DOI 10.1007/s10559-020-00279-w
Cybernetics and Systems Analysis, Vol. 56, No. 4, July, 2020

MATHEMATICAL TOOLS FOR THE INTERNET OF THINGS ANALYSIS

G. Mamonova[1] **and N. Maidaniuk**[2]

UDC 004.02

Abstract. *An overview of recent publications on the use of mathematical methods and models for the analysis of the Internet of Things is given. It is shown that IoT modeling uses such sections of mathematics as game theory, probability theory, theory of random processes, Boolean and matrix algebra, graph theory, number theory, complex variable theory, measure theory, optimization theory, simulation modeling, cluster analysis, and numerical and mathematical analysis.*

Keywords: *Internet of Things, methods, models, modeling, technologies, structure, system.*

Recently, the term "Internet of Things (IoT)" has been widely used not only by information technology professionals but also in everyday life.

The term IoT was first coined by British researcher and entrepreneur Kevin Ashton. In the late 1990s, Ashton studied radio frequency identification (RFID). This technology implies small sensors attached to objects that contain important information and allow you to read it remotely using the Internet. Ashton coined the term to illustrate the RFID capabilities used in enterprise supply systems. One of the tasks was to count the goods and track their movement without human intervention. Today, the term IoT is most commonly used to describe scenarios in which Internet connections and computing power extend to many objects, devices, and sensors.

Today, the term IoT refers to a network consisting of interconnected physical objects or devices that have built-in sensors. It is also associated with software that allows transferring and exchanging data between the physical world and computer systems, using standard communication protocols. In addition to sensors, the network may have actuators built into physical objects and interconnected through wired and wireless networks. These interconnected objects have the ability to read and activate, program and identify, as well as prevent human participation using smart interfaces.

It is impossible to analyze the features of modeling and implementation of IoT technologies, as well as the main technical characteristics of the devices they use without the use of mathematical methods and programming models.

The scientific achievements of domestic and foreign scientists, theorists and practitioners, who study IoT, use a certain mathematical apparatus. Only in the last decade have scientists begun to actively analyze the work of the IoT and apply a wide range of mathematical methods and models. The systematization of the specified methods and models for the analysis of the mathematical apparatus used to model work of IoT technologies is worth the attention.

The physical security system for the region infrastructure, based on the functioning of IoT technologies, is considered in [1]. There the set-theoretical model of functions, components and failures of the investigated system is used, and hierarchical structure of failures of the basic structural elements of physical security system is projected. Diagram IDEF0 (function modeling methodology and graphical notation) is designed to formalize and describe business processes and shows a scenario of accidental or intentional power outage in the lighting and video surveillance subsystems. In this work, models and methods of risk analysis of physical security systems are developed.

[1]Kyiv National Economic University named after Vadym Hetman, Kyiv, Ukraine, *mamonova@kneu.edu.ua*. [2]International Scientific and Training Center of Information Technologies and Systems, National Academy of Sciences of Ukraine and Ministry of Education and Science of Ukraine, Kyiv, Ukraine, *n.maydanyuk@ukr.net*. Translated from Kibernetika i Sistemnyi Analiz, No. 4, July–August, 2020, pp. 119–127. Original article submitted October 26, 2019.

The authors of [2] argue that when ensuring the innovative development of machine-building enterprises in the Industry 4.0 framework, it is necessary to use mathematical models that will correspond to the technologies of machine vision, robotic technology, automated and smart production, and control systems within cyber-physical systems at enterprises. According to the authors of [2], such cyber-physical systems should be connected to the outer world through sensors and actuators that allow receiving data streams from the physical world, installing and continuously updating the virtual twin of the physical world and providing interaction in reality according to instructions from the virtual world. The presented classes of mathematical models for cyber-physical systems are proposed to be used in accordance with innovations in machine-building enterprises. This will automate manual labor, update already used innovative technologies, and integrate them in a single information space.

The main problem encountered when developing applications for the Internet of Things is the optimal use of energy resources, in particular the shelf life of IoT batteries. The method proposed by scientists from Greece [3] was used to analyze the characteristics of the parameters that affect energy consumption and to verify the energy consumption of IoT devices. Special requirements are placed on the system energy efficiency (for example, the service life of the construction management system). This approach allows you to detail the formal idea of how the system behave and its subsequent verification, which provides feedback for improvement before deployment or direct production.

Narrowband Internet of Things (NB-IoT) is a promising low-power network (LPWN) technology standardized by 3rd Generation Partnership Project (3GPP) “Release-13” as part of the upcoming fifth generation (5G) wireless system. The main goal of NB-IoT development was to enhance radio coverage by repeating the signal over an additional period. The paper [4] provides a brief overview of NB-IoT technology, including deployment options, physical channels and signals, uplink resource grid structure, and resource unit configuration. In this paper, a system model for the NB-IoT uplink based on the 3GPP Release-13 specification is developed. The effectiveness of the proposed NDMRS auxiliary channel evaluators in comparison with others was also investigated using extensive computer modeling at the channel level.

The feasibility of using an IoT-based management platform to provide real-time feedback data was investigated in [5]. The authors suggest this will increase the efficiency of spectrum use and energy consumption by creating a broadcasting network with adaptive radiated power. This paper presents a network architecture that includes an IoT feedback loop. This network is designed and optimized to ensure minimum electricity consumption and efficient infrastructure. In addition, a new indicator of its efficiency has been proposed to assess the improvement in spectrum use.

In the age of technology, when you need a connection between computers, the Internet of Things and various IoT-based applications, they are more efficient than a wireless touch network. According to the authors of [6], the rapid development of technology in general and IoT in particular requires the efficient use of energy and communications. Interaction between different devices at different levels requires grouping and using a cluster approach. The authors presented the pragmatic IoT architecture and proposed two clustering algorithms: based on heuristic and graphical approaches that allow bottom-up and top-down clustering depending on the need for IoT. The algorithms are evaluated using a number of standard parameters and compared with existing algorithms, and the multilevel IoT structure provides a hierarchical structure for efficient connection.

A thorough analysis of the traffic of “smart” devices used in the development of smart systems was conducted in [7], which revealed significant differences in the main characteristics of traffic of similar devices from different manufacturers. This paper notes the lack of generally accepted standards for building smart networks and in some modes of their operation shows the impossibility of predicting traffic jumps, which significantly complicates the modeling of smart systems. The authors pointed to the need for in-depth analysis of the data, which will give a fuller picture of how these devices operate and the feasibility of building a simulation model of the IoT device network with further complication and increase in the number of nodes.

Modern approaches to the creation of a single information space of industrial complexes to determine the methodology that will more fully consider the information and communication links of modeling systems are given in [8]. Based on the SADT methodology (Structured Analysis and Design Techniques), an information IDEF0 model of smart enterprise development has been developed, which, according to the authors, will provide a complete picture of the relevant processes. Note that the above approach considers the logical relationship between the works, rather than their sequence in time.

A group of researchers in [9], after analyzing the use of IoT, pointed to significant problems associated with confidentiality. This, according to the authors, leads to a loss of control over the collection and transmission of data. Confidentiality is a key requirement in any IoT ecosystem, and its violation inhibits the widespread use of the Internet of Things. First, the authors assess the issue of confidentiality in IoT systems and express concern about the limited resources, in particular personal data, which are directly transmitted from sensors to the outer world. Second, they describe the proposed IoT solutions, which cover various problematic aspects of confidentiality, such as identification, tracking, monitoring and profiling. The authors consider mechanisms and architectures for IoT data protection in case of device mobility, as well as for platform and application layer infrastructure [9].

Researchers from Greece [10] reviewed the available network communication technologies for IoT, paying attention to encapsulation and routing protocols. The paper also investigates the relationship between IoT network protocols and its new applications. A thorough taxonomy of protocols based on network layers is proposed, while network protocols are suitable and operate for addressing.

A study of software for the development of a smart health care system based on IoT was conducted in [11]. Based on various technological standards and communication protocols, the requirements for the IoT system are analyzed, which is the basis for the development of appropriate platforms. The proposed model consists of three levels, and each performs a specialized task. The authors are confident in the effectiveness of smart health services, especially in underdeveloped countries and rural areas.

The architecture, which is the basis for the development of light microservices based on socially connected web objects for the implementation of SIoT (Social Internet of Things) services, was studied in [12]. The proposed paper analyses the model of social relations, which allows for effective identification of web objects and eases provision of services. The model of semantic ontology is developed for realization of compatible social interaction between heterogeneous objects.

In 2016, the European Parliament adopted the General Data Protection Regulation (GDPR), which directly concerns the IoT in terms of security and confidentiality of user data. The study [13] analyzes IoT processing of personal information and investigates the direct impact of GDPR on IoT. Given the GDPR, the economic impact of the IoT industry on the value of firms is analyzed using the Gordon–Loeb model. It is also investigated which industries are vulnerable to these legislative changes.

A new stand-alone security structure, represented by an effective network traffic filtering system for virtualized and multitasking NB-IoT networks with 5G support, is described in [14]. This paper argues that the proposed security structure and filtering system can significantly mitigate attacks by dynamically collapsing and loading thousands of filtering rules into a Firewall that has the appropriate number of NB-IoT devices.

Modern security problems in the IoT network and their classification are considered in [15]. It addresses in more detail the issues of privacy, light cryptographic structures, secure routing and forwarding, reliability and stability of management, denial of service, and detection of insider attacks. According to the authors, confidentiality is crucial in IoT because the characteristics of such a network are significantly different from a typical Internet. In this paper, it is proposed to use such visualization technology as Software Defined Networking (SDN). The use of SDN involves centralization of network monitoring, which in turn will ensure the coordinated provision of services.

The study [16] considers the following evaluation models for probabilistic-time characteristics of information interoperability in the Internet of Things: simulation model of information interoperability in the Internet of Things based on a multi-agent approach; access models in “fog computing” with the permitted collisions of data sources in the temporal domain, which implement polling, interruption, multiple access modes, respectively. The proposed models can be used at the initial stages of IoT design.

With the availability of the Internet through probing and automation, network interactions are becoming more critical and secure and require improved security tools to design and test system components, platforms, and services. Many chaotic, heterogeneous data passes through such networks. The study [17] argues that the theory of categories (the field of abstract mathematics) provides a conceptual basis for information modeling of IoT.

When developing wireless sensors and environments for many application areas (e.g., environmental, medical, “smart” interconnected vehicles and trucks, and “smart” buildings), the requirements for the transmission of many different scales of heterogeneous data are considered, for which it is necessary to build effective strategies for mathematical modeling of the measured data. The study [18] considers these topical problems and describes a number of design methodologies, which are used for known functions in autonomous IoT (smart mining industry, smart reliable sounding, closed (network) control, and energy efficiency).

TABLE 1

Source Number	Mathematical Apparatus	The Purpose of Modeling (Main Task)	Prospects for Further Research
1	2	3	4
[1]	Boolean algebra, matrix algebra, expert evaluation, probability theory	Develop structural and functional decomposition of the physical security system, find applied solutions for the implementation of structural functions of subsystems in the physical security system; analyse a set-theoretic model of components, environment and physical security system	Given that the model describes a static situation, it is proposed to consider the attack to study the dynamic model
[3]	Probability theory, graph theory	Create a model of energy consumption in IoT systems and devices that are their components to improve energy efficiency (the model is illustrated by the example of a building management system)	Remote control in the building and its impact on total energy consumption
[4]	Number theory, complex variable theory, probability theory and mathematical statistics, matrix algebra	Build NDMRS-enabled channel evaluation algorithms and test their efficiency in terms of bit-rate error associated with signal–noise ratio	Analysis of carrier frequency offset and receiver diversity to improve the performance of NB-IoT systems
[5]	Measure theory, optimization theory	Develop a model of energy consumption of a broadcast network (to take into account the energy consumption of a radio station, four main components of energy consumption are considered: optical receiver, modulator, high power amplifier, and cooling)	Emulation of a dynamic broadcast network with an IoT feedback loop with a real scenario
[6]	Graph theory, set theory, cluster analysis	Build two clustering algorithms based on the heuristic method and graph theory (proposed clustering approaches are evaluated on the IoT platform using standard parameters and compared with different approaches)	Extension of the proposed algorithm to the IoT cloud; increasing the number of model parameters and determining the characteristics of heuristic or graph edges for clustering, depending on the application
[7]	Simulation modeling, probability theory	Build a plausible simulation model for predicting traffic spikes	In-depth analysis of the data obtained to build a simulation model of a network of IoT devices with further complications and increasing the number of nodes
[12]	Graph theory	To evaluate the performance of the semantic model of ontology developed by operating services	Overcoming monolithic approaches, microservices that can independently create new service functions
[14]	Optimization theory	Minimize the negative consequences of cyberattacks	Overcoming extremely undesirable self-organizational opportunities in the network to provide virtualized, multilateral IoT 5G-based traffic
[16]	Probability theory, mathematical statistics, theory of random processes, simulation modeling, numerical analysis	Evaluate the temporal characteristics of information interoperability in the IoT network. Find the dependence of time characteristics on the parameters of the IoT network	Calculation of expressions, algorithms, and models required at the early stages of designing the Internet of Things
[18]	Theory of random processes, optimization theory	Develop a design methodology used for functions in autonomous IoT	Creating an energy-efficient, reliable, and integrated IoT system

Table 1 continued

1	2	3	4
[21]	Probability theory, graph theory, optimization theory	Develop a message modification algorithm for reliable storage of information	Establishment of cryptographically secure connections between IoT devices, which requires prior consensus with the secret encryption key
[22]	Mathematical analysis, optimization theory	Build algorithms for Big Data analytics	Development of practical and efficient algorithms for specific applicable IoT programs, to ensure a reasonable allocation of resources, automatic network operation, and smart service delivery
[23]	Game theory, graph theory	Analyze mathematical methods and models of IoT	Finding a balance between the problems of technical and non-technical research

According to the authors of [19], there are two main problems associated with scaling and a high level of detail when modeling the Internet of Things. Technical solutions to avoid these problems are in conflict. This paper presents an overview of existing modeling methods and, on the basis of the analysis, proposes the use of adaptive, agent, parallel, and distributed modeling in combination with multilevel and hybrid approaches. IoT modeling allows evaluating strategies for deployment of smart services in different domains of simulated areas.

IoT devices are limited in resources and cannot use traditional key distribution schemes. As a result, there is a growing interest in the local generation of secret random keys using the common randomness of the communication channel. The study [20] presents the SKYGlow secret key generation scheme that is focused on IoT platforms with limited resources and tested on IEEE 802.15.4 devices.

Numerous methods of IoT data analysis are considered in [21] to solve practical problems and tasks. It is proposed to take into account three facts when applying analytical algorithms to smart data. First, various applications in IoT and smart cities have their own features, such as the number of devices and the types of data they generate. Second, the data obtained will have specific features that should be taken into account. Third, the taxonomy of algorithms is another important aspect in applying analysis to smart data. Analytical data make it easy to select the appropriate algorithm to solve a particular problem.

Thorough analysis of massive analytical data on their heterogeneous, non-linear, high-dimensional, distributed, and parallel processing was performed in [22]. Here are systematic guidelines for developing efficient algorithms for Big Data analysis in IoT. Algorithms are grouped into four classes: various data processing; non-linear data processing; multidimensional data processing; distributed and parallel data processing.

The paper [23] presents a broad overview of operations research methods for IoT analysis. The paper analyses 144 publications and systematizes the methods and approaches used in IoT modeling.

Note that [2, 8–11, 13, 15, 17, 19] mostly announce the use of mathematical methods but give no specific mathematical formulas and calculations.

Table 1 contains systematized information on mathematical theories, methods, and models used in the works considered, namely, the purpose and main tasks set by the authors of these works, and the prospects for further research.

The term IoT and the English adjective “smart” have been often used in the Ukrainian language recently. The number of devices that capture relevant information has increased many times, and the amount of data generated by smart devices has increased by an order of magnitude. It is clear that the use of mathematical methods and models is necessary for the analysis, efficient operation, and forecasting of the complex Internet of Things system. It requires a sufficient level of theoretical knowledge in certain disciplines of the mathematical cycle. The article presents an overview of recent publications on the use of mathematical methods and models for IoT analysis. It is shown that IoT modeling uses such sections of mathematics as game theory, probability theory, theory of random processes, Boolean and matrix algebra, graph theory, number theory, complex variable theory, measure theory, optimization theory, simulation modeling, cluster analysis, numerical analysis, and mathematical analysis. This work will be useful for scientists, practitioners interested in IoT, and for teachers of higher education institutions, who train IT specialists.

REFERENCES

1. Ahmed Waleed Al-Khafaji, "Development of PSMECA analysis technique applying IoT components in physical security systems," Radioelectronic and Computer Systems, No 3(87), 63–73 (2018). http://doi.org/10.32620/reks.2018.3.07.
2. O. F. Tarasov and S. S. Turlakova, "Mathematical modelling of advanced engineering technologies for smart enterprises: An overview of approaches and ways of implementation," Economy of Industry, No. 3 (83), 57–75 (2018). http://doi.org/10.15407/econindustry2018.03.057.
3. A. Lekidis and P. Katsaros, "Model-based design of energy-efficient applications for IoT systems," in: S. Bliudze and S. Bensalem (eds.), Methods and Tools for Rigorous System Design (MeTRiD 2018) EPTCS 272, (2018) pp. 24–38. http://doi.org/10.4204/EPTCS.272.3.
4. Md Sadek Ali, Y. Li, Md Kh. H. Jewel, O. J. Famoriji, and F. Lin, "Channel estimation and peak-to-average power ratio analysis of narrowband internet of things uplink systems," Wireless Communications and Mobile Computing, Vol. 2018, Article ID 2570165 (2018). https://doi.org/10.1155/2018/2570165.
5. R. M. Alonso, D. Plets, E. F. Pupo, M. Deruyck, L. Martens, G. G. Nieto, and W. Joseph, "IoT-based management platform for real-time spectrum and energy optimization of broadcasting networks," Wireless Communications and Mobile Computing, Vol. 2018, Article ID 7287641 (2018). https://doi.org/10.1155/2018/7287641.
6. J. S. Kumar and M. A. Zaveri, "Clustering approaches for pragmatic two-layer IoT architecture," Wireless Communications and Mobile Computing, Vol. 2018, Article ID 8739203 (2018). https://doi.org/10.1155/2018/8739203.
7. O. N. Lodneva and E. P. Romasevich, "Analysis of devices traffic of the Internet of Things," Modern Information Technology and IT-Education, Vol. 14, No. 1, 149–169 (2018). https://doi.org/10.25559/SITITO.14.201801.149-169.
8. S. S. Turlakova, "Information and communication technologies for the development of "smart" industries," Economy of Industry, No. 1(85), 101–123 (2019). https://doi.org/10.15407/econindustry2019.01.101.
9. M. Seliem, Kh. Elgazzar, and K. Khalil, "Towards privacy preserving IoT environments: A survey," Wireless Communications and Mobile Computing, Vol. 2018, Article ID 1032761 (2018). https://doi.org/10.1155/2018/1032761.
10. A. Triantafyllou, P. Sarigiannidis, and T. D. Lagkas, "Network protocols, schemes, and mechanisms for Internet of Things (IoT): Features, open challenges, and trends," Wireless Communications and Mobile Computing, Vol. 2018, Article ID 5349894 (2018). https://doi.org/10.1155/ 2018/5349894.
11. M. Pasha and S. M. W. Shah, "Framework for E-health systems in IoT-based environments," Wireless Communications and Mobile Computing, Vol. 2018, Article ID 6183732 (2018). https://doi.org/10.1155/2018/6183732.
12. S. Ali, M. G. Kibria, M. A. Jarwar, H. K. Lee, and I. Chong, "A model of socially connected web objects for IoT applications," Wireless Communications and Mobile Computing, Vol. 2018, Article ID 6309509 (2018). https://doi.org/10.1155/2018/6309509.
13. J. Seo, K. Kim, Mookyu Park, Moosung Park, and K. Lee, "An analysis of economic impact on IoT industry under GDPR," Mobile Information Systems, Vol. 2018, Article ID 6792028 (2018). https://doi.org/10.1155/2018/6792028.
14. P. Salva-Garciamailto, J. M. Alcaraz-Calero, Q. Wang, J. B. Bernabe, and A. Skarmeta, "5G NB-IoT: Efficient network traffic filtering for multitenant IoT cellular networks," Security and Communication Networks, Vol. 2018, Article ID 9291506 (2018). https://doi.org/10.1155/2018/9291506.
15. S. Hameed, F. I. Khan, and B. Hameed, "Understanding security requirements and challenges in internet of things (IoT): A review," J. of Computer Networks and Communications, Vol. 2019, Article ID 9629381 (2019). https://doi.org/10.1155 /2019/9629381.
16. M. A. Elizarov, " Models and algorithms of information interaction in Internet of Things networks," Author's Abstracts of Ph.D. Theses, St. Petersburg (2017).
17. S. Breiner, E. Subrahmanian, and R. D. Sriram, "Modeling the internet of things: A foundational approach," in: WoT'16: Proc. of the Seventh International Workshop on the Web of Things (Stuttgart, Germany, November 2016), (2016), pp. 38–41. http://doi.org/10.1145/3017995.3018003.

18. P. Bogdan, M. Pajic, P. P. Pande, and V. Raghunathan, “Making the Internet-of-things a reality: from smart models, sensing and actuation to energy-efficient architectures,” in CODES’16: Proc. of the Eleventh IEEE/ACM/IFIP International Conference on Hardware/Software Codesign and System Synthesis (Pittsburgh, Pennsylvania, October 2016), Article No. 25 (2016). http://doi.org/10.1145/2968456.2973272.
19. G. D’Angelo, S. Ferretti , V. Ghini, “Modeling the Internet of Things: A simulation perspective,” arXiv:1707.00832v2 [cs.DC], 20 Sep 2017. URL: https://arxiv.org/abs/1707.00832v2.
20. G. Margelis, X. Fafoutis, G. Oikonomou, R. Piechocki, T. Tryfonas, and P. Thomas, “Efficient DCT-based secret key generation for the Internet of Things,” Ad Hoc Networks, Vol. 92, 101744 (2019).
21. M. S. Mahdavinejad, M. Rezvan, M. Barekatain, P. Adibi, P. Barnaghi, and Amit P. Sheth, “Machine learning for Internet of Things data analysis: A survey,” Digital Communications and Networks, Vol. 4, Iss. 3, 161–175 (2018).
22. G. Ding, L. Wang, and Q. Wu, “Big data analytics in future Internet of things,” arXiv:1311.4112v1 [cs.DC], 17 Nov 2013. URL: https://arxiv.org/abs/1311.4112.
23. P. J. Ryan and R. B. Watson, “Research challenges for the Internet of things: What role can or play?” Systems, Vol. 5, Iss. 24 (2017). http://doi.org/10.3390/systems5010024.