues before they have a substantial impact on your business.
- Increased resource efficiency and longer equipment service life. The sensors must detect equipment issues since limited awareness of equipment deterioration might result in expensive replacement [15].

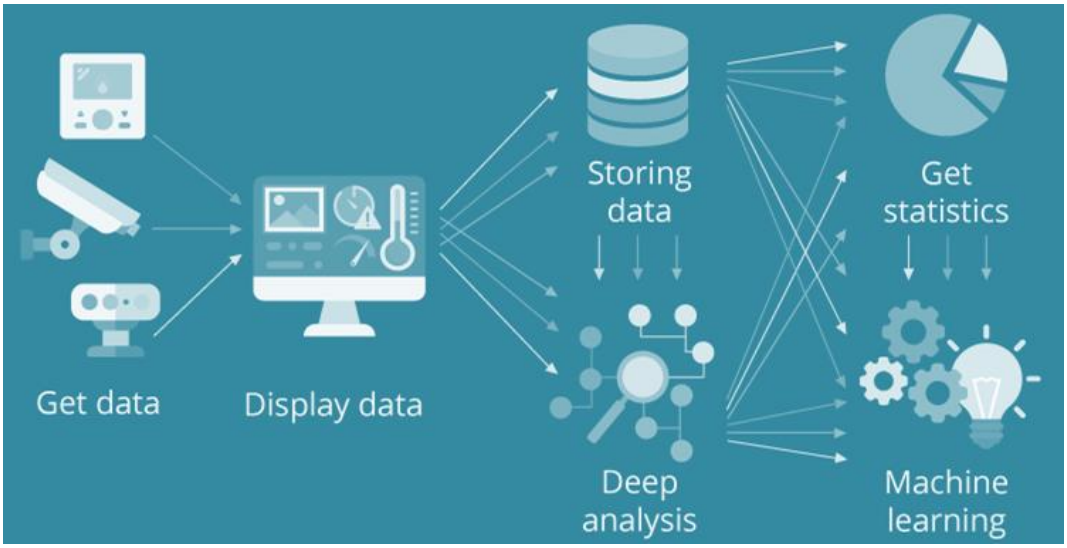

Figure 8: Scheme of cloud IoT monitoring ecosystem

The following requirements must be met by an efficient IoT performance management and monitoring system [16-18]:

- ability to manage all new devices, independent of the communication standard or performance metrics; the capacity to handle the rapid development of traffic and data quantities;
- ability to operate simultaneously with IPv4 and IPv6 protocols;
- visibility of traffic in each segment with an accuracy of seconds;
- one-screen administration of a hybrid cloud system includes physical and virtual KPIs for all monitoring levels.

Following the recommendations of E.430, E.800, X.134, and other documents of the International Telecommunication Union, the Quality of Service (QoS) is understood as a generalized (integral) beneficial effect of the service, which is determined by the degree of satisfaction the user both from the received service and from the service system itself. The QoS criterion in the telecommunications business is usually determined by a set of indicators of the properties of both the provided telecommunications service and the network resources used. Service quality indicators are called service QoS parameters, and network resource quality indicators are called network performance parameters (NP). To quantify most of the properties of the quality of telecommunications services defined in the recommendations of TL 9000 and E.800, the corresponding indicators are introduced, which are determined based on the performance characteristics (parameters) of the network. The analysis of recommendations I.350 showed that the quality of the provided telecommunication services is ensured at three stages [18-20]:

1. access to information transfer (connection establishment);
2. transfer of user information;
3. termination of the information transfer session (disconnection).

6. Conclusions

In the paper IoT concepts and requirements were analyzed, advantages and disadvantages were defined as well as benefits for companies were declared. Main standards and best practices in different aspects of IoT implementation were analyzed in this study.

Based on the developed mathematical models of WSN, model studies were conducted to verify the theoretical dependences of the collision probability basis of the collision probability modeling, which allowed to verification of the proposed models. Cloud-based monitoring information technology was further developed, which through the use of stochastic models of wireless sensor networks and advanced monitoring methods, allowed to development of software and hardware monitoring of real-time environmental parameters in real real-time IoT concepts. This complex of real-time environmental parameters monitoring can be used as a prototype for the organization of monitoring in dynamically changing environments and the event of various critical situations. It can be effectively implemented in various critical infrastructures for both cybersecurity and physical security parameters monitoring.

The next steps will be related to software realization of the proposed models for cloud IoT-based monitoring system realization in the critical infrastructures.

7. References

[1] ITU-T Y. 2060 “Overview of the Internet of Things”, 06/12.

[2] S. Gnatyuk, Critical Aviation Information Systems Cybersecurity. Meeting Security Challenges Through Data Analytics and Decision Support, NATO Science for Peace and Security Series, D: Information and Communication Security, IOS Press Ebooks, volume 47(3), 2016, 308-316.

[3] M. Kalimoldayev, S. Tynymbayev, M. Ibraimov et al, The device for multiplying polynomials modulo an irreducible polynomial, News of the National Academy of Sciences of the Republic of Kazakhstan, Series of Geology and Technical Sciences 2(434) (2019) 199-205.

[4] A. Roukounaki, S. Efremidis, J. Soldatos, J. Neises, T. Walloschke and N. Kefalakis, “Scalable and Configurable End-to-End Collection and Analysis of IoT Security Data: Towards End-to-End Security in IoT Systems, in: Global IoT Summit (GIoTS), Aarhus, Denmark, 2019, pp. 1-6, doi: 10.1109/GIOTS.2019.8766407.
[5] W. Iqbal, H. Abbas, M. Daneshmand, B. Rauf, Y. A. Bangash, An In-Depth Analysis of IoT Security Requirements, Challenges, and Their Countermeasures via Software-Defined Security, IEEE Internet of Things Journal 7(10) (2020) 10250-10276. doi: 10.1109/JIOT.2020.2997651.
[6] F. T. Jaigirdar, C. Rudolph and C. Bain, Prov-IoT: A Security-Aware IoT Provenance Model in: 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Guangzhou, China, 2020, pp. 1360-1367. doi: 10.1109/TrustCom50675.2020.00183.
[7] S. Sarvaiya, D. N. Satange, Security in IP-Based IoT Node and Device Authentication, in: 2022 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS), Pune, India, 2022, pp. 1-5. doi: 10.1109/ICBDS53701.2022.9935920.
[8] N. M. Karie, N. M. Sahri, W. Yang, C. Valli, V. R. Kebande, A Review of Security Standards and Frameworks for IoT-Based Smart Environments, IEEE Access 9 (2021) 121975-121995. doi: 10.1109/ACCESS.2021.3109886.
[9] New security obligations for Australian Critical Infrastructure Providers. URL: https://privacy108.com.au/insights/new-security-obligations-critical-infrastructure-providers/#_ftn16.
[10] S. Gnatyuk, B. Akhmetov, V. Kozlovskyi et al., New Secure Block Cipher for Critical Applications: Design, Implementation, Speed and Security Analysis, Advances in Intelligent Systems and Computing 1126 (2020) 93-104.
[11] M. Iavich, T. Kuchukhidze, S. Gnatyuk, A. Fesenko, Novel certification method for quantum random number generators, International Journal of Computer Network and Information Security 13(3) (2021) 28-38.
[12] S. Gnatyuk, Z. Hu, V. Sydorenko, M. Aleksander, Yu. Polishchuk, Kh. Yubuzova, Critical aviation information systems: Identification and protection, Cases on Modern Computer Systems in Aviation (2019) 423-448.
[13] S. Holub, N. Khymytsia, M. Holub, S. Fedushko, The intelligent monitoring of messages on social networks, CEUR Workshop Proceedings 2616 (2020) 308-317. URL: https://ceur-ws.org/Vol-2616/paper26.pdf.
[14] How Beneficial is IoT in Monitoring for Your Business Performance?. URL: https://www.altamira.ai/blog/iot-monitoring.
[15] A. K. Singh and P. Kumar, “Advancement in Quality of Services in Wireless Sensor Networks,” 2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU), 2018, pp. 1-5, doi: 10.1109/IoT-SIU.2018.8519842.
[16] L. Hernández-Alpizar, A. Carrasquilla-Batista, L. Sancho-Chavarría, Monitoring adjustment based on current data of an IoT-COTS monitor for environmental chemical analysis, in: 2021 IEEE 12th Latin America Symposium on Circuits and System (LASCAS), 2021, pp. 1-4. doi: 10.1109/LASCAS51355.2021.9459119.
[17] A. Carrasquilla-Batista, A. Chacón-Rodriguez, M. Solórzano-Quintana, M. Guerrero-Barrantes, IoT applications: On the path of Costa Rica's commitment to becoming carbon-neutral, in: 2017 International Conference on Internet of Things for the Global Community (IoTGC), 2017, pp. 1-6.
[18] M. Karpmski, P. Raif, S. Rajba, T. Rajba and V. Martsenyuk, Wireless sensor networks with randomized parameters, in: 2016 16th International Conference on Control, Automation and Systems (ICCAS), 2016, pp. 1470-1475. doi: 10.1109/ICCAS.2016.7832497.
[19] M. O. Onibonoje, An IoT Design Approach to Residential Energy Metering, Billing and Protection, in: 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), 2021, pp. 1-4. doi: 10.1109/IEMTRONICS52119.2021.9422580.
[20] Z. Hu, S. Gnatyuk, T. Okhrimenko, S. Tynymbayev, M. Iavich, High-speed and secure PRNG for cryptographic applications, International Journal of Computer Network and Information Security 12(3) (2020) 1-10.