UDC: 004.9: 004.056 https://doi.org/10.15407/jai2022.02.071

THE METHODS AND MEANS TO IMPROVE THE INTELLIGENT SYSTEMS COMMUNICATION COMPONENT'S EFFICIENCY

I. O. Rozlomii[1], A. V. Yarmilko[2], S. V. Naumenko[3]
[1,2,3]Bohdan Khmelnytsky National University of Cherkasy, Ukraine
81, Shevchenka blv., Cherkasy, 18031
a-ja@ukr/net
[1]https://orcid.org/0000-0001-5065-9004
[2]https://orcid.org/0000-0003-2062-2694
[3]https://orcid.org/0000-0002-6337-1605

Annotation. The article is devoted to the issues of protection against the loss of confidential information and unauthorized access to it in communication networks of intelligent systems. The conditions and tasks of using cryptographic methods to protect such systems are analyzed. Practical methods are proposed to increase the efficiency of communication in intelligent systems by protecting messages from unauthorized access, detection, localization, and recovery of damaged blocks of information, and application of optimization encryption. The method of vector encryption is based on the application of matrix lattices and localization of defective blocks of information by methods of the cross and redundant hashing methods.

Keywords: intelligent system, cybersecurity, authentication, vector encryption, hash function.

Introduction

The sign of the times is the intellectualization of interaction in a wide range of computer systems, including multi-agent systems of autonomous robots, various forms of human-machine interaction systems, IoT systems, etc. Such systems rely on both artificial and hybrid (human-machine) intelligence. Modern concepts of intelligent systems development envisage their construction on the technological platform of computer networks. This allows the creation of a unified communication field and within it significantly increases the efficiency of information processes and systems as a whole due to the automation of control functions, integration of heterogeneous equipment, and main and auxiliary technological processes within one software environment.

The efficiency of functioning of systems of this type is largely determined by the security of the common communication field, used programs, and data. On the one hand, by combining the capabilities of intellectual system components with integrated security systems, a high level of efficiency in their protection against technical failures and external influences is achieved. But, at the same time, the key role of information technology in ensuring the functioning of the integrated security system leads to the fact that it is the information resources of these systems that become the object of illegal actions in the implementation of various attempts to disrupt the performance [1].

This, in turn, is the reason for the need to introduce into the information processes of intelligent systems the mechanisms of information protection against unauthorized access, the effectiveness of which should be constantly monitored.

In today's world, in connection with the ever-increasing opportunities for attackers to obtain unauthorized access to confidential and critical information and the improvement of methods of conducting information attacks, there is a need to develop new methods of information protection. However (especially in the case of human-machine systems with hybrid intelligence), in addition to the technical component, risk factors related to the human component of intelligent systems should not be neglected. After all, as a result of its manifestations related to the cognitive properties of a person, the functioning mechanisms of his memory, and the quality of the performance of individual operations, up to 52% of information leaks (intentional and accidental) occur in the world [2].

Software, technical and hardware tools are the main mechanisms that ensure security in modern information systems. This also applies to intelligent systems. Cryptographic means are considered effective methods of protection. Those of them that meet the

requirements of the current time is characterized by the greatest reliability and are built on all possible crypto-algorithms for data encryption [3]. Data encryption is used to ensure the protection of information during its storage and transmission through open communication channels.

There are two types of cryptographic algorithms: symmetric (the same key is used for encryption and decryption) and asymmetric (the private key is used for encryption, and the public key obtained by a certain algorithm from the private key is used for decryption). For example, the principle of asymmetric encryption algorithms is used to create an electronic digital signature (ESD). This technology allows you to identify the person who signed the document and confirm with the help of special software the content of the signed document and the time of its signing.

In the case of intelligent systems, in addition to general factors influencing the integrity of data and programs, specific features of the structure or parameters of information flows may also manifest themselves. Thus, the intellectualization of human-machine interaction, the cooperative nature of the activity of intelligent agents, and their interaction in an open functional space exacerbates the issue of efficiency, safety, and predictability of such systems. The acuteness of these problems, directly related to the state of communications, is related not only to the systemic complexity of these intelligent technologies but also to their exit from the category of unique and experimental projects to the category of mass utilitarian and applied applications. Modern concepts of creating production systems (in particular, Industry 4.0, and Industry 5.0) are also focused on artificial intelligence systems as safe, reliable, and responsible components of a single human-machine functional and communication space.

The implementation of systems for the protection of intelligent information systems should also take into account the forms of technical implementation of such systems. Since the typical solution is their reproduction on the platform of embedded systems or autonomous mobile modules (e.g., systems with the structure described in [4]), the functioning of security systems will be directly affected by the presence of constrained devices (CPU, ROM, and RAM) in their composition, as well as battery life). In general, these resources may not be sufficient to adequately support the security mechanisms for the transmission of messages over the Internet or other wireless communication systems. In addition, such rather limited resources of the components of the intelligent system should ensure the reception and placement of potentially large single blocks of information. This can be an additional technical challenge even without encumbering messages with additional safeguards.

Statement of the problem

The possibility of unauthorized modification, extraction, or destruction of information is the most relevant threat when working with data and programs in intelligent systems. Improving the effectiveness of their communication component should contribute to solving the problem. The effectiveness of communications in a multi-agent system of intelligent modules or an intelligent man-machine system should be considered as the ability to provide the following basic functions:

– protect messages (data, programs) from unauthorized access;

– detect information damage, localize defective blocks and restore primary information;

– coordinate the metric parameters of messages with the parameters of the technical subsystem of individual intelligent agents and communication channels;

– to function in conditions of communication multimodality and multitasking of intelligent agents.

Provision of the listed functions requires the development or adaptation of methods and means of information optimization, cryptanalysis, and encryption of information blocks.

Analysis of recent research and publications

Although smart technologies are widely

recognized and have become an integral part of, for example, implemented smart city projects, they also create new challenges in terms of privacy and security. Access control is one of the main security issues, which is crucial for the protection of resources and information on the devices of such systems. Various aspects of ensuring information security, in particular - secure messaging in IoT, are considered in the works of O.G. Korchenko, I.R. Opirskyi, S.O. Hnatyuk, O.I. Beley, T.G. Logutova. and other authors.

Determining the reasons for the emergence of the most common threats in the IoT network, Opirskyi I.R., Golovchak R.V., Mosiichuk I.R., Balyanda T.S., Haranyuk S.P. consider information security approaches by analyzing data transmission technologies and analyzing the threats themselves [5].

Lobanchikova N.M., Pilkevich I.A., Korchenko O.H. an analysis of attacks on components of IoT systems was carried out. It is emphasized that the use of wireless communication technologies between individual components of the system creates prerequisites for a cyber-attack on the nodes of its communication network. The security of the system should be achieved by implementing a multi-stage complex protection system based on the use of the latest technical means, qualified personnel, control procedures, and compliance with administrative regulations [6].

The use of protection mechanisms based on blockchain technology in intelligent technologies is currently the focus of research. Thus, a group of methods based on this technology is highlighted in his work by Lee Keun-Ho [7]. A decentralized access control scheme as a scalable, thin, and light solution for modern IoT networks is proposed by Ronghua Xu, Yu Chen, Erik Blasch, and Genshe Chen. In their work, these authors consider a decentralized mechanism based on combined capabilities to support hierarchical delegation and delegation with several transitions [8].

The aim of the research

The purpose of the study is to identify and analyze methods and means of protection and maintenance of communication networks of intelligent multi-agent systems with artificial or hybrid intelligence.

An overview of the main material

The task of successfully combating the threat of disclosure of content or violation of data integrity is best handled by cryptographic protection tools.

As mentioned, one of the functions of an intelligent system is to protect messages from unauthorized access. Unauthorized access means access to data by persons or devices that have not been registered and do not have the right to use the relevant resources. Unauthorized access can be expressed in copying, modification, or destruction of data, interception and blocking of information, the substitution of data processing processes, and other operations on messages not foreseen by the owner.

Solving the problem of preventing unauthorized access in an intelligent system is directly related to authentication - a process that verifies the user's identity when accessing the system. Faulty or incorrectly configured authentication mechanisms are the main reason for access by unauthorized subjects of the communication process. Unauthorized access has a large number of causes. The main ones are weak passwords, social engineering attacks (phishing), destroyed accounts, insider threats, malicious software (bots), and others [9].

The application of the mechanisms of identification of participants in the communication process and their authentication allows organizing the interaction with agents in the intelligent system within the limits of separate permanent or situational subsystems - communication clusters. Thanks to this, conditions are created for the involvement of intelligent system modules in the parallel execution of tasks in several separate scenarios, which consist of spontaneous interaction with other agents that form such clusters.

Another important task in communication in a multi-agent system is the detection and localization of defective blocks to restore primary information.

To ensure the integrity and reliability of

the information, it is advisable to use hashing - the cryptographic transformation of data of arbitrary size into data of fixed size (Fig. 1).

The information flow is a set of messages that circulate in the network of the intelligent system. Calculating the hash function of the information stream allows you to guarantee the integrity of the information, as informational signs are created, by which it is possible to control that the messages were not modified in the process of exchange.

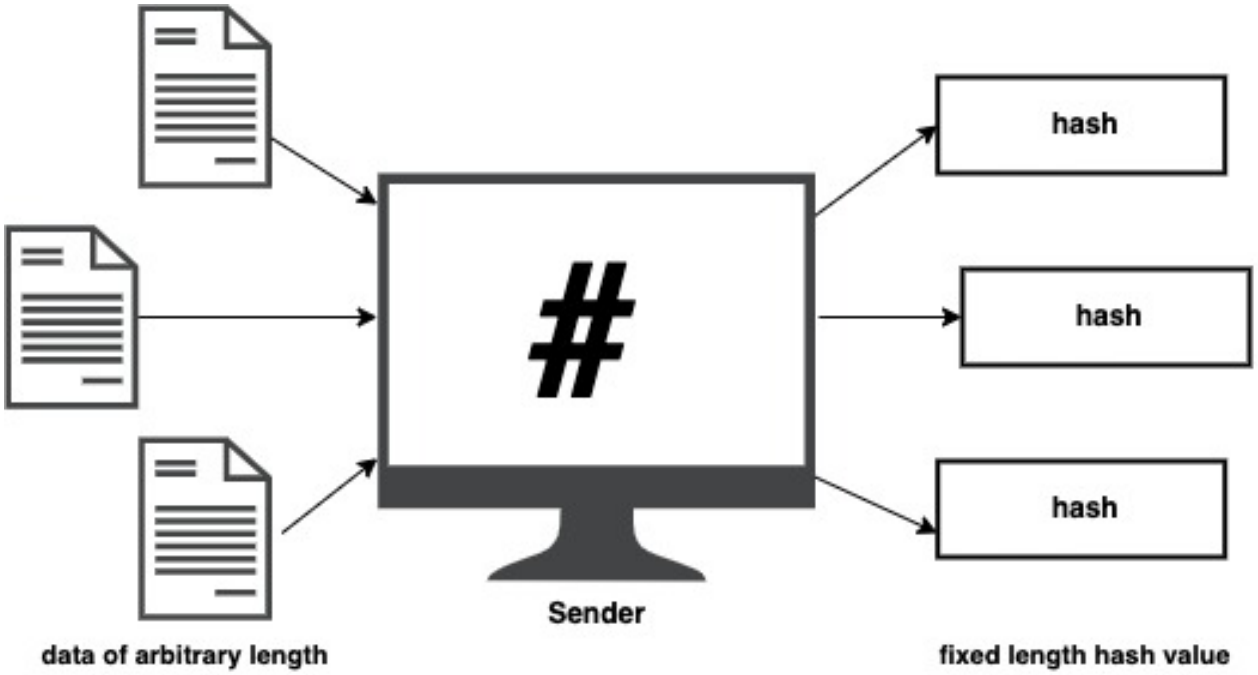


Fig. 1. The general concept of hashing

To localize defective blocks, it is proposed to use methods of cross-hashing or redundant hashing [10-11]. The cross-hash method allows you to detect a single corrupted message. Another method - redundant hashing - allows you to detect a specific number of corrupted messages.

Since the redundant hashing method can ensure the guaranteed detection of a given number of corrupted messages, let's take a closer look. The method is developed based on the concept of self-controlled and self-adjusted Hamming codes and operations of matrix cryptographic transformations. The corrective possibility of Hamming codes is characterized by a minimum code distance. The minimum code distance is equal to the number of positions that differ between two compared code sequences. Providing the appropriate code distance allows you to determine, firstly, how many defective blocks can be detected and, secondly, how many can be localized.

The essence of the method is to calculate the hash function not of the entire stream of information, but of each message separately. In addition, according to the Hamming coding principle, redundant information blocks are added to the main information blocks. The number of redundant blocks directly depends on the minimum code distance. For example, according to theoretically justified possibilities, the minimum code distance $d_0=5$ will ensure the guaranteed localization of two defective blocks (1) or the detection of four such blocks (2):

$$t_{випр} \le \frac{d_0 - 1}{2} \quad (1)$$

$$t_{вияв} \le d_0 - 1 \quad (2)$$

Hash methods can also be used in procedures for analyzing the content of sent

messages [12].

In the process of exchanging messages between individual agents of the intelligent system, complete blocks of information can be quite large. This can create threats to their placement in the memory of receiving agents. Minimizing the memory requirements of the system components and offloading the equipment of their receiving and transmitting nodes is possible thanks to the reduction of the volume of data by compressing it. A fundamental possibility for this is provided by a characteristic feature of any information: its redundancy [13]. Encryption methods are used for this transformation of messages.

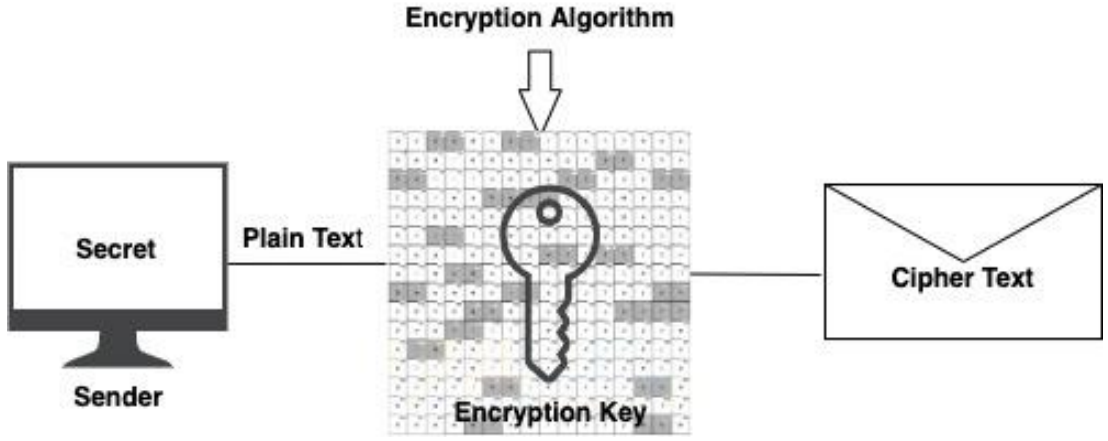
In modern information systems, encryption operations are performed "on the fly", almost imperceptibly for the user. Usually, the power of processors is enough to encrypt and decrypt large volumes of information using reliable symmetric cryptosystems with a key length of more than 256 bits.

A method of vector encryption of information based on the use of a matrix lattice is proposed. The matrix grid is the key to the encryption and decryption of information. The key is built based on statistical text analysis and matrix cryptographic transformation operations, as shown in works [14-15].

First, a statistical analysis of the text is performed. As a result of the analysis, we will get the frequency of occurrence of each letter of the alphabet in the grid. Next, it is necessary to perform matrix cryptographic transformations of numbers from a given range, which is equal to the lattice size (key length). According to the results of matrix cryptographic transformations, it is necessary to place the letters on the grid. In this way, we get an encryption/decryption key - a matrix lattice.

The prototype of the matrix grid is the Cardano encryption grid - the first encryption stencil proposed back in 1550. The similarity of the matrix lattice with the encryption lattice consists of the visual (external) similarity: a table with slotted cells, in which the information to be encrypted is placed. The general scheme of encryption/decryption by the proposed method is shown in fig. 2.

In the process of communication, the components of the intelligent system can send data and programs. Each type of information is characterized by a different indicator of redundancy. In this regard, the information that needs to be encrypted can be divided into structural parts - vectors and assigned a weight, where the weight of the vector is the number of symbols. The encryption method consists in finding the positions of the vectors in the matrix grid, which will be the result of encryption. In existing encryption methods, the encrypted information is also of the same volume as the input information. Since the vector encryption method allows encryption with compression, as a result of encryption we get smaller data.



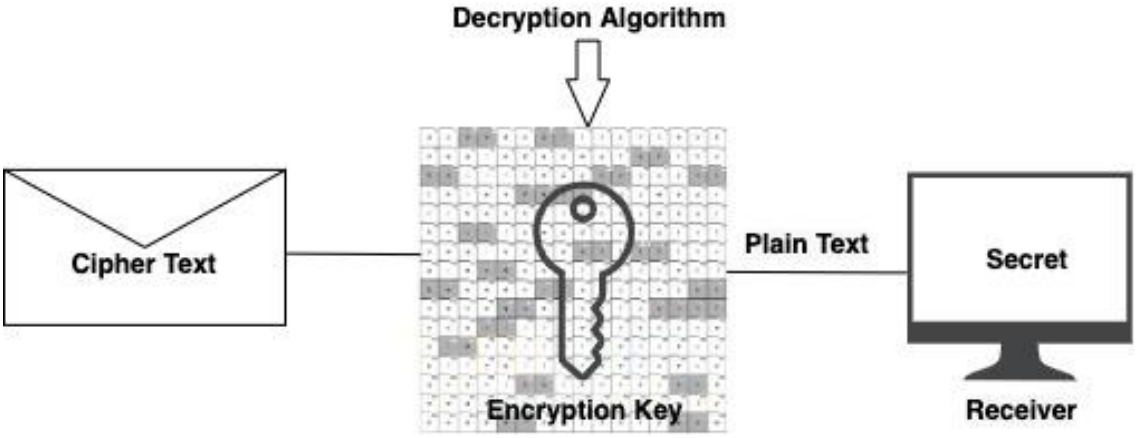


Fig. 2. Encryption and decryption schemes based on a matrix lattice

Conclusions

The cyber security of intelligent systems has features due to their structure and method of technical implementation. A relevant approach to the practical implementation of the protection of their communication subsystem is the use of cryptographic methods. Such methods allow for mutual identification of subjects of the communication process, detection of damaged blocks of information being forwarded, and their restoration. A promising method of protecting messages in an intelligent system is encryption using a matrix lattice.

References

1. Yarmilko A., Rozlomii I., Kosenyuk H. (2022) Hash Method for Information Stream's Safety in Dynamic Cooperative Production System. In: Serhiy Shkarlet et al. (Eds): Mathematical Modeling and Simulation of Systems. Lecture Notes in Networks and Systems, vol 344. Springer, Cham. PP. 173-183. https://doi.org/10.1007/978-3-030-89902-814
2. Vovk, Methods of information security IoT, Master's thesis, NTU of Ukraine «KPI named after Igor Sikorsky», 2018.
3. Belej, O., & Tamara, L. (2019). Bezpeka peredachi danykh dlia internetu rechei. Elektronne fakhove naukove vydannia «Kiberbezpeka: osvita, nauka, tekhnika». 2(6), 6-18.
4. Yarmilko A. V., Nikitiuk V. S. (2021) Modeliuvannia hrupovoi povedinky avtonomnyh ahentav za stsenariiem konsolidatsii. Visnyk KrNU imeni Mykhaila Ostrohradskoho. 6(131). 66–72. DOI: 10.30929/1995-0519.2021.6.66-72.
5. Opirskyy, I., Holovchak, R., Moisiichuk, I., Balianda, T., & Haraniuk, S. (2021). Problemy ta zahrozy bezpetsi IoT prystroiv. Elektronne fakhove naukove vydannia «Kiberbezpeka: osvita, nauka, tekhnika». 3(11), 31-42. https://doi.org/10.28925/2663-4023.2021.11.3142
6. Lobanchykova, N. M., Pilkevych, I. A., & Korchenko, O. (2021). Analysis of attacks on components of IoT systems and cybersecurity technologies. In CEUR Workshop Proceedings (2021, in press) (pp. 83-96).
7. Lee, K. H. (2019). A Scheme for Information Protection using Blockchain in IoT Environment. Journal of Internet of Things and Convergence, 5(2), 33-39.
8. Xu, R., Chen, Y., Blasch, E., & Chen, G. (2018). Blendcac: A smart contract enabled decentralized capability-based access control mechanism for the IoT. Computers, 7(3), 39.
9. Sloan, R., & Warner, R. (2017). Unauthorized access: The crisis in online privacy and security (p. 401). Taylor & Francis.
10. Rozlomii I. O., Koseniuk H. V. (2018) Vyiavlennia porushen tsilisnosti elektronnoho dokumentu shliakhom perekhresnoho kheshuvannia. Visnyk KhNU. Radiotekhnika, elektronika ta telekomunikatsii. 5 (265), 32–35.
11. Rozlomii I. O., Rudnytskyi V. M., Aliekseieva S. M. (2017) Vykorystannia khesh-funktsii dlia vyiavlennia falsyfikovanykh frahmentiv elektronnoho dokumentu. Skhidnoievropeiskyi naukovyi zhurnal. 3(19), 68–72.
12. Yarmilko A. V., Rozlomii I. O., Mysiura Yu. O. (2021) Zastosuvannia khesh-metodiv u kryptohrafichnomu analizi potokiv informatsii. Visnyk KhNU. Tekhnichni nauky. 6(281). 49–54.
13. Liang, H., & Fu, K. W. (2019). Network redundancy and information diffusion: The impacts of information redundancy, similarity, and tie strength. Communication Research, 46(2), 250-272.
14. Rozlomii I. O., Naumenko S. V. Metodolohiia vykorystannia matrychnykh reshitok Kardano dlia kompleksnykh system zakhystu informatsii. «Kompleksne zabezpechennia yakosti tekhnolohichnykh protsesiv ta system» (KZIaTPS – 2022): materialy tez dopovidei XII Mizhnarodnoi naukovo-praktychnoi konferentsii (m. Chernihiv, 26–27 travnia 2022 r.) NU «Chernihivska politekhnika», 2022. – T. 2. S. 201.
15. Rozlomii I. O. (2022) Metod pobudovy matrychnykh reshitok Kardano dlia stysnennia informatsii. Visnyk KhNU. Tekhnichni nauky. 1(305). 85–90.

The article has been sent to the editors 13.11.22
After processing 25.12.22