IOP Conference Series: Materials Science and Engineering

PAPER • OPEN ACCESS

Security methods for a group of mobile robots according to the requirements of Russian and foreign legislation

Security methods for a group of mobile robots according to the requirements of Russian and foreign legislation

A S Basan [1], E S Basan[1], M A Lapina[2], V N Kormakova[3], V G Lapin[4]

[1] South Federal University, 2 Chekhov St., Taganrog, 347928, Russia

[2] North-Caucasus Federal University, 1 Pushkin St., Stavropol, 355017, Russia

[3] Belgorod State National Research University, 85 Pobeda St., Belgorod, 308015, Russia

[4] Stavropol regional clinical consulting and diagnostic center, 304 Lenina St., Stavropol, 355000, Russia

E-mail ele-barannik@yandex.ru

Abstract. This paper is devoted to the problem of creating security methods for mobile robotic systems. The urgency of the problem of ensuring the security of mobile robotic systems is associated with the presence of a contradiction between the growing popularity of the mobile robotic systems and the presence of many vulnerabilities. Development of a universal security system which should provide protection not only against an malicious attack, but also allow the system to cope with unintentional errors, interference or changes in the external environment, thereby improving the operation of group control algorithms for robots, and increasing the reliability and stability of the mobile robotic systems.

Keywords: Protection, mobile robots, standards, laws, requirements.

1. Introduction

Today, there is a trend associated with the growing popularity of mobile robotic systems, for example, in 2018, the global market for domestic robots reached $ 3.02 billion, according to the research company Research and Markets. According to experts asserts, by 2024 this revenue will be $ 9.13 billion, increasing by about 22.37% annually. The main purpose of robotic systems is to monitor and control the object. This research investigates the use of group control system which include distribution goals and tasks between robots. Of course, the use of a group control system to manage the operation of mobile robots is an effective solution that allows achieving a given goal in a shorter time, with the least loss of resources. It is critical in the case of robots with a limited energy supply [1]. The solution to the problems connected with the designer of the group control system is associated with the growth of interest, both in the scientific, and in the industrial and military spheres.

Nevertheless, a group of mobile robots equipped with a group control system is a rather complicated structure that is vulnerable enough to malicious attacks. The analysis of the group control systems from the point of view of information security revealed that such systems aren't satisfied security principles. However, the standard security methods which applied in information systems are not always applicable to mobile robots' groups. The main vulnerabilities of group control systems are: the presence of a wireless data transmission medium that allows to analyze the transmitted data by intercepting them; the ability to modify the transmitted data, as well as the ability to implement malicious data, causing a destructive effect on the network, due to wireless data transfer and insecure transmission channels; physical insecurity of mobile robotic tools, leading to the possibility of reverse engineering ; the location of the mobile robots outside of the controlled area, which can lead to interception of devices, as well as to the ability to influence environmental indicators, which can lead to disruption of the system.[2]

At the same time, there are the main stages of the group control system for the mobile robots: strategic, tactical and executive. The preparing attacks at the level of target distribution and group formation can lead to significant negative impact. Such as: a complete disruption of the group control system of robots, the incorrect distribution of goals, roles, the choice of incorrect ways to achieve goals. In this case, the following types of attacks are possible: spoofing, violation of the integrity of the transmitted data, compromise of trusted nodes, attacks aimed at disrupting the network clustering process — an attacker will be able to implement these types of attacks by penetrating the network or by conducting a man in the middle attack [3]. In addition, external attacker can affect this control level by conducting denial of service attacks and distributed attacks, as well as cyber-attacks involving physical impact. The following attacks are possible at the tactical control level: affecting on the performance of the robot's sensor system; carry out attacks on the position-tractor control, as well as attacks on the availability of nodes.

At the same time, despite the fact that today there are researches related to the development of security methods, the disadvantage of existing solutions are:

Incompleteness of threats and vulnerabilities databases for a mobile robotic system, as well as a list of possible attacks on the robotic systems.

Lack of an integrated approach to ensuring security in mobile robotic systems at the network, physical and application levels [4].

There is a problem associated with the development of a security system for the mobile robot groups: the difference between this type of network and the typical computer networks. This requires the development of special methods and approaches that must take into account the following factors: the limited computing and energy resources of mobile robots, which makes such solutions as artificial intelligence to detect an attacker difficult and resource-intensive. Thus, the development of a comprehensive security solution for a mobile robotic system is not a trivial task and requires an analysis of all possible threats and vulnerabilities, as well as building a model of the intruder, and also definition of a set of recommendations to increase the degree of system security [5].

2. The problem statement

The main aim of this research is to develop an architecture of protection system for a self-organizing group of mobile robots, taking into account the requirements of Russian and foreign legislation. To achieve this goal it is necessary to solve the following tasks:

- analysis of structural and functional characteristics of a group of mobile robots;
- analysis of types of group control systems for organizing operation a group of mobile robots;
- analysis of network structures for communication in a group of mobile robots;
- analysis of Russian and foreign standards in the field of information security of industrial control system and internet of things (as the most similar in structure and functionality to groups of mobile robots);
- implementation of a protection system in accordance with the developed methodology;
- analysis of the impact of protective equipment on the performance of the robotic system.

3. Development of a security system architecture for a mobile robotic system

3.1. Analysis of structural and functional characteristics of a mobile robotic system

The group control system for mobile robots consists of two main parts: a central station (CS) and on-board computers (BC) with a communication controller (CC).

The central station is installed stationary in the command center and solves the problem of planning the actions of the entire group of robots. In addition, the central station provides a human operator with each robot in the group in case of unforeseen situations, and is also used to set a target [6].

An on-board computer is designed to solve the problem of computational tasks such as distributing goals, determining trajectories, calculating the shortest path, etc. The communication controller is used to provide communication between the robot and the central station and with other robots of the group [7].

There are several ways to organize the process of controlling robots:

- operator control level;
- level of autonomous control level;
- group control level;
- centralized control level.

Let's consider a Flying Ubiquitous Sensor Networks (FUSNs) are one of the classes of WSN / USN wireless or all- pervasive sensor networks. The technology of these networks is based on the self-organizing association of many different sensors with low energy consumption in the network and their placement in hard-to-reach places [8].

Architecturally, they can be decomposed into:

- peer-to-peer networks,
- hierarchical (cluster) networks,
- centralized star topology network.

The architecture of the wireless sensor network, which represents the flying network, consists of three types of nodes:

The coordinator is the only stationary and "trusted" device in the network. It determines the routes for transmitting information, sets the network parameters, controls devices connected to the network, selects the necessary frequency channels, and also acts as a gateway to provide access to the external network. Depending on the application, it can perform various additional functions, for example, it can be a hub or a network manager that monitors the level of interference on a selected channel and can transfer the entire network to a channel of a different frequency;

Router – a device responsible for receiving, storing and transmitting information between nodes. It allows connecting end devices to the network and sends them packets with parameters from the coordinator. In hierarchical network end devices are connected to a node that acts as a router, which, in turn, has a connection to the coordinator. The coordinator can have a connection with several cluster groups;

Sensor nodes (end devices) - are collect data, such as temperature, pressure, dust, etc. Can control a remote object, if necessary. The touch device should have a small size, low power consumption and the ability to stay in sleep mode for a long time. Collectively form a sensory field, which is the place of monitoring[9].

The structural description of the analyzed UAV control system is presented in the table 1.

Table 1. Structural description of the UAV control system.

Control system elements	**Structure**
Operator	PC with any operating system, special software.
Data Transfer Standards	IEEE 802.15.4(ZigBee),IEEE 802.15.1(Bluetooth),IEEE 802.11 (WI- FI), IEEE 802.16-2004, BLE (Bluetooth Low Energy) [10], 6LoWPAN, LTE.
Protocols	TBRPF (Topology distribution base on reverse-path forwarding),DSR (Dynamic Source Routing), GPSR (Greedy Perimeter Stateless Routing),OLSR (Optimized Link State Routing Protocol), DOLSR (Directional Optimized Link State Routing Protocol), AODV (Ad-hoc On-Demand Distance Vector), HWMP (Hybrid Wireless Mesh Protocol), IEEE 802.11 n,s, ZigBee.
Navigation system	Omnidirectional transceiver antenna-feeder devices that monitor the location of an unmanned aerial vehicle
Hardware	Control system components: micro controller, GPS module, communication antenna, engine. Sensor system components: tactile sensors, optical sensors, sound sensors, position sensors, tilt sensors, infrared sensors, temperature sensors, gyro stabilizer.

3.2. Analysis of Russian and foreign legislation field of protection of industrial control systems

In the Russian Federation, one of the main government regulators, as well as special and control functions in the field of state information security, is the FSTEC (Federal Service for Technical and Export Control). The main regulatory document for ICS (industrial control systems) and ISPD (information systems of personal data), according to orders No. 17, 21 and 31, is the methodological document of the FSTEC “Measures for the protection of information in government information systems”. The document describes the methodology for implementing organizational and technical measures to protect information in typical information systems (IS) [11].

This standards and recommendations are directed at realization of information security measures, starting with identification and authentication and ending with the informing and educating users. The information security process, according to the standards, should be structured as follows:

- definition of a basic set of protection measures according to the class of IS,
- adaptation of the basic set of protection measures ,
- refinement of the protection measures according to the threat model,
- addition, taking into account a different regulatory framework in terms of information protection.

In 2008, a safety standard for industrial control systems was issued. National Institute of Standards and Technology represents SP 800-82 Guide to Industrial Control Systems.

- In addition to this order, there are also foreign standards. For example is the NIST, the ISO, but these standards are mainly aimed at examining protection systems for the Internet of things. NIST has developed a Framework for Improving Critical Infrastructure Cybersecurity, where represented the necessary security subsystems that should be implemented in information systems (National Institute of Standards and Technology, 2018). For each of the proposed security subsystems, there are specified sections of the standards where the procedure for developing each subsystem. This Framework presents a large number of requirements, but it is also not clear how to select a specific requirement for the system, how to assess the need to protect one or another component of the system. At the first stage, it is proposed to conduct a risk identification, which includes the following stages:
- Asset Management -The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization’s risk strategy.
- Business Environment - The organization’s mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions;

- Governance - The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.;
- Risk Assessment - The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals;
- Risk Management Strategy - The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions;
- Supply Chain Risk Management - The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk.

The organization has established and implemented the processes to identify, assess and manage supply chain risks [12]. The following assets must be considered when assessing risks according to this document:

- Physical devices and systems within the organization.
- Software platforms and applications within the organization.
- Organizational communication and data flows.
- External information systems.
- Resources (e.g., hardware, devices, data, time, personnel, and software).
- Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders.

The document provides references to other standards that allow realized risk assessment: CIS CSC, COBIT 5, ISA 62443-2-1: 2009, ISO / IEC 27001: 201 NIST SP 800-53. Most of these documents are in the public domain, but are paid, which makes it difficult to study. Nevertheless, it can be concluded that when assessing risks, documents do not refer to methods for determining the current threats. Thus, the issues related to the identification of current threats are practically not worked out.

In 2008, the NIST Special Publication 800-82 standard was introduced [13]. This standard defines key components are:

- Control node. The control node consists of measurement sensors, a controller (includes equipment and actuators, such as PLC controllers, valves, switches, levers, motors) and variable systems.
- Human Machine Interface (HMI). Operators and engineers use the HMI to monitor, control and change set points, algorithms, control and set controller parameters.
- Remote diagnosis and support program. Remote diagnostic and support programs are used to prevent, recognize, and correct malfunctions.

This structure is fundamentally different from that presented in the FSTEC. In May 2015, the standard was released in the second version. The document describes the structure of ICS as follows. A typical ICS contains numerous control loops, human interfaces, and remote diagnostics and maintenance tools built using an array of network protocols on layered network architectures. Control loops utilize sensors, actuators, and controllers (e.g., PLCs) to manipulate some controlled process. A sensor is a device that produces a measurement of some physical property and then sends this information as controlled variables to the controller. The controller interprets the signals and generates corresponding manipulated variables, based on a control algorithm and target set points, which it transmits to the actuators. Actuators such as control valves, breakers, switches, and motors are used to directly manipulate the controlled process based on commands from the controller. As a whole, this document gives a clear understanding of what control systems are, a large number of examples of such systems, their architecture and description are given. This standard can serve as an example for creating a similar document for a robotic system. The document also provides a list of vulnerabilities specific to ICS. In addition, much attention is paid to network protection. Examples of firewall rules and network segmentation options are provided.

Another example is the Robot Security Framework (RSF) [14]. This article describes a security assessment system. Robotic system is divided into 4 components and evaluates the safety of each of them. At the same time, the assessment does not rely at all on the possible threats characteristic of each component of the system, and takes into account only the physical, network, firmware, and application. This Framework also lacks the ability to evaluate the intelligent control system of the robot, evaluate the robot if it is mobile, and the group control system. Authors hereby propose a framework based on four layers that are relevant divide them into aspects considered relevant to be covered. Also, they provide relevant criteria applicable for security assessment. For each of these criteria they identify what needs to be assessed (objective), why to address such (rationale) and how to systematize evaluation (method) [15].

In general, the standards provides for a wider set of requirements than the specified documents, as can be seen from Figure 1, where the number of requirements is presented vertically.

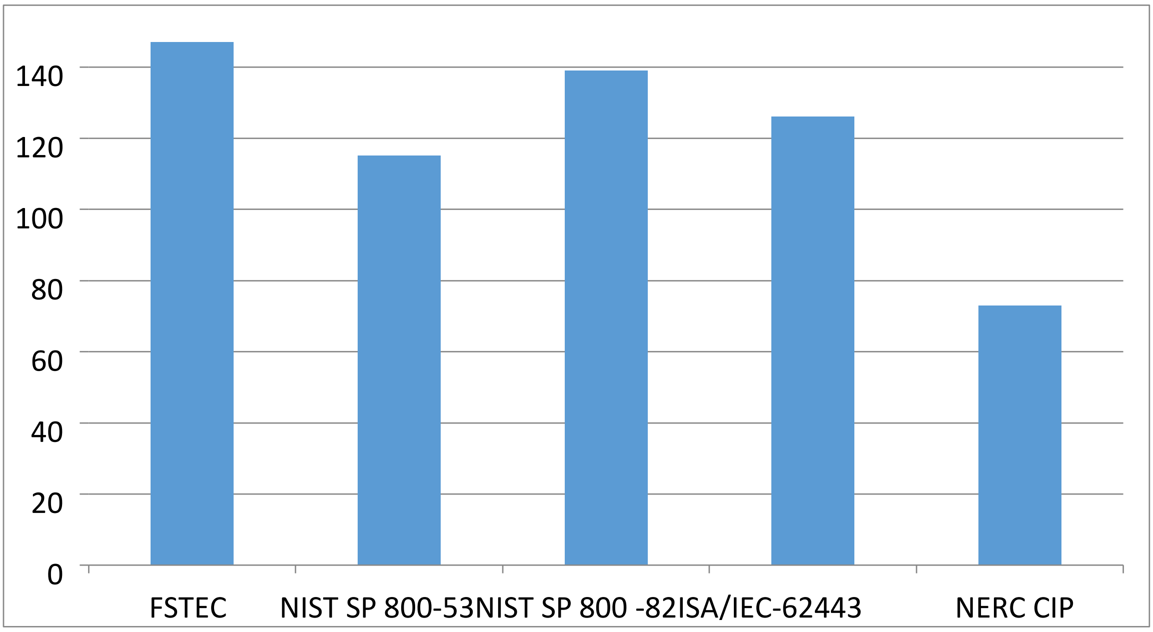

Figure 1. Comparison of the requirements of the FSTEC order with the requirements of International standards

3.3. *Implementation of security requirements for a group of mobile robots*

During the implementation of the security requirements, we installed and configured the firewall, Openvpn, USBGuard, wpasupplicant, denyhosts, eCryptfs [16].

The firewall provides security against network attacks. Openvpn provides security of transmitted information from interception and spoofing. Wpasupplicant provides settings to ensure network security with the use of security protocols such as WPA/WPA2. USBGuard and eCryptfs provide information security from physical downloads. Denyhosts limits the number of login attempts.

Before installing security systems, let's see how busy the system is. To display information about the system load, we will use the built-in htop program. Prior to installing security features, the system is loaded at 2.0%. After carrying out all the settings , the load of CPU was 18–23%. Based on this, we can conclude that with the installed means of protection, for the main activity of the device there is enough performance, about 80%.

Thus, we can conclude that the protection system is not fully implemented, the implemented protection measures provide protection against interference with the operation of the robotic system from the network, encrypted communication channels are installed, the stored information is encrypted, and the device is also protected from physical access to stored information. But the device is not completely protected from physical interference, an attacker can gain access to the components of the device and go unnoticed due to the lack of monitoring of connected components.

The following protection measures are shown in Table 2.

Table 2. implemented protection measures.

Protection measure	Implementation
Physical security	
Unused ports disable	Not implemented
When connecting to physical ports, require authentication	Implemented
Components and cables hidden under the case	Not implemented
Logging of disconnecting / connecting components to the event log	Not implemented
Logging device on / off events in the event log	Not implemented
Network security	
The network is password protected.	Implemented
Using complex passwords	Implemented
Using modern protocols	Implemented
Encryption and mutual authentication	Implemented
Disable unused network ports	Implemented
Operator receives real-time alerts for suspicious activity from the external network	Not implemented
Event logging attempts to connect to the security log	Implemented
Software security:	
Installed current OS versions	Implemented
No known vulnerabilities	Implemented
Verification of signatures before installation	Not implemented
Application Security:	
Programs do not have known vulnerabilities	Implemented
Confidential data is transmitted over an encrypted channel.	Implemented
Access to applications only from authorized users	Implemented

4. Conclusion

Groups of mobile robots are actively being introduced into many areas of activity, thereby questions about the security of robots remain open, including methods and means of protection for a group of mobile robots [17].

The main goal of the work was to research methods and develop protective equipment for a self-organizing group of mobile robots, taking into account the requirements of Russian and foreign legislation.

Description of the Groups of mobile robots helped to learn the control system of mobile robots, varieties of network typologies, components of mobile robots, data transfer protocols, and communication channels.

Comparison of standards allowed us to consider the advantages and disadvantages of Russian and foreign standards.

The use of protective equipment on an experimental bench made it possible to identify the effect of protective equipment on the performance of the entire system.

The result obtained, a comprehensive solution of protection measures for a group of mobile robots, can be used in the future to provide protection to a group of mobile robots, used for subsequent modernization in the development of security methods.

5. Acknowledgment

This work was supported by the RFBR grant 18-07-00212 "Development of a method and decision protocol for detecting anomalous node behavior in group control systems of autonomous mobile robots".

References

[1] Amullen E M, Shetty S, & Keel L H 2016 *Model-based resilient control for a multi-agent system against Denial of Service attacks* World Automation Congress (WAC) Rio Grande Puerto Rico pp. 1-6. doi: 10.1109/WAC.2016.7582963.

[2] Ani U P D, He H M, & Tiwari A 2016 *Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective*. Journal of Cyber Security Technology 1(1) pp 32-74 doi: 10.1080/23742917.2016.1252211

[3] Basan E, Basan A, Grutsynin A 2019 *Overview of Information Issues for a Robotic System* In Proceedings of 19th Interantional Conference on Communication Technology (IEEE ICCT 2019) Xian, China pp 1275-1280

[4] Basan A, Basan E, Makarevich O 2019 *Analysis of ways to secure group control for autonomous mobile robots* In Proceedings of the 10th International Conference on Security of Information and Networks, Jaipur, India pp 134-139

[5] Basan A S, Basan E S, Stepenkin A A 2017 *Analysis and implementation of threats for mobile robot management systems* In Proceedings of the XIII Russian Scientific-practical Conference Mathematical Methods and Information Technology means, Krasnodar, Russia pp 20–23

[6] Faizal K & Palaniappan P LK 2014 *Risk Assessment and Management in Supply Chain* Global Journal of Researches in Engineering: G Industrial Engineering, 14(2), pp 19-30

[7] Hagele M 2016 *Robots conquer the world* IEEE Robotics & Automation Magazine 23(1), 118-120 doi:10.1109/MRA.2015.2512741

[8] Hoang T, Kirichek R, Paramonov A, Koucheryavy A 2016 *Supernodes-based solution for terrestrial segment of flying ubiquitous sensor network under intentional electromagnetic interference* In Proceedings of the ruSMART: Conference on Internet of Things Smart Spaces and NEW2AN: International Conference on Next Generation Wired/Wireless Networking, St. Petersburg, Russia pp 351-359

[9] Holm H, Karresand M, Vidström A & Westring E A 2015 *Virtual Industrial Control System Testbed* Swedish Defence Research Agency Stockholm, Sweden

[10] Kirichek, R V & Kucheryavy A E 2014 *Flying sensor networks* Electrosvyaz 11, pp 2-5

[11] Liang L, Ren W, Song J, Hu H, et al 2013 *The state of the art of risk assessment and management for information systems* In Proceedings of 9th International Conference on Information Assurance and Security (IAS) Gammarth, Tunisia pp 43-56 doi: 10.1109/ISIAS.2013.6947735

[12] Mitchell R, & Chen I R 2014 *Adaptive Intrusion Detection of Malicious Unmanned Air Vehicles Using Behavior Rule Specifications* IEEE transactions on systems, man, and cybernetics: systems, 44 (5) pp 2168-2216

[13] *National Institute of Standards and Technology* 2018 Framework for Improving Critical Infrastructure Cybersecurity version 1.1 pp 1-48

[14] Pshikhopov V, Medvedev M, Kolesnikov A, Fedorenko A, Gurenko R 2016 *Decentralized control of a group of homogeneous vehicles in obstructed environment* Journal of Control Science and Engineering (7192371) pp 1-9 doi: 10.1155/2016/7192371

[15] Pshikhopov V, Ali A 2011 *Hybrid motion control of a mobile robot in dynamic environments* In Proceedings of the IEEE International Conference on Mechatronics, Istanbul, Turkey pp 540–545 doi: 10.1109/ICMECH.2011.5971345

[16] Pshikhopov V K, Medvedev M Y, Gaiduk A R, Gurenko B V 2013 *Control system design for autonomous underwater vehicle* In Proceedings of the Robotics Symposium and Competition (LARS/LARC) Arequipa, Peru pp 77–82 doi: 10.1109/LARS.2013.61

[17] Phillips-Wren G 2012 *Ai Tools in Decision Making Support Systems*: a Review International Journal of Artificial Intelligence Tools 21(2) pp 1-13 doi: 10.1142/S0218213012400052.