UDC 004.383.8:004.422 **doi: 10.26906/SUNZ.2025.4.98-102**

Nina Kuchuk[1], Maksym Tregubenko[1], Danylo Kovalenko[1], Dmytro Lysytsia[2], Oleksandra Bellorin-Herrera[2]

[1] Kharkiv National University of Radio Electronics, Kharkiv, Ukraine
[2] National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine

RESEARCH OF DISTRIBUTED DATA EXCHANGE TECHNOLOGIES IN THE CONTEXT OF INTELLIGENT TRANSPORT SYSTEMS

Abstract. The article presents the results of a study of distributed data exchange technologies aimed at ensuring effective interaction between components of intelligent transport systems (ITS). Modern approaches to the organization of decentralized information transmission networks are considered, in particular, the use of the concepts of distributed registries, peer-to-peer protocols, and service-oriented architectures. An analysis of the requirements for reliability, latency, and bandwidth of communication channels, which are critical for data exchange scenarios between vehicles and infrastructure, is conducted. Based on a comparative analysis, the advantages and limitations of existing technological solutions in the context of ensuring security, scalability, and fault tolerance are determined. The results of the study can be used to design adaptive traffic management models and develop intelligent interaction modules in new generation transport networks.

Keywords: intelligent transportation systems; distributed data exchange; decentralized networks; distributed ledger; scalability; data transmission reliability.

Introduction

With the continuous development of information technology, which facilitates the creation of complex computing systems solving diverse problems, data communication networks play a key role in ensuring fault tolerance and operational stability. Many components of modern information systems generate their own information flow, requiring processing and distribution to other devices across the network. Prioritizing traffic, balancing, and accounting for peak load periods dictate specific requirements for the technologies used, based on the computing resources expended, memory, volume, and processing and transmission speed requirements for the network traffic they generate. Furthermore, considerable attention is paid to ensuring the security and transparency of certain information system activities, to monitor incidents and potential malicious threats, as well as to guarantee the integrity of data (or the recording of the date and volume of these changes). Blockchain technology can meet many of the requirements for secure and resilient data systems; however, in the vast majority of cases, it requires excessive computing resources, which are critical when using variations of the most popular consensus algorithms. However, there are more computationally lenient consensus algorithms, the continuous use of which also introduces a number of limitations: requirements for creating trusted network sections, delays in communication sections, or ensuring a fully connected system where each network node is directly connected to all other nodes. This encourages the creation of a variety of consensus algorithms with their own characteristics to solve specific problems, which is due to different goals and use cases [1]. For example, financial applications may require high transaction speeds, while data storage systems may emphasize security and reliability. This requires the development of specialized consensus algorithms adapted to specific needs [2]. Given the characteristics of modern heterogeneous communication networks, the lack of flexibility in transmitting blockchain traffic is one of the key reasons for not implementing it. Thus, a system for regulating the volume and speed of blockchain traffic throughout the day would ensure the required flexibility for all situations—more frequently when blockchain traffic is not a priority, less frequently when it is, depending on the ultimate goals and implementation. In addition to regulating traffic volumes, computing resource requirements should also be considered. Modern communication networks consist of components with varying computing power, the primary task of which is data processing and transmission. Under current conditions, installing a blockchain client on network components will have a significant impact on equipment and data processing speed, especially during peak hours. Since consensus algorithms largely determine the resource-intensive nature of the computations required to process transactions and generate blocks, regulating them during data processing, taking into account specific network and computing parameters, will allow for flexible decisions about whether to use the most resource-intensive algorithm and switch to a less resource-intensive one during peak loads.

1. Literature analysis

The application and integration of blockchain technology, as a specific implementation of distributed ledger technology, its impact on network characteristics, and applicability issues are discussed in the works of Ukrainian and international scientists V. Buterin, S. Kasahara, Q. Xia, Y. Sun, L. Cocco, and others. Many works are devoted to investigating issues of network traffic distribution and its impact on network characteristics [3], examining the technical maturity of the approach for integration into existing systems [4], and also the security aspects of the technology. A number of scientific papers are devoted to optimization based on research into consensus algorithms [5]. However, the problem of adapting these algorithms to telecommunication network conditions remains understudied, particularly in terms of developing an adaptive algorithm for selecting blockchain consensus on communication networks [6].

2. Main part

To evaluate a number of parameters, as well as the viability of the concept of integrating blockchain technology into modern communication networks and

the IT landscape, a series of experiments were conducted in the context of an intelligent transportation network, since such a network, in its architecture and structure, reflects all the main features important for measurement. For example, the hardware of network sections, the different levels of network activity for data transmission in the context of a large city center and a remote highway in the northern regions.

For this reason, many experiments and testing were conducted specifically under ITS emulation conditions [6]. The main goal of the study is to evaluate the node's operability and its operating speed under the load imposed by the infrastructure elements of the intelligent transportation network concept. To date, various studies have already presented scenarios for transmitting information from automotive and road sensors, but without interaction and integration with the blockchain network. From the standpoint of studying the operability of a classic blockchain node, the most indicative is testing close to load testing of the node, in which the number of requests to it is sufficiently large over a limited period of time. A study [7] assessing traffic intensity at a toll plaza on an Austrian toll road was used as reference data.

These studies revealed the average number of vehicles passing the toll plaza per week at each hour of the day. Table 1 presents the number of vehicles at each hour, as well as the percentage of vehicles passing this section at each hour of the day.

Table 1 – **Correlation between time of day and the number of passing vehicles**

Hours	Number of OBU	OBU %	Hours	Number of OBU	OBU %
0	600	1,65	12	1920	5,26
1	350	0,96	13	2000	5,48
2	250	0,69	14	2200	6,03
3	200	0,55	15	2300	6,31
4	150	0,41	16	2500	6,85
5	100	0,27	17	2900	7,95
6	125	0,34	18	3100	8,5
7	225	0,62	19	3000	8,23
8	1000	2,74	20	2850	7,81
9	2100	5,76	21	1850	5,07
10	2200	6,03	22	1500	4,11
11	2050	5,62	23	1000	2,74
Total number of OBU: 36470					

In this study, it is assumed that each vehicle passing through the toll plaza sends one transaction to a blockchain network node [8]. The transaction sent can contain various information, ranging from the fact of payment, the fact of passage, to the condition of the road surface. The objective of this study is to evaluate the node's performance and the ability to process all incoming transactions without data loss.

Based on the tabular data, a graph was obtained showing the peak values as well as the overall traffic intensity profile after correlating the values 12 times, and is presented in Fig. 1.

Thus, each vehicle sends a transaction based on the received data. To simulate these transactions, the authors developed a Python script. This allows them to simulate network load based on traffic intensity data for the segment in question. The correlation process accelerates the study and, using load testing, evaluates whether the blockchain network node can handle the increased load. The calculations performed accelerated the simulation process. During the study, 1 hour of real time becomes 5 minutes of the study, which also affects the number of vehicles, as shown in Fig. 1. From a script perspective, this simulation also requires multithreading to correctly send transactions according to the obtained load distribution. During transaction sending, the script interacts with the Web3 library API, which enables interaction with a node of a private instance of the blockchain networks under study on the developed simulation rig.

To develop the model rig and conduct further research, two blockchain platforms were used: Ethereum, which operates on the PoW algorithm (as it supports two implementations – PoW and PoS [9]) and Waves, which operates on the LPoS algorithm. Due to the operational specifics of private network instances of the platforms under consideration, two model rigs were organized. The choice of these blockchain networks was motivated by several reasons. These blockchains allow for the organization of private networks based on open source code, enable the launch of smart contracts, as well as the construction of hybrid systems and the creation of solutions with the integration of third-party technologies. The key difference between these blockchain platforms is the underlying consensus algorithms, which impacts the performance of the blockchain network, its security, and the hardware requirements for the node of the organized network. Waves Enterprise is a blockchain platform that enables the creation of various blockchain solutions based on smart contracts. The distributed network infrastructure allows for the execution of a large number of transactions in short periods of time. One of the platform's advantages is the ability to create your own private network using an open jar file containing all the necessary files and configuration data for setting up your

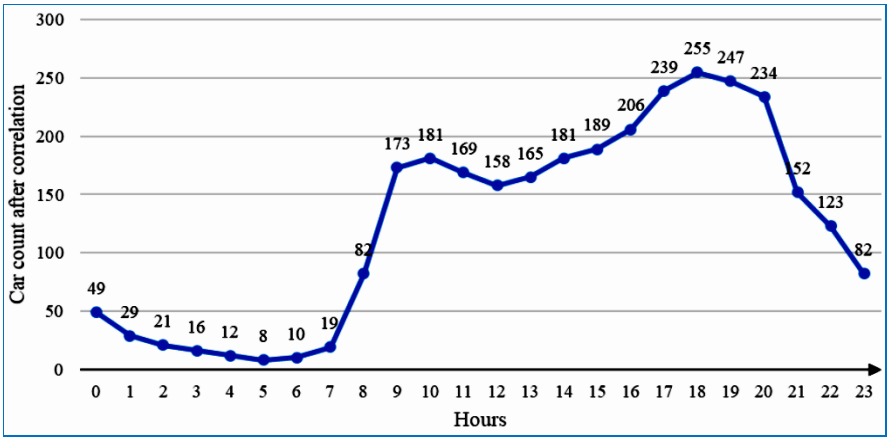

Fig. 1. Calculation of the number of cars in relation to hours after correlation

own node in a closed blockchain network. The Waves blockchain network uses Leased Proof of Stake (LPoS) consensus algorithm. This consensus algorithm does not require energy-intensive computations, unlike the Proof of Work consensus algorithm. The main parameter determining the probability of generating a new block is the amount of platform currency in the node's account. Thus, the amount of currency is analogous to the number of lottery tickets: the more tickets, the higher the chance of winning.

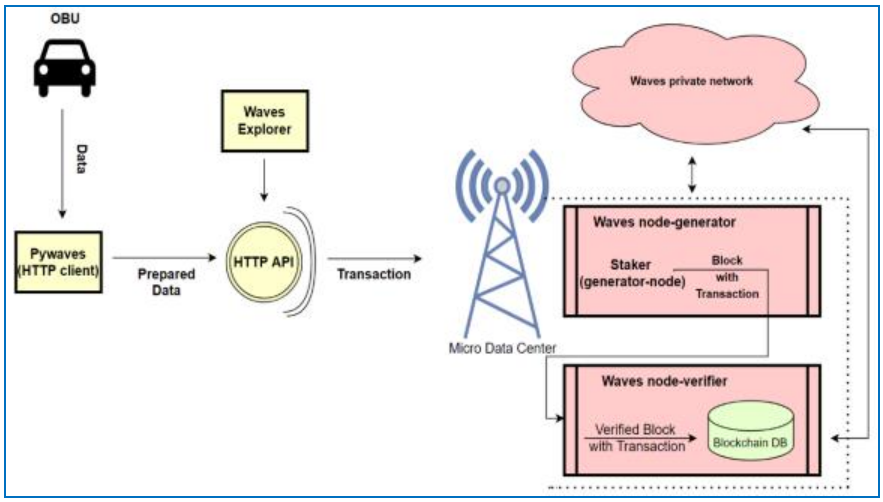

Fig. 2. Model rig for conducting an experiment based on the open blockchain client LPoS Waves

A similar principle applies to the Waves network. A diagram of a simulation using Waves blockchain network nodes is shown in Fig. 2. The Waves model stand consists of the following elements:

− OBU - a user device initiating a transaction based on current data,

− pywaves (HTTP client) - a framework whose main purpose is to interact with the Waves node's HTTP API,

− HTTP API - Waves node software interface, which provides the ability to interact with the Waves node,

− Waves node – A staker (generator node) is the main software node of the Waves blockchain network. It initiates the process of block assembly and transaction processing.,

− Waves node - Verifier - an additional software node of the Waves blockchain network whose main task is to confirm transactions and blocks,

− Waves Explorer, a web interface that allows you to check the current state of nodes and deploy smart contracts, the Waves blockchain network - a private network was created for testing purposes.

The OBU initiates a transaction and transmits its current state to Pywaves. Pywaves, using the received data, creates a transaction request in a format readable by the HTTP interface and sends it to the HTTP API. The HTTP API processes the received request and records information about the attempted transaction on the primary node (the generator node).

The generator node (staker), upon receiving the transaction, sends it for verification to its quorum – a meeting of all nodes in the network –and awaits verification from the verifier node. The generator node, having collected a certain number of verified transactions or having waited a certain period of time, initiates the formation of a block that will consolidate all accumulated transactions. Information about a successfully formed block is returned to the client via a similar path. Two scenarios were considered in this study: in the first case, transactions were sent to the blockchain network for recording, and in the second, they were requested from the blockchain network, which allowed us to evaluate the response time from the blockchain node. It should be noted that the write request to the blockchain network and the read request from the blockchain network were executed simultaneously. The write request to the blockchain network occurred according to the schedule shown in Fig. 3.

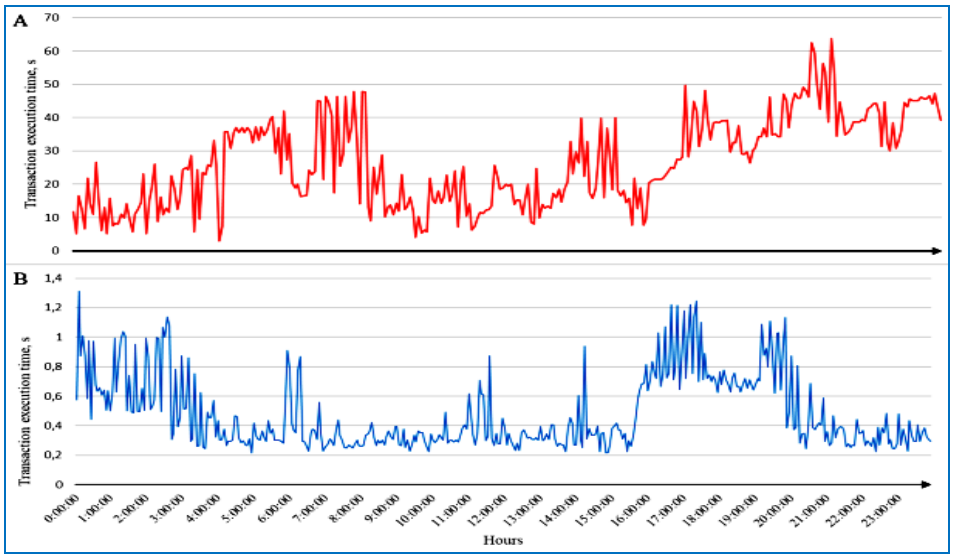

Fig. 3. Transaction processing time (A – for the Ethereum network, B – for the Waves network)

The read request from the blockchain network, in turn, occurred every 1 second. Thus, Fig. 3 (A) shows the results of writing data to the Ethereum blockchain network, and Fig. 3 (B) shows the results of writing data to the Waves blockchain network. It should be noted that all experiments are performed while waiting for confirmation of the transaction being written to the network. That is, to write the next transaction, a response from the blockchain network confirming that the transaction has been successfully processed and recorded is required. The need for confirmation of the write is due to the system's sensitivity to losses, as the loss of data from the OBU, in the case of recording fare data, could result in incorrect vehicle information.

As can be seen in Fig. 3 (A), the long transaction processing time and obvious losses are clearly visible. During the experiment, 3,000 transactions were written to the blockchain network, of which only 2,554 were successfully processed, meaning that 446 transactions were discarded and not registered in the blockchain network. The losses amount to 14.9%. In the case of writing data to the Waves blockchain network, there are no losses when writing transactions to the blockchain network. Fig. 3 (B) clearly demonstrates that the transaction writing speed is 20-40 times higher than in the Ethereum blockchain network. It is also necessary to take into account that private networks were configured to process incoming transactions as quickly as possible with relatively low hardware characteristics. Thus, when constructing the SD-IoV-Blockchain network architecture [5], the implementation of a single blockchain network node is only possible if the LPoS consensus algorithm is used.

Fig. 4 shows the result of processing a read request from the blockchain network. Similarly, a clear advantage can be seen in the Waves blockchain network with the LPoS algorithm, where the read request processing speed is, on average, 10 times higher than that of the Ethereum PoW blockchain network.

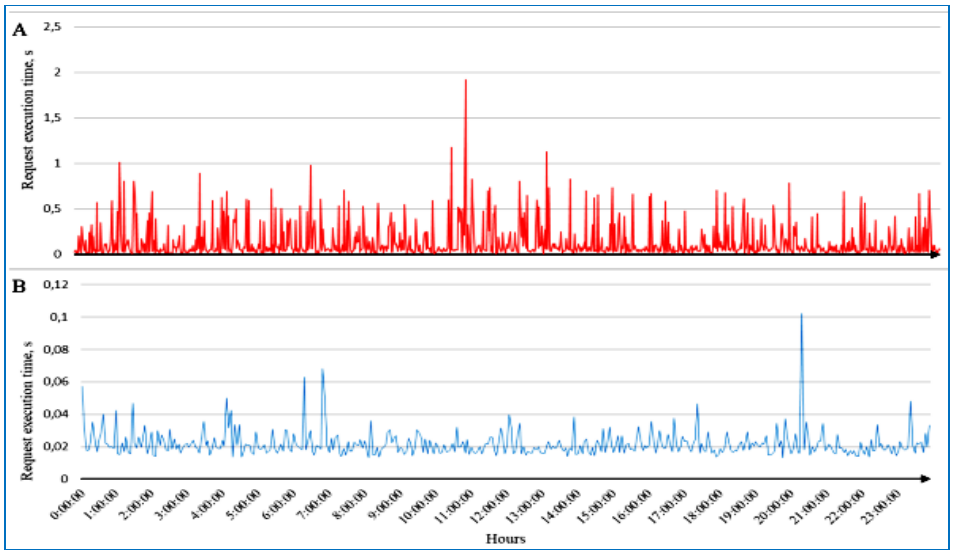

Fig. 4. Data reading processing graph (A – for Ethereum-based implementation, B – for Waves-based implementation)

Висновки

Based on the obtained research results, it can be concluded that the Proof of Stake consensus algorithms and the Waves blockchain network are more suitable than the classic Ethereum blockchain network under conditions of limited hardware specifications. This study demonstrates the feasibility of integrating and applying blockchain technology within the ITS concept and its overall suitability for use. It also clearly demonstrates the need for balancing depending on current network conditions, as the graphs show the periods of effectiveness of each algorithm. Implementing an adaptive algorithm for blockchain data flows would enable efficient data recording and hardware load balancing. Further research should be directed towards the development of mathematical models for optimizing distributed data exchange processes, taking into account the dynamic characteristics of the transport environment. The use of artificial intelligence and machine learning technologies for adaptive management of information flows in conditions of variable traffic intensity is promising. Particular attention should be paid to issues of data security and confidentiality in distributed networks, in particular the use of cryptographic methods and trust mechanisms between system nodes.

Another important direction is the integration of distributed technologies with 5G/6G communication systems to ensure ultra-reliable and low-latency communication (URLLC), which is critically important for Vehicle-to-Everything scenarios. Conducting simulation and experimental studies will help assess the effectiveness of the proposed solutions and contribute to the formation of architectural standards for new-generation intelligent transport systems.

СПИСОК ЛІТЕРАТУРИ

1. Dotsenko, N., Chumachenko, I., Galkin, A., Kuchuk, H. and Chumachenko, D. (2023), “Modeling the Transformation of Configuration Management Processes in a Multi-Project Environment”, *Sustainability (Switzerland)*, Vol. 15(19), 14308, doi: https://doi.org/10.3390/su151914308

2. Zuev, A., Karaman, D. and Olshevskiy, A. (2023), “Wireless sensor synchronization method for monitoring short-term events”, *Advanced Information Systems*, vol. 7, no. 4, pp. 33–40, doi: https://doi.org/10.20998/2522-9052.2023.4.04
3. Buterin, V., Illum, J., Nadler, M., Schär, F. and Soleimani, A. (2024), “Blockchain privacy and regulatory compliance: Towards a practical equilibrium”, *Blockchain Research and ApplicationsOpen source preview*, vol. 5(1), no. 100176, doi: https://doi.org/10.1016/j.bcra.2023.100176
4. Kasahara, S., Kawahara, J., Minato, S.-I. and Mori, J. (2023), “DAG-Pathwidth: Graph Algorithmic Analyses of DAG-Type Blockchain Networks”, I*EICE Transactions on Information and SystemsOpen source preview*, E106D(3), pp. 272–283, doi: https://doi.org/10.1587/transinf.2022FCP0007
5. Xia, Y., Hua, Z., Yu, Y., Zang, B. and Guan, H. (2022), “Colony: A Privileged Trusted Execution Environment with Extensibility”, *IEEE Transactions on Computers*, vol. 71(2), pp. 479–492, doi: https://doi.org/10.1109/TC.2021.3055293
6. Cocco, L. and Tonelli, R. (2024), “A Self-Sovereign Identity–Blockchain-Based Model Proposal for Deep Digital Transformation in the Healthcare Sector”, *Future Internet*, vol. 16(12), 473, doi: https://doi.org/10.3390/fi16120473
7. Kuchuk, N., Kovalenko, A., Ruban, I., Shyshatskyi, A., Zakovorotnyi, O. and Sheviakov, I. (2023), “Traffic Modeling for the Industrial Internet of NanoThings”, *2023 IEEE 4th KhPI Week on Advanced Technology*, KhPI Week 2023 - Conference Proceedings, 2023, doi: 194480. http://dx.doi.org/10.1109/KhPIWeek61412.2023.10312856
8. Kuchuk, H. and Malokhvii, E. (2024), “Integration of IOT with Cloud, Fog, and Edge Computing: A Review”, *Advanced Information Systems*, vol. *8*(2), pp. 65–78, doi: https://doi.org/10.20998/2522-9052.2024.2.08
9. Decker, C. and Wattenhofer, R. (2014), “Bitcoin transaction malleability and MtGox”, *European symposium on research in computer security*, 370, pp. 313–326, doi: https://doi.org/10.1007/978-3-319-11212-1_18

Received (Надійшла) 25.07.2025
Accepted for publication (Прийнята до друку) 23.10.2025

ВІДОМОСТІ ПРО АВТОРІВ / ABOUT THE AUTHORS

Кучук Ніна Георгіївна – доктор технічних наук, професор, професорка кафедри комп’ютерної інженерії та програмування, Національний технічний університет “Харківський політехнічний інститут”, Харків, Україна;
Nina Kuchuk – Doctor of Technical Sciences, Professor, Professor of Computer Engineering and Programming Department, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine;
e-mail: nina_kuchuk@ukr.net; ORCID Author ID: http://orcid.org/0000-0002-0784-1465;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57196006131.

Трегубенко Максим Андрійович – студент кафедри електронних обчислювальних машин, Харківський національний університет радіоелектроніки, Харків, Україна;
Maksym Tregubenko –student at the Department of Electronic Computers, Kharkiv National University of Radio Electronics, Kharkiv, Ukraine;
e-mail: Maksym.Tregubenko@nure.ua; ORCID Author ID: http://orcid.org/0009-0004-6206-7435.

Коваленко Данило Андрійович – студент кафедри електронних обчислювальних машин, Харківський національний університет радіоелектроніки, Харків, Україна;
Danylo Kovalenko – student at the Department of Electronic Computers, Kharkiv National University of Radio Electronics, Kharkiv, Ukraine;
e-mail: Danylo.Kovalenko@nure.ua; ORCID Author ID: http://orcid.org/0000-0002-6465-7111 .

Лисиця Дмитро Олександрович – кандидат технічних наук, доцент кафедри комп’ютерної інженерії та програмування, Національний технічний університет “Харківський політехнічний інститут”, Харків, Україна;
Dmytro Lysytsia – Candidate of Technical Sciences, Associate Professor of Computer Engineering and Programming Department, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine;
e-mail: Dmytro.Lysytsia@khpi.edu.ua; ORCID Author ID: https://orcid.org/0000-0003-1778-4676;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57220049627.

Бельорін-Еррера Олександра Михайлівна – кандидат наук, старший викладач кафедри комп’ютерної інженерії та програмування, Національний технічний університет “Харківський політехнічний інститут”, Харків, Україна;
Oleksandra Bellorin-Herrera – PhD, Senior Lecturer of Computer Engineering and Programming Department, National Technical University “Kharkiv Polytechnic Institute”, Kharkiv, Ukraine;
e-mail: Oleksandra.Bilorin-Ererera@khpi.edu.ua; ORCID Author ID: https://orcid.org/0000-0001-7974-5301;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=59224314800.

Дослідження технологій розподіленого обміну даними у контексті інтелектуальних транспортних систем

Н. Г. Кучук, М. А. Трегубенко, Д. А. Коваленко, Д. О. Лисиця, О. М. Бельорін-Еррера

Анотація. У статті представлено результати дослідження технологій розподіленого обміну даними, орієнтованих на забезпечення ефективної взаємодії між компонентами інтелектуальних транспортних систем (ІТС). Розглянуто сучасні підходи до організації децентралізованих мереж передачі інформації, зокрема використання концепцій розподілених реєстрів, однорангових протоколів та сервісно-орієнтованих архітектур. Проведено аналіз вимог до надійності, затримки та пропускної здатності каналів зв’язку, що є критичними для сценаріїв обміну даними між транспортними засобами та інфраструктурою. На основі порівняльного аналізу визначено переваги та обмеження існуючих технологічних рішень у контексті забезпечення безпеки, масштабованості та стійкості до збоїв. Результати дослідження можуть бути використані для проєктування адаптивних моделей управління трафіком і розроблення інтелектуальних модулів взаємодії в транспортних мережах нового покоління.

Ключові слова: інтелектуальні транспортні системи; розподілений обмін даними; децентралізовані мережі; розподілений реєстр; масштабованість; надійність передачі даних.