UDC 004.056

Yarmilko A.V., PhD, Associate Professor,
Rozlomii I.O., PhD, Senior Lecturer,
Naumenko S.V., post graduate student
Bohdan Khmelnytsky National University of Cherkasy, inna-roz@ukr.net

ROBUST COMMUNICATION CLUSTERS: SECURE INFORMATION EXCHANGE AND REDUNDANT HASHING FOR THIRD-PARTY INCLUSIONS LOCALIZATION

Due to the proliferation of robotics and process automation technologies in the interaction between humans and robotic systems, there is an increasing need to ensure the security and protection of information transmitted between the components of these systems. Communication clusters formed spontaneously, involving robotic modules and humans engaged in cooperative tasks, are particularly vulnerable to information compromise. Therefore, it is crucial to securely protect the information from security attacks or communication failures.

Protecting information in communication clusters of this type requires the use of various measures to ensure data confidentiality, integrity, and availability, including:

1. Encryption: The use of cryptographic algorithms to encrypt transmitted data can ensure the confidentiality of information. Robotic system clusters can employ symmetric or asymmetric encryption for protecting communication channels [1].
2. Authentication and Authorization: The use of authentication mechanisms allows verifying the identity of users and robots accessing the system, based on the use of passwords, certificates, or biometric methods. After authentication, the system can employ authorization mechanisms to control access to various resources and functions, limiting privileges of users and robots within communication clusters.
3. Intrusion Protection: Deploying intrusion detection and prevention systems (IDS/IPS) helps detect and block potential attacks on communication clusters. This may include monitoring network traffic, vulnerability analysis, and other methods for recognizing anomalous activity [2].
4. Hashing: Redundant hashing is a technique used to ensure data integrity and detect unauthorized modifications within communication clusters. It relies on the use of hash functions that transform input data into fixed-length hash codes. Redundant hashing involves using multiple independent hash functions for processing data, generating several hash codes for a single dataset.

In the context of communication clusters, hashing can be applied to ensure reliability and integrity in information exchange. The principle of hashing involves each cluster node generating its own hash code for the received data using its own hash function.

After generating the hash code, the node transmits the data and its hash code to other nodes in the cluster. Each node receives data from other nodes and verifies integrity by comparing the received hash code with its own generated hash code. If the hash codes match, it indicates data integrity.

If at least one hash code doesn't match, it may indicate potential data modification or the presence of a third-party inclusion. In such cases, the cluster can take appropriate actions, such as ceasing data exchange with the suspicious node or notifying the system administrator.

Implementing the mentioned practices helps detect and isolate potential threats, as well as enabling a swift response to prevent further compromise of the system. Localization of third-party inclusions in communication clusters remains an unresolved issue. It is proposed to localize third-party inclusions in a communication cluster using redundant hashing techniques. This is intended to ensure secure information exchange among cluster participants.

Redundant hashing involves creating additional hash sums for each object in the communication cluster. These hash sums are constructed using Hamming encoding principles and matrix cryptographic transformation operations. The use of redundancy allows for error detection and correction in transmitted information that may occur during transmission. There are codes designed solely for error detection and error-correcting codes capable of both error detection and correction. The simplest error detection methods are checksumming and parity checking. However, they are not sufficiently reliable, especially in the case of a large number of errors.

The use of redundant codes, including Hamming codes, can be applied to detect and localize foreign inclusions in the communication cluster of robotic systems. Instead of traditional checksums, additional hash sums are utilized for this purpose. They incorporate extra information that allows for the detection and localization of foreign inclusions in the communication cluster of robotic systems. Existing hashing methods such as MD5, SHA-1, SHA-256, and CRC32 can be used to compute the checksums. Matrix cryptographic transformation-based hashing methods can also be employed for calculating the checksums. These methods are based on mathematical operations of linear algebra and utilize matrices for data processing. One example of such a method is SHA-3 (Secure Hash Algorithm 3), which is one of the latest standards for hash functions. SHA-3 employs matrix operations, including symmetric transformations like Keccak. This method relies on complex logical operations and irreversible matrix transformations, ensuring high security and resistance to cryptanalysis. Matrix cryptographic transformation-based hashing methods can provide efficient and secure data processing with high resistance to alterations. They are widely used in cryptographic protocols and systems where data security and integrity are critical aspects.

The proposed method for data integrity control utilizes a system of hash codes constructed according to the rules similar to those of linear redundant codes. This system is known as a linear hash code system. It consists of a set of hash codes obtained using a standard hash function implementation procedure on message blocks defined by a special block selection procedure. This procedure is based on the mathematical apparatus of linear algebra [3].

Localization of third-party inclusions in a human-machine communication cluster can be crucial for ensuring system security and efficiency. Third-party inclusions can be various software modules, applications, or libraries that are compatible with the system but were not specifically developed for it. Incorporating such components can provide rapid and efficient system expansion, but they can also pose certain threats to system security and reliability. One possible risk of third-party inclusions is security vulnerabilities that can be exploited by attackers to target the system. Third-party inclusions may contain malicious code, such as viruses or spyware that can modify the cluster's operation, harm the system, and its users.

In general, the localization and control of third-party inclusions are important steps in ensuring security in a communication cluster, as unauthorized use of such inclusions can lead to data confidentiality breaches, increased risk of cyber-attacks, and other serious threats. Redundant hashing is an effective method to secure information exchange in robotic system clusters. By detecting potential third-party inclusions and data modifications, it ensures integrity and reliability of information exchange as the foundation for the system's sustainable functioning.

List of references

1. Pereira, T., Barreto, L., & Amaral, A. (2017). Network and information security challenges within Industry 4.0 paradigm. Procedia manufacturing, 13, 1253-1260.

2. Breiling, B., Dieber, B., & Schartner, P. (2017, April). Secure communication for the robot operating system. In 2017 annual IEEE international systems conference (SysCon) (pp. 1-6). IEEE.

3. Yarmilko, A., Rozlomii, I., & Kosenyuk, H. (2022, February). Hash Method for Information Stream’s Safety in Dynamic Cooperative Production System. In Mathematical Modeling and Simulation of Systems: Selected Papers of 16th International Scientific-practical Conference, MODS, 2021 June 28–July 01, Chernihiv, Ukraine (pp. 173-183). Cham: Springer International Publishing.