DOI:10.26104/NNTIK.2023.25.64.007

Гаджиев Р.М., Алакбарова Т.Ш., Аббасова П.А.

КИБЕРФИЗИКАЛЫК СИСТЕМАЛАРДЫН КООПСУЗДУК МАСЕЛЕЛЕРИ

Гаджиев Р.М., Алакбарова Т.Ш., Аббасова П.А.

ВОПРОСЫ БЕЗОПАСНОСТИ КИБЕРФИЗИЧЕСКИХ СИСТЕМ

R. Hajiyev, T. Alakbarova, P. Abbasova

SECURITY ISSUES OF CYBER-PHYSICAL SYSTEMS

УДК: 681.518

Макала киберфизикалык системалардын маалыматтык коопсуздугу көйгөйүнө арналган. Мындай системалардын маалыматтык коопсуздугуна байланыштуу негизги суроолор каралат: «Чабуул деген эмне?», «Ким кол салат?», «Алар эмне үчүн кол салышат?», «Кантип кол салышат? жана, «Өзүңдү кантип коргоо керек?». Киберфизикалык системалардын аныктамасы жана классификациясы берилип, кол салуучулардын классификациясы кирүүнүн түрү, мүмкүндүк алуу ыкмасы, ниети, билими жана ресурстары сыяктуу мүнөздөмөлөрдүн негизинде сунушталган. Макалада ошондой эле ар кандай мүнөздөмөлөрү боюнча кол салуу аракеттеринин классификациясы талкууланат. Коргоо ыкмаларынын жана каражаттарынын классификациясы сунушталат. Киберфизикалык системалар аз өткөрүү жөндөмдүүлүгүнүн шарттарында аз өндүрүмдүүлүктөгү түзүлүштөрдүн негизинде иштегендиктен, мындай системалар коопсуздуктун жетиштүү деңгээлине ээ эмес. Бул типтеги системалар чечүүчү милдеттердин өзгөчөлүгүнөн улам аларда ишке ашырылган коопсуздук чаралары биринчи кезекте жогорку жеткиликтүүлүктү жана ишенимдүүлүктү камсыз кылууга багытталган. Макаланын илимий мааниси предметтик чөйрөдөгү изилдөөлөрдүн учурдагы абалын системалаштырууда.

Негизги сөздөр: *чабуулчу модели, чабуул жасоочу аракеттердин модели, коргоонун ыкмасы, коргоонун каражаттары, маалыматтык коопсуздук, киберфизикалык система, чабуулчунун максаты.*

Статья посвящена проблеме информационной безопасности киберфизических систем. Рассмотрены основные вопросы, связанные с информационной безопасностью таких систем: «Что такое атака?», «Кто атакует?», «Почему атакуют?», «Как атакуют?» и «Как защитить себя»? Были даны определение и классификация киберфизических систем, предложена классификация злоумышленников по таким признакам, как тип доступа, метод доступа, намерения, знания и ресурсы. В статье также рассмотрена классификация наступательных действий по их различным признакам. Предложена классификация методов и средств защиты. В связи с тем, что киберфизические системы функционируют на основе малопроизводительных устройств в условиях низкой пропускной способности, такие системы не обладают достаточным уровнем безопасности. Ввиду специфики задач, решаемых этими типами систем, реализованные в них меры безопасности направлены, прежде всего, на обеспечение высокой доступности и надежности. Научная значимость статьи заключается в систематизации современного состояния исследований в предметной области.

Ключевые слова: *модель злоумышленника, модель атакующих действий, метод защиты, средства защиты, информационная безопасность, киберфизическая система, цель злоумышленника.*

The article is devoted to the problem of information security of cyber-physical systems. The main questions related to the information security of such systems are considered: "What is an attack?", "Who attacks?", "Why do they attack?", "How do they attack?" and "How to protect yourself"? A definition and classification of cyber-physical systems were given, and a classification of attackers was proposed based on such characteristics as type of access, access method, intentions, knowledge and resources. The article also discusses the classification of offensive actions according to their various characteristics. A classification of methods and means of protection is proposed. Due to the fact that cyber-physical systems operate on the basis of low-performance devices in low-bandwidth conditions, such systems do not have a sufficient level of security. Due to the specific nature of the tasks solved by these types of systems, the security measures implemented in them are aimed, first of all, at ensuring high availability and reliability. The scientific significance of the article lies in the systematization of the current state of research in the subject area.

Key words: *attacker model, model of attacking actions, method of protection, means of protection, information security, cyber-physical system, attacker's goal.*

Introduction. A cyber-physical system (CPS) is a system that can effectively integrate cyber and physical components using modern sensor, computing and networking technologies. From CPS and cyber-social systems (CSS) has emerged a new computing paradigm known as cyber physical-social or physical-cyber-social computing. Cyber-physical-social systems (CPSS) extend CPS to include social space and features of human participation and interaction. The wide application of TSS is associated with the concept of Industry 4.0, which organizes the process of combining technology and knowledge, ensuring reliability, consistency and control without human intervention. The main technology trends that form the basis of CPS include: *Internet of Things, Big Data, smart technologies, cloud computing, etc.* CPS systems are the basis for the development of the following areas: *smart manufacturing, smart medicine, smart buildings and infrastructure, smart cars, mobile systems, defense systems and weather surveillance systems.* The rapid growth in the use of CPS applications raises a number of security and privacy concerns. Due to the wide application of wireless technologies for the collection and transmission of data and control commands, where a wireless sensor network (WSN) is used, the need for the development of information security systems in the industry is increasing.

Scientific innovation. Scientific novelty of the obtained results:

1. A method is proposed based on the cluster analysis of the called system functions for the initial assessment of the potential danger of the program execution paths, which allows to prioritize them and reduce the set of analyzed paths.

2. It was proposed for the first time to use machine learning with reinforcement to solve the problem of optimization of the choice of execution paths when analyzing dynamic software.

3. A system of reliability and criticality indicators is proposed, which allows detecting the execution of potentially dangerous operations during the dynamic analysis of software.

Conditions and methods of research. While working on the article, the author tried to comprehensively systematize all sources and information based on the analysis, to create a comprehensive picture of the topic. In the research process, scientificity, objective attitude to the processes, their comparative analysis were chosen as the main research methods.

Results and discussions. A cyber-physical system is a complex system consisting of computing and physical elements that constantly receive information from the environment and use it to further optimize management processes [1]. An example of such a system can be: «smart» home, «smart» city and other «smart» automated control systems. The main feature of cyber-physical systems is the connection of physical production processes or other processes that require continuous real-time control with software and hardware systems [2].

The Internet of Things (IoT) is a dynamic distributed environment that connects many intelligent devices capable of sensing the environment and performing appropriate actions [3]. Such devices make it possible to monitor the state of the external environment, collect information about the real world, and create ubiquitous computing systems in which every device can communicate with every other device in the world, regardless of where it is located.

The concept of cyber-physical systems is often considered together with the concept of the Internet of Things. Both types of systems have similar elements, but cyber-physical systems are a broader concept and have a more complex architecture. The main similarity of the architectures is that there is a sensor network at the bottom level of cyber-physical systems and IoT systems. A sensor network is a dynamic, self-organizing and distributed network of sensors and actuators. It is designed to solve automation, diagnostics, telemetry and machine-to-machine interaction problems. A sensor network should be easy to build and manage, not require frequent maintenance, have high fault tolerance and reliability, and should be easily scalable [4].

The sensor network data transmission technology is selected depending on the range and power consumption, noise level and device performance requirements. At first glance, many wireless standards used in sensor networks have similar properties, but these standards are designed to solve different problems and behave differently accordingly. Table 1 shows a comparative table of popular standards.

Table 1

Comparative characteristics of wireless communication standards for sensor networks

Wireless technology (standard)	**Bluetooth (IEEE 802.15.1)**	**Wi-Fi (IEEE 802.11b)**	**ZigBee (IEEE 802.15.4)**	**LoRa**	**Z-Wave**
Frequency range, GHz	2,4-2,483	2,4-2,483	2,4-2,483	2,4-2,483	0,8-0,9
Bandwidth, kbit/s	723,1	11 000	250	до 50	до 100
Protocol stack size, KB	More 250	More 1000	32–64	64	64
Continuous battery life, days	1-100	0,5-5	100-1000	365-1000	90-700
The maximum number of nodes in the network	7	10	65 536	1000	232
Operating range, m (average values)	10-100	20-300	10–100	500	40-100
Areas of application	creation private networks	created local networks	From a distance monitoring and control	Remote data transmission	Remote monitoring and control

As sensor network devices have to operate for a long enough time under harsh conditions, this imposes limitations, affecting their size, data transmission range and power consumption. In addition, depending on the tasks to be solved, up to several thousand devices are required. Therefore, such devices have low cost, low productivity and operate under conditions of low throughput [4].

The security of sensor networks is affected by the lack of intrusion detection, authentication and encryption mechanisms. Due to the low productivity and cost of the devices, security measures and mechanisms are usually greatly simplified, which makes these devices vulnerable. All of the above factors affect the attacker's ability to penetrate the sensor network with minimal costs [5].

The tasks solved by the sensor network require it to meet the following characteristics: autonomy, reliability, fault tolerance and scalability. In some cases, the task may be to collect and analyze data in real time, which imposes additional latency requirements. Therefore, security measures implemented in sensor networks are aimed at ensuring high availability: providing stable communication channels, establishing optimal routes, protecting against external influences, etc.

Bluetooth. The Bluetooth network has a star or mesh topology and uses the high-density 2.4 GHz band, which causes interference during communication. The Bluetooth standard's support for a small number of nodes in a network limits system developer in complex building systems. A Bluetooth-based sensor network is not a reliable solution. However, the widespread adoption of this standard makes it extremely easy to interact with sensor network end devices using personal mobile devices. The Bluetooth standard covers all layers of the OSI model. This standard supports both network-level and application-level message authentication and encryption mechanisms, but has a number of significant weaknesses [6].

Wifi. A Wi-Fi network has a centralized structure and therefore has a single point of failure, as the typical topology of a Wi-Fi network is a «star» or «tree». The failure of one router disrupts the normal operation of the entire network. The mechanism of adding new nodes does not allow flexible scaling of the sensor network. High Wi-Fi network bandwidth is associated with high energy consumption. The speeds offered by the Wi-Fi standard are excessive for a sensor network; low energy consumption is more important to him. Despite the widespread use of this wireless standard, there are cheaper solutions that do not have these drawbacks. But the Wi-Fi network has a significant advantage - the ability to use data security tools that are used to protect regular local networks. Wi-Fi covers only the physical and data link layers of the OSI model; accordingly, system developers have the ability to flexibly configure and use protocols of other layers. However, this reduces the compatibility of devices from different manufacturers with each other [4].

ZigBee. The ZigBee network has a mesh topology. There are two security models in ZigBee network: distributed model and centralized model [1]. Both security models use AES-128 encryption at both the network and application levels. ZigBee also provides integrity checking using the Message Integrity Check (MIC) mechanism. However, to connect to a ZigBee network, a pre-configured global toggle switch with a default value is used. This key is used to ensure compatibility between ZigBee devices from different manufacturers. To increase the level of security, it is necessary to register a non-standard key on all devices in the ZigBee network, otherwise the network will be vulnerable to attacker penetration. An attacker can also capture the network layer key or physically remove it from the device firmware. Application-level encryption is also vulnerable, as this key can also be compromised [1].

LoRa. LoRa forms a network with a star topology and covers all layers of the OSI model. LoRa provides confidentiality of transmitted data using AES encryption at several levels: at the network level using a unique network key (EUI64); end-to-end security at the application level using a unique application key (EUI64); device private key (EUI128). However, LoRa technology also has its weaknesses [1].

Z wave. The Z-Wave network implements a mesh network topology. This fact, together with the use of the less loaded 0.8-0.9 GHz range, the availability of self-healing mechanisms (Explorer Frame procedure) and the establishment of optimal delivery routes, make Z-Wave one of the most reliable solutions. sensor network. Z-Wave also covers all layers of the OSI model. Z-Wave uses its Security 2 [2] security standard, which supports AES-128 encryption and uses mechanisms to connect new devices to the network using PIN codes and QR codes so that an attacker cannot disconnect and go online. The use of the Elliptic Curve Diffie-Hellman protocol for key exchange also significantly increases the security level of the Z-Wave network. However, like any other technology, it has its weaknesses [3].

Application layer protocols. The most commonly used application layer protocols in cyberphysical systems are MQTT, CoAP, AMQP, DDS, and XMPP. MQTT and CoAP are particularly suitable for services that require data collection (such as sensor updates) on limited systems. In contrast, AMQP, DDS, and XMPP address specific service requirements, namely business messaging, instant messaging, and presence detection and real-time messaging.

When it comes to security services, there are many solutions that ensure the integrity and confidentiality of data exchange, provide authentication and authorization mechanisms. Messaging protocols typically support both standard and custom security services. Based on this, it is up to developers to implement appropriate security solutions. Table 2 below shows the capabilities of previously reviewed protocols in the field of encryption, authorization and privacy [3].

Table 2

Summary of security services supported by messaging protocols

Protocol	**Identification**		**Authorization**	**Privacy**	
	SASL	Sp*	Sp*	TLS	DTLS
MQTT		+		+	
CoAP					+
AMQP	+			+	
DDS		+	+	+	
XMPP	+		+	+	

From the above information, it is clear that encryption mechanisms exist in all messaging protocols. For example, confidentiality is provided by standard services such as TLS and DTLS, and authentication and authorization mechanisms are based on standard (i.e. SASL) or custom solutions.

It is important to note the lack of some security mechanisms during development:

• message delivery: the publisher sends messages that cannot be delivered due to lack of subscribers. This vulnerability could lead to a significant reduction in brokerage activity;

• message verification: Broadcaster sends messages containing illegal characters which are misinterpreted by brokers and subscribers. it is possible that this vulnerability can be used to perform various malicious attacks;

• message encryption: clients and servers exchange messages in clear text, which allows an attacker to eavesdrop and falsify messages in transit. This vulnerability can be exploited to perform man-in-the-middle (MITM) attacks [5].

Analysis of CVEs affecting MQTT-based products and services revealed approximately 60 CVE vulnerabilities. In particular, spoofed MQTT messages can easily cause brokers to not respond to requests. For example, a malicious MQTT client could cause a stack overflow simply by sending a SUBSCRIBE packet containing at least 65,400 "/" characters (CVE-2019-11779). Similarly, a CONNECT packet combined with a malformed SUBSCRIBE request packet can be used to launch a denial-of-service (DoS) attack against the broker (CVE-2019-6241).

Other security issues relate to authentication and authorization categories, as in clients setting usernames to "#", thereby bypassing access control and subscribing to all MQTT topics (CVE-2017-7650).

In addition, an actual denial-of-service attack aimed at making the broker unresponsive or even crashing can be performed by sending large messages or messages with a high QoS level. In addition, unauthorized publications intended to physically damage or disable IoT devices can be accomplished using privileged messages that give an attacker remote control over these devices. Thus, the discussed security threats can seriously affect the MQTT-based network and endanger the availability and privacy of the data circulating there.

To address security threats, the MQTT standard lists mechanisms that must be included in an MQTT implementation, namely:

– user and device authentication;

– authorization of access to server resources

– Integrity of MQTT control packages and program data;

– Confidentiality of MQTT control packets and application data.

For each of these mechanisms, the standard provides some general recommendations (eg, authenticating long-running sessions, preventing subscriptions to all threads, using a VPN). However, these countermeasures apply to simple scenarios, ie. For more sophisticated attacks, these measures may be insufficient or simply useless [3].

Although the use of TLS is highly recommended by the MQTT standard to ensure secure communication, TLS does not solve all security problems. Older versions of TLS, its misconfiguration, and the use of weak cipher suites make the protocols vulnerable to security attacks. In addition, implementing TLS requires significant computing power and network bandwidth, which may simply not be available in compute-constrained IoT networks.

CoAP supports the use of Datagram Transport Layer Security (DTLS), a UDP implementation of the TLS protocol that provides equivalent security guarantees. DTLS binding for CoAP is defined in terms of four security modes that differ in authentication and key agreement mechanisms and range from no security to certificate-based security. That is, when using them, the task is to find an optimal compromise between performance/energy constraints and safety requirements. Of course, the lack of appropriate security services may allow an attacker to easily compromise CoAP environments [4].

Ensuring the security of cyber-physical systems. Availability, reliability, and integrity trump privacy because of the potential impact on the physical world. Strong encryption and authentication systems can result in unacceptable delays. It is necessary to implement security measures on the entire system infrastructure, not on individual devices.

Firewall, antivirus protection, intrusion detection and prevention tools, etc. Traditional security tools such as IoT are often ineffective for protecting IoT infrastructure due to the specificity and difficulty of analyzing system-generated traffic and the interoperability of devices. directly with each other. friend over a wireless connection [7]. At the same time, the cyber-physical system should be resistant to intrusions, have backup routes for the delivery of information, and have mechanisms to detect and combat the actions of attackers: network penetration, frame distortion, node switching, etc.

Interference resistance is achieved by sound-immune transmission. A mesh network topology assumes multiple delivery paths, but the topology must be designed in such a way that there are redundant delivery paths for each node.

Generally, for cyber-physical systems, an intrusion detection system collects traffic or its statistics and compares the collected data to a standard. Any deviation from the standard may indicate an attack:

– Changing the number of nodes in the network. This directly indicates the presence of an illegal node.

– Changing the strength level of the node signal. A sharp change in the level of the received signal may indicate a replacement of the transmitter node.

– Changing data delivery routes. Most cyber-physical systems have a mesh topology, and one of the criteria for choosing a delivery route is signal quality. Therefore, a change in the route can add a new node or change the existing one and affect the transmission quality accordingly.

– Increase or decrease the number of frames, change the type of traffic. In cyber-physical systems, nodes usually generate the same type of traffic, so changes in the volume and type of traffic, such as an increase in the number of service packets, can indicate the presence of an attacker.

– Network performance degradation. Reduced throughput and increased latency may also indicate the presence of an attacker on the system.

– Reducing or increasing the response time to requests. This fact may indicate that the legitimate node is replaced by a more productive device, for example, when requests are answered faster.

– Changing the deadlines for sending data. Nodes in cyber-physical systems, as a rule, work for certain periods of time, often in a mode of low power consumption. Accordingly, the activity is anomalous during periods that are not characteristic of the node.

It is clear that each deviation parameter can give wrong results individually, so they should be used together.

The following encryption algorithms should be used to ensure the confidentiality and authenticity of messages. [6], the Wenbo scheme focuses on system delay requirements, as well as energy efficiency requirements and low performance of end devices. The development of such solutions is currently one of the popular areas of research.

Conclusion. Due to the fact that cyber-physical systems operate on the basis of low-performance devices in low-bandwidth conditions, such systems do not have a sufficient level of security. Due to the specific nature of the problems solved by these types of systems, the security measures implemented in them are primarily aimed at ensuring high availability and reliability.

Wireless communication, network topology, low performance, high energy consumption requirements - all this leads to the fact that traditional security measures cannot be applied to cyber-physical systems. However, the use of noise-resistant transmission technologies, the redundancy of data delivery paths, the analysis of the system for anomalies, the use of encryption algorithms from the class of «light» cryptography, as well as the use of authentication schemes for low productivity. systems can significantly increase the security level of a cyber-physical system.

There is another approach to protection - moving target protection technology. This technology does not limit the actions of the attacker, but it does not allow him to obtain long-term information about the system, based on which he can effectively plan his attack.

References:

1. Десницкий В.А. Анализ защищенности программ но-аппаратных компонентов в беспроводных сенсорных сетях / В.А. Десницкий, А.В. Мелешко. // Информационные технологии и телекоммуникации. - 2019. - Т.7, №1. - С. 75-83.
2. Чеклецов В.В. Чувство планеты. Интернет вещей и следующая технологическая революция. - М.: Изд. Рос сийского исслед. центра по интернету вещей, 2013. – 130 с.
3. Куприяновский В.П. Киберфизические системы как основа цифровой экономики / В.П. Куприяновский, Д.Е. Намиот, С.А. Синягов // International Journal of Open Information Technologies. – 2016. – Т. 4, № 2. – С. 18-25.
4. Русанов П.И. Особенности работы беспроводных сенсорных сетей / П.И. Русанов, А.Г. Юрочкин // Вестник Воронежского института высоких технологий. – 2019. – №4 (31). – С. 79-81.
5. Security and Privacy Threats for Bluetooth Low Ener gy in IoT and Wearable Devices: A Comprehensive Survey / A.Barua, A. Al Alamin, S. Hossain, E. Hossain // IEEE Open Journal of the Communications Society. - 2022. - Vol. 3. - P. 251-281.
6. Security analysis of ZigBee / X. Fan, F. Susan, W. Long, S. Li // MWR InfoSecurity. – 2017. – P. 1–18.
7. ZigBee/ZigBee PRO security assessment based on compromised cryptographic keys / P. Radmand, M. Domingo, J. Singh, J. Arnedo, A. Talevski, S. Petersen, S. Carlsen // 2010 International Conference on P2P, Parallel, Grid, Cloud and Internet Computing. – 2010. – P. 465-470.
8. Three practical attacks against ZigBee security: Attack scenario definitions, practical experiments, countermeasures, and lessons learned / O. Olawumi, K. Haataja, M. Asikainen, N. Vidgren, P. Toivanen // 2014 14th International Conference on Hybrid Intelligent Systems. - 2014. - P. 199-206.