Paper

Cyber-security for Mobile Service Robots – Challenges for Cyber-physical System Safety

Wojciech Dudek and Wojciech Szynkiewicz

Warsaw University of Technology, Institute of Control and Computation Engineering, Warsaw, Poland

https://doi.org/10.26636/jtit.2019.131019

Abstract—A review of the known and an indication of the new threats for cyber-physical robotic systems, caused by cybernetic attacks, serves, in this paper, as a basis for the analysis of the known methods relied upon to detect and mitigate consequences of such attacks. A particular emphasis is placed on threats specific for cyber-physical systems, as they are a feature distinguishing these systems from their traditional Information and Communication Technologies (ICT) counterparts. Based on the review of literature and own analyses, unresolved issues regarding the cyber-security of robot systems are presented and discussed.

Keywords—cyber-security, mobile robot safety, robot, robot threats.

1. Introduction

Robots are commonly considered as devices that sense their environment with receptors and act upon the environment with effectors to accomplish a given task. Their intelligence, imperative to act, and the tasks they execute are managed by a control system. The control system, using sensory data and models, plans high-level activities and commands the effectors to execute elementary actions or movements. Service robots are well-equipped with a variety of sensors in order to perform complex robotic tasks (e.g. door approaching and opening [1]) and to store classified data (e.g. medical information [2], door lock types [3]).

Development of robot control systems, with utilization of complex control and planning algorithms included, has a strong impact on the robot's requirements regarding computing power and memory size. Instead of increasing onboard robot computational resources, developers of robot software commonly distribute processing operations between the built-in computer and a cloud. A machine backed with cloud computing technology is not only able to accomplish more complex tasks, but is also capable of sharing its knowledge and experience with other devices [4].

Furthermore, there are platforms that remotely provide robotic applications to perform diverse tasks [5]. The concept behind such platforms is to not only to deliver services which are typical of connected robots, but also to provide independent applications. After an application has been downloaded from the cloud, it takes control of the robot's sensors and effectors. The hazard detection application [6] is an example of a solution that takes advantage of distributed robot software. In addition, work has been performed to develop cloud services suited for robots [7], [8].

Connection of robots to clouds brings about many other benefits, e.g. the ability to integrate the robot with a network of devices, such as the Internet of Things (IoT) or wireless sensor networks [9], [10] where the machine is able to sense the environment with distributed sensors and act upon the enivronment with external effectors, being a part of a distributed network.

Distribution of the control system between the on-board computer and a cloud, and its integration with IoT opens new research paths. One of them focuses on the design of a distributed robot software architecture [11] and on the development of a software framework by means of which this concept may be implemented. The key issue that needs to be considered in the design process is the requirement for a short response time. A significant share of robot control systems requires real time constraints to be satisfied [12]. Additionally, end users expect responsivity, i.e. a short lead time between task request and the beginning of its execution. Robot software architectures should also be developer-friendly. Fast prototyping and quick implementation of robot tasks should be considered a standard requirement.

Another research area that is crucial for the integration of robots and IoT is cyber-security of such distributed systems. A robot, being a software-controlled machine, should be well tested against various cyber-attacks and developers of robot systems should be aware of vulnerabilities of robot programming frameworks and components. However, most of the projects implement its own connections with the cloud (sometimes even as plain text, as it's not the main scope of these works), and robot control system designers do not pay enough attention to protect the systems against cyber-attacks.

As robots are connected to the Internet and rely upon sensors and effectors, they are considered to be cyber-physical systems (CPS) [13]. While no commonly accepted defini-

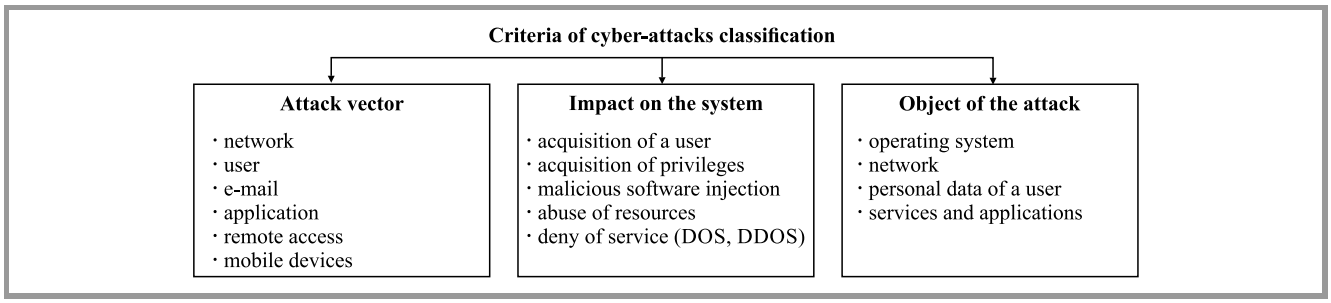

Fig. 1. Example of criteria for classification of cyber-attacks.

tion of CPS exists, we may state that it is a specifically designed network of collaborating components used to monitor and control the physical world. There are two types of components: "cyber" (computation, communication) and physical (e.g. sensors, effectors). Such components are integrated, their operation is monitored and managed [14]. It is expected that CPS, when connected to the Internet, may revolutionize many areas, e.g. transport, healthcare, manufacturing, agriculture, military, civil and space engineering. Many attacks on CPS area have been identified and categorized to date [14], [15]. Some examples of criteria used for the classification of cyber-attacks are: attack vector (route or means by which the attacker acquires access to a system or network), impact on the system, object of the attack.
Specific cases for each of those types are presented in Fig. 1. The examples of consequences of a CPS cyber-attack include the following:

- physical damage to a CPS device and/or objects within its environment,
- financial and image-related losses of the user/developer,
- injuries or death of people.

More threats and potential consequences of cyber-attacks on CPS are discussed in [16].
Many types of devices are classified as CPS and they differ in terms of the potential threats and consequences of cyber-attacks. Robots are usually well-equipped with sensors (e.g. RGB, RGB-D, IR and time-of-flight cameras, microphones, inertial measurement units, laser scanners, IR emitters) and they are able to move around. Therefore, this type of CPS should be considered as particularly vulnerable to a wide range of risk categories arising from cyber-threats.
In this paper we present cyber-attacks that are specific for CPS, methods for identification of such cyber-attacks and tools to protect against them. Section 2 contains an analysis of the different types of cyber-attacks, methods of their detection and CPS security-related issues. In Section 3, a survey of issues related to cyber-security of robots, based on the analysis performed, is presented. Section 4 discusses future work and research areas in the field of robot cyber-security.

2. Cyber-security in Cyber-Physical Systems

Stuxnet was one of the first worms used against CPS [17]. It was discovered in June 2010 and was used to attack industrial installations. Its impact was huge – the authors of the report [17] estimate that approximately 100,000 hosts from over 155 countries were infected. The successor of this worm – Industroyer malware – was used in a cyber-attack on Ukraine's power grid that deprived a part of its capital, Kiev, of power for an hour [18]. The next recent attack relied on ransomware with which the Office of Urban Transport in San Francisco (SMFTA) was infected. In October 2016, a hacker hashed 900 computers that belonged to the SMFTA. The attack disabled the ticket distribution system and the value of the ransom required was 73,000 USD.
It is quite obvious that the problem of cyber-security in cyber-physical systems is essential not only for the industry, state offices and city authorities, but also for almost every single person. The cost of the ransom, repairs of damaged systems, reconstruction of important data is huge and may impact the reliability of a company, a government or any other attacked institution. Some countries have established organizations to coordinate various aspects of cyber-security and cyber-attack mitigation efforts. In the US, such an entity is known as The National Cyber-security and Communications Integration Center (NCCIC). In its 2016 report [19], the organization published statistical data pertaining to incidents that have been identified and technologies used during the attacks. Figure 2 is based on data from this report and presents the prevalence of known threat vectors in CPS. Based on its annual reports, NCCIC released a cyber-security review tool – the Cyber Security Evaluation Tool (CSET). It contains a set of questionnaires, analyzes the answers given and generates a set of graphs and plots that visualize the strong and the weak points of the system concerned. The program gives also recommendations to enhance the level of protection. Many projects and papers are available that refer to methods used for anomaly, breach and cyber-attack detection and defense in CPSs [15], [20], [21].
It should be noted that the above analysis is focused on industrial installations based on the CPS concept. Technological evolution makes it possible to create CPS devices that are used in private homes, e.g. small service robots,

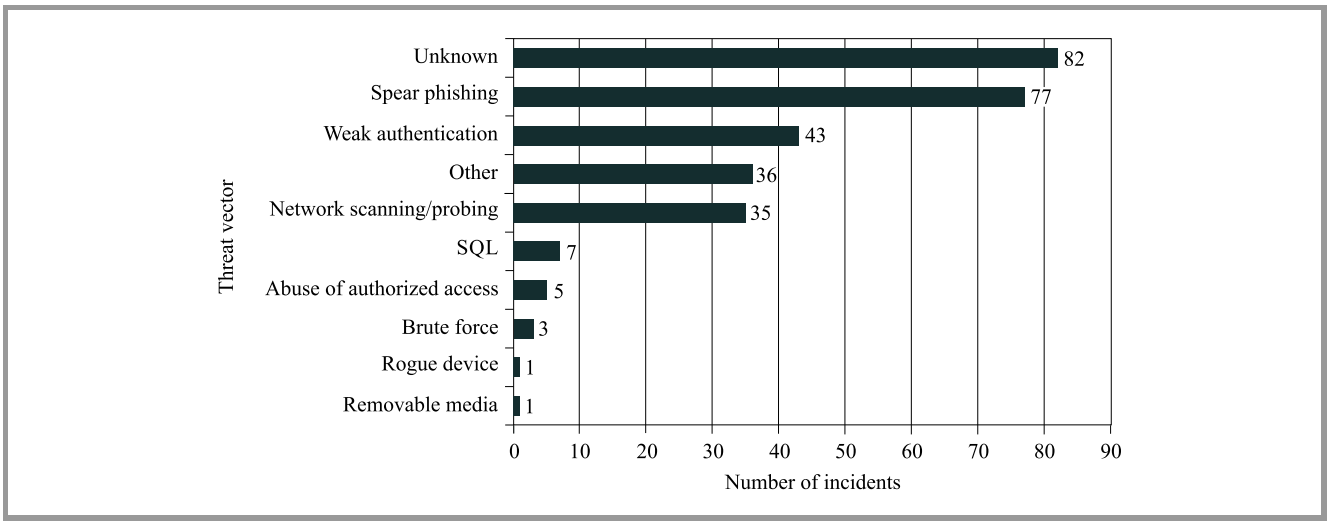

Fig. 2. Prevalence of known threat vectors in the case of CPS [22].

toys and appliances connected to the Internet. A robot that has been conquered poses an obvious physical threat residents (especially the young ones). Such a device may also exert a strong impact on human privacy and compromise sensitive data (bank accounts, passwords, etc.), or may be used to blackmail the device user. By collecting information, a corrupted robot may be also used as an element of a more sophisticated attack. In contrast to industry workers, people at home are neither aware of cyber-security, nor trained on how to diagnose a cyber-attack.

The security of CPS is mainly based on seven security functions that have been proposed for IT systems in the ISO/IEC 10746-3 [23] standard:

- **access control** – prevents unauthorized interactions with an object,
- **security audit** – ensures that security-related information is collected and monitored. Such information is analyzed to review security policies and procedures,
- **authentication** – guarantees that a given object is identified properly,
- **integrity** – detection and/or prevention of an unauthorized creation, alteration or deletion of data,
- **confidentiality** – prevents unauthorized disclosure of information,
- **non-repudiation** – provides assurance that a given object is/was involved in all or part of the interaction,
- **key management** – provides mechanisms for the management of cryptographic keys and includes all of the following key-related operations: generation, registration, certification, deregistration, distribution, storage, archiving and deletion.

The above functions are used to achieve three main security-related objectives:

- **integrity** – maintaining the reliability of data sources,
- **availability** – providing access to the system and its services,
- **confidentiality** – hiding data from unauthorized objects.

The authors of [24] reveal that although CPS are based on information systems, there is a need to widen the definition of integrity, availability and confidentiality due to physical elements of CPS. For example, providing integrity in CPS means also an ability to remain operational in the case of an attack on sensors or effectors. Furthermore, availability of CPS should take into consideration a scenario in which an attack is performed on the network of sensors, control-related transmissions and on actions performed by effectors. One of the tasks of CPS is to register information about its environment. Because of that, in many applications there is a high risk of corruption of the user's privacy. Moreover, reasoning about the state of CPS based on its inter-component communication is yet another important threat.

In order to perform the aforementioned security functions, system developers rely on a variety of tools to secure CPS. The classification of tools that were presented in [24] (Table 1) is used as well. Prevention tools are used to limit the range of threats to the system. Every object of the system and any object that cooperates with the system should be identified, should operate with a limited access, and messages that the objects exchange should be protected. Reactive tools comprise a collection of mechanisms that are activated during an attack. Intrusion Detection System (IDS), for example, observes the communication patterns and behaviors of objects within the entire system [25], [26]. Its role is to identify any exceptional situations, behaviors or any undesired actions within the system that may be the trace of an attack. The attacker's model is a profile of threats and potential attack scenarios affecting the system.

Table 1
Tools and functions used for securing cyber-physical systems

Prevention	Reaction	Adversary model
Authentication	Intrusion Detection System	Assumptions of probable attacks
Access control	Key revocation	Threat profile
Redundancy of communication channels, diversity of technology and secure methods		Identifiers of trusted system elements
Message signatures and freshness		
Managing access privileges of system components		
Tools for security verification		

It offers a whole picture of the system's security, and as the development of the adversary model progresses, security updates are released.

3. Mobile Robot Cyber-security Survey

Robots are complex CPS systems, thus their cyber-security still poses a big challenge. Frequently, security systems developed for conventional information systems are insufficient and cannot be implemented in a scenario with mobile robots. Some of the security systems demand too much computational and storage resources, while others are incorrect due to insufficient experimental data or inaccurate adversary models. Most of works described in the literature consider the detection of an attack on a robot system only. There are many works regarding IDS, and some studies on securing specific components of the robot system. Table 2 shows the selected, recent works that consider the implementation of cyber-security functions in the robotics domain. The survey presents a comparison taking into account the following aspects:

- considered security functions and attack vectors,
- methods used to establish the security function,
- data needed by the method to realize the function,
- purpose of the solution (prevention against an attack, detection of an attack and reaction in the case of an attack).

The first two papers [21], [27] are concerned with the principles of research on robot cyber-security and with a general analysis of the issue. In [21], authors present a study and some clues for conducting experiments related to robot cyber-security, in the event of a sensor spoofing attack[1]. Furthermore, the work presents an analysis of machine vulnerabilities and attack detection methods. The purpose of the work is to maintain proper behavior of the system. However, the authors do not address the problems of ensuring the privacy of users (e.g. confidentiality of user data). Paper [27] describes the process of research platform design, as well as presents metrics and key performance indicators for robot security analysis.

Recent works concentrate on the threat detection aspect. Authors of [28], [29] propose an algorithm to detect an attack based on the network traffic analysis, data gathered and the physical system parameters. The algorithm relies on machine learning and rule tracking methods. Papers [30], [31] present algorithms which are also based on machine learning. This work, however, uses them to secure the Real-Time Locating System (RTLS). Based on data gathered by the localization system, the algorithm identifies a potential attack.

Detection of the attack on the robot system has also been considered by the authors of [32]. Their solution is based on confronting sensor data with the robot motion dynamic model, and on identification of potential anomalies. In work [33], a security audit of a popular robot programming framework – ROS – is described. The authors identify a potential threats, propose lightweight security mechanisms for the application level and a key management component for the ROS framework. Most of the above works focus on the prevention and detection aspects of the security system. In paper [34], authors describe the recursive state estimator that compares the calculated state with measurements obtained from redundant sources. The algorithm returns a high variance of measurement noise for the compromised sensor driver. The solution requires a well-defined noise profile for every sensor used. An inaccurate profile for a given sensor may result in the rejection of most of its measurements, or in the acceptance of data crafted by the attacker.

The most recent work [35] targets securing the successor of ROS – ROS2. A new release of the framework is expected to be more suitable for real world applications and for implementing robots to the IoT environment. The work

[1] Set of attacks that are based on imitations of the system's elements and that rely on injecting crafted data packets into the communication network of the system.

Table 2
A survey of recent studies on implementation of cyber-security functions in the robot systems

Work	Cyber-security function	Attack vector	Method used	Data required	Purpose
[21]	Security audit, integrity	Injection, sensor spoofing, hidden attacks	Penetration testing	Tests results and conclusions	Detection
[27]	Security audit	DoS	Construction of the research platform, determination of key performance indicators	Analysis of the platform tests	Prevention
[28], [29]	Access control, integrity	DoS, data injection, malware	Tracking of the defined rules, machine learning	Network traffic, obtained data, robot speed, physical vibration, power consumption	Detection
[30], [31]	Integrity	DoS, sensor spoofing	Machine learning	Data from the RTLS localization system	Detection
[32]	Integrity	Sensor spoofing, logic bomb, signal interruption, physical damage	Comparison of real-time data with dynamics model of the physical system, anomaly spotting	Dynamics equations of the physical system	Detection
[33]	Security audit, key management, non-repudiation, confidentiality	Injection, unauthorized access, DoS	Threats analysis, penetration tests	Conclusions and results of the tests	Prevention
[34]	Integrity	Sensor spoofing	Sensor data fusion	Redundancy of data sources	Reaction

describes the implementation of a secure data distribution service (DDS) into the ROS2 framework. The method provides valuable tools for securing robot systems that utilize the ROS2 framework and offers procedural provisioned access control policies for the software layer. Moreover, the authors of the article show a method for the verification of compliance between generated transport artifacts and decision point implementation.

4. Research Paths in Cyber-security for Robots

Our analysis of the literature regarding cyber-security of robots has identified numerous open research issues. The most obvious one is the fragmentary character of secure systems. Juxtaposition of potential threat vectors that are typical of CPS (Fig. 2), and of the security solutions proposed in the literature shows some crucial gaps in the robot security systems.

For example, there is a shortage of methods protecting against spear phishing[2]. Gaps in the robot cyber-security system may provide access to a considerable amount of crucial, personal information about the victim and his or her family. Such information may be used, for instance, to submit blackmail or ransom demands. Moreover, an attacker using an unsecured robot may gain access to confidential information or the victim's passwords.

[2] Directed form of a phishing attack. Fake messages are being sent to a specific organization or person in order of gain access to confidential information.

In order to develop a secure robot system, a need exists to design a security policy for such a system. This issue is another research area that required more attention. The abovementioned CSET tool that verifies the security of CPS is a good clue for the task of designing a similar tool suitable for robot systems. It should take into account the vulnerabilities, threats and attack vectors that are specific for robot systems.

One of the greatest challenges in the field of robot security is the design of a range of methods that will cover every aspect of service robot cyber-security. Service robots usually utilize a control system that is extremely complex and often distributed across the network. Furthermore, it is well equipped with a great variety of sensors that are used to investigate the environment. The first step in the design of a security system for such a robot is to define threats and vulnerabilities of a typical service robot control system. This step should be followed by the design of secure methods and tools. Figure 3 presents the result of a preliminary analysis of such system threats. The analysis has rendered the following conclusions.

A robot application that uses a low-level robot controller gains access to critical information about the environment and the robot itself. Furthermore, it has the ability to command robot effectors. Therefore, every application that may interact with the low-level controller should require authentication. Such a security mechanism is especially crucial in a situation in which robot applications are downloaded from a remote repository.

Developers of low level controllers should take into account a possibility of the attacker hindering communication

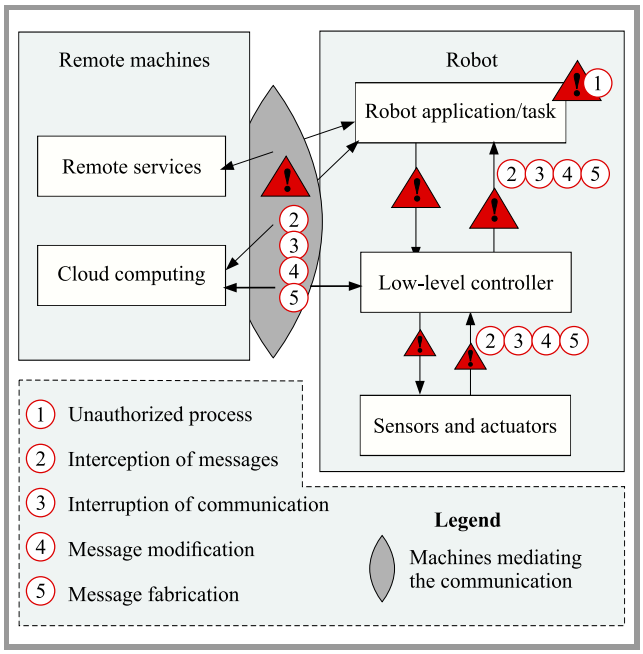

Fig. 3. Examples of threats to a complex, distributed control system of a service robot.

with hardware. One of the possible solutions is to develop a built-in IPS[3] into the robot system, or at least provide interfaces to integrate one. This kind of security mechanism depends on the robot structure and the equipment (especially the sensors) used. Therefore, it is difficult to devise both a complete and a universal model of a security system for robots.

Nowadays, when robots frequently utilize cloud computing, developers should address the issue of secure communication between these entities. As information exchange is performed by two computers through the network, this aspect of the robot cyber-security domain is similar to the well-known security aspect of information systems. The main differences are in the data that is transferred and in the Quality of Service (QoS) required, as some parts of the robot system are controlled in real time.

Developers of robot systems and providers of remote services for robots should define and disseminate standards of secure communication applicable to robot systems, so that various types of robots could take advantage of services rendered by different providers.

Another remark based on the cyber-security analysis of the service robot system performed is that the current classification of cyber-attacks (Fig. 1) is insufficient and needs to be supplemented with new subgroups.

Taking into account that both robot structures and their software are frequently application-specific, the design of a robot security system model is necessary. It would empower developers of a dedicated robot system to deliver more secure machines. Moreover, there is another crucial area in the field of robots cyber-security that has not been addressed so far, namely design and implementation of reaction methods relied upon in the event of a cyber-attack. The easiest one would be to restart the robot software from a backup. However, in some configurations and during execution of some tasks, the machine should not be shut down. Such a reaction may result in damage to the robot or the environment, or may even may threaten the health or life of people present nearby.

[3] IPS (Intrusion Prevention Systems) is designed to protect the secured system from attacks by detection of an intrusion and prevention from carrying out of one. IPSs are either software or hardware based.

5. Summary

Service robots are equipped with many types of sensors. They acquire a lot of information about the surrounding environment. Access to such data has to be well protected, or an unauthorized person may collect confidential information about the user or even take over control of the robot to inflict damage on the environment or its owner. Leakage of confidential information may be related to: presence of people, passwords and logins, banking information and many other domains.

Moreover, media reports about attacks on the privacy of many people will undoubtedly have a negative impact on the sale of service robots. Hence, the interest of potential investors in financing research in this area. In addition to known types of attacks on IT systems, service robots may be affected by specific attack vectors, and after by-passing security, the attacker will have access to a well-equipped spying device. Therefore, security solutions used in traditional ICT systems are not sufficient for robotic system applications.

It is necessary to develop appropriate methods for securing service robots against cyber-attacks. Several such methods are already known, but they do not provide consistent and comprehensive protection against all known attack vectors. New and robot-specific solutions are still expected in response to the newly identified vulnerabilities and threats. Additionally to the development of new security features and identification of new threats related to the service robots operating in domestic environment, it is necessary to devise a comprehensive protection module that will be easily integrable with service robot controllers. Such a module should be configurable due to a variety of machine structures and applications, whereas it should not significantly affect the implementation of the task itself while working in the mode of identification of a potential attack. In addition, invention of cyber-attack detection and defense methods that depend on the task being currently performed is needed.

Acknowledgements

This work constitutes a part of the CYBERSECIDENT/ 369195/I/NCBR/2017 project supported by the National Centre of Research and Development, within the framework of the CyberSecIdent Programme.

References

[1] T. Winiarski, K. Banachowicz, and D. Seredyński, "Multi-sensory feedback control in door approaching and opening", in *Intelligent Systems '2014. Proceedings of the 7th IEEE International Conference Intelligent Systems ISñ2014, September 24-26, 2014, Warsaw, Poland, Volume 2: Tools, Architectures, Systems, Applications*, D. Filev, J. Jabłkowski, J. Kacprzyk, M. Krawczak, I. Popchev, L. Rutkowski, V. Sgurev, E. Sotirova, P. Szynkarczyk, S. Zadrozny, Eds. Springer, 2015, pp. 57–70 (doi: 10.1007/978-3-319-11310-4_6).

[2] A. M. Okamura, M. J. Mataric, and H. I. Christensen, "Medical and health-care robotics", *IEEE Robotics & Autom. Mag.*, vol. 17, no 3, pp. 26–37, 2010 (doi: 10.1109/MRA.2010.937861).

[3] T. Winiarski, W. Kasprzak, M. Stefańczyk, and M. Wałęcki, "Automated inspection of door parts based on fuzzy recognition system", in *Proc. 21th IEEE Int. Conf. on Methods and Models in Autom. and Robot. MMAR'2016*, Międzyzdroje, Poland, 2016, pp. 478–483 (doi: 10.1109/MMAR.2016.7575182).

[4] M. Tenorth and M. Beetz, "KnowRob – knowledge processing for autonomous personal robots", in *Proc. IEEE/RSJ Int. Conf. on Intell. Robots and Syst. IROS 2009*, St. Louis, NO, USA, 2009, pp. 4261–4266 (doi: 10.1109/IROS.2009.5354602).

[5] C. Zieliński *et al.*, "Variable structure robot control systems: The RAPP approach", *Robot. and Autonom. Syst.*, vol. 94, pp. 226–244, 2017 (doi: 10.1016/j.robot.2017.05.002).

[6] W. Dudek, K. Banachowicz, W. Szynkiewicz, and T. Winiarski, "Distributed NAO robot navigation system in the hazard detection application", in *Proc. 21st Int. Conf. on Methods and Models in Autom. and Robot. MMAR 2016*, Międzyzdroje, Poland, 2016, pp. 942–947 (doi: 10.1109/MMAR.2016.7575264).

[7] R. Doriya, P. Chakraborty, and G. Nandi, "Robot-cloud: A framework to assist heterogeneous low cost robots", in *Proc. Int. Conf. on Commun., Inform. & Comput. Technol. ICCICT 2012*, Mumbai, India, 2012 (doi: 10.1109/ICCICT.2012.6398208).

[8] W. Dudek, W. Szynkiewicz, and T. Winiarski, "Cloud computing support for the multi-agent robot navigation system", *J. of Autom., Mob. Robot. and Intell. Syst.*, vol. 11, no 2, pp. 67–74, 2017 (doi: 10.14313/JAMRIS_2-2017/18).

[9] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: A survey", *J. of Netw. and Comp. Appl.*, vol. 88, pp. 10–28, 2017 (doi: 10.1016/j.jnca.2017.04.002).

[10] E. Niewiadomska-Szynkiewicz and A. Sikora, "A software tool for federated simulation of wireless sensor networks and mobile ad hoc networks", in *Applied Parallel and Scientific Computing, PARA 2010, Reykjavík, Iceland, June 6-9, 2010, Revised Selected Papers, Part I*, K. Jónasson, Ed. *LNCS*, vol. 7133, pp. 303–313, Berlin, Heidelberg: Springer, 2012 (doi: 10.1007/978-3-642-28151-8_30).

[11] A. Ahmad and M. A. Babar, "Software architectures for robotic systems: A systematic mapping study", *J. of Syst. and Software*, vol. 122, pp. 16–39, 2016 (doi: 10.1016/j.jss.2016.08.039).

[12] F. Dietrich *et al.*, "Dynamic distribution of robot control components under hard realtime constraints–modeling, experimental results and practical considerations", *J. of Syst. Architecture*, vol. 59, no. 10, pp. 1047–1066, 2013 (doi: 10.1016/j.sysarc.2012.12.001).

[13] R. R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, "Cyber-physical systems: the next computing revolution", in *Proc. of the 47th Design Autom. Conf.*, Anaheim, CA, USA, 2010, pp. 731–736 (doi: 10.1145/1837274.1837461).

[14] Y. Ashibani and Q. H. Mahmoud, "Cyber physical systems security: Analysis, challenges and solutions", *Computers & Secur.*, vol. 68, pp. 81–97, 2017 (doi: 10.1016/j.cose.2017.04.005).

[15] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-physical systems security – a survey" *IEEE Internet of Things J.*, vol. 4, no. 6, pp. 1802–1831, 2017 (doi: 10.1109/JIOT.2017.2703172).

[16] C. W. Axelrod, "Managing the risks of cyber-physical systems", in *Proc. IEEE Long Island Syst., Appl. and Technol. Conf. LISAT 2013*, Farmingdale, NY, USA, 2013 (doi: 10.1109/LISAT.2013.6578215).

[17] N. Falliere, L. O. Murchu, and E. Chien, "W32.stuxnet dossier", White paper, Symantec Corp., Security Response, vol. 5, no. 6, p. 29, 2011 [Online]. Available: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

[18] A. Cherepanov and R. Lipovsky, "Industroyer: Biggest threat to industrial control systems since Stuxnet", 2017 [Online]. Available: https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/ (accessed 15 Nov., 2018).

[19] National Cybersecurity and Communications Integration Center, ICS-CERT Year in Review, 2016 [Online]. Available: https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2016_Final_S508C.pdf (accessed 15 Nov., 2018).

[20] J. Giraldo, E. Sarkar, A. A. Cardenas, M. Maniatakos, and M. Kantarcioglu, "Security and privacy in cyber-physical systems: a survey of surveys", *IEEE Design Test*, vol. 34, no. 4, pp. 7–17, 2017 (doi: 10.1109/MDAT.2017.2709310).

[21] G. Sabaliauskaite, G. S. Ng, J. Ruths, and A. Mathur, "A comprehensive approach, and a case study, for conducting attack detection experiments in cyber–physical systems", *Robot. and Autonom. Sys.*, vol. 98, pp. 174–191, 2017 (doi: 10.1016/j.robot.2017.09.018).

[22] National Cybersecurity and Communications Integration Center, Incident response pie charts FY2016, 2016 [Online]. Available: https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2016_IR_Pie_Chart_S508C.pdf (accessed 15 Nov., 2018).

[23] "ISO/IEC JTC 1/SC 7 security functions iso/iec 10746-3" [Online]. Available: http://joaquin.net/ODP/Part3/15.html (accessed 15 Nov., 2018).

[24] A. A. Cardenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems", in *Proc. 28th Int. Conf. on Distrib. Comput. Syst. Worksh. ICDCS'08*, Beijing, China, 2008, pp. 495–500 (doi: 101109/ICDCS.Workshops.2008.40).

[25] A. A. Aburomman and M. B. Ibne Reaz, "A survey of intrusion detection systems based on ensemble and hybrid classifiers", *Computers & Secur.*, vol. 65, pp. 135–152, 2017 (doi: 10.1016/j.cose.2016.11.004).

[26] P. Szynkiewicz and A. Kozakiewicz, "Design and evaluation of a system for network threat signatures generation", *J. of Computat. Sci.*, vol. 22, pp. 187–197, 2017 (doi: 10.1016/j.jocs.2017.05.006).

[27] T. A. Zimmerman, "Metrics and Key Performance Indicators for Robotic Cybersecurity Performance Analysis", US Department of Commerce, National Institute of Standards and Technology, 2017 [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8177.pdf

[28] T. P. Vuong, G. Loukas, D. Gan, and A. Bezemskij, "Decision tree-based detection of denial of service and command injection attacks on robotic vehicles", in *Proc. IEEE Int. Worksh. on Inform. Forensics and Secur. WIFS2015*, Rome, Italy, 2015 (doi: 10.1109/WIFS.2015.7368559).

[29] T. P. Vuong, G. Loukas, and D. Gan, "Performance evaluation of cyber-physical intrusion detection on a robotic vehicle", in *Proc. IEEE Int. Conf. on Comp. and Inform. Technol.; Ubiquitous Comput. and Commun.; Dependable, Auton. and Secure Comput.; Pervasive Intell. & Comput. CIT/IUCC/DASC/PICOM 2015*, Liverpool, UK, 2015, pp. 2106–2113 (doi: 10.1109.CIT/IUCC/DASC/PICOM.2015.313).

[30] Á. M. Guerrero-Higueras, N. DeCastro-García, F. J. Rodríguez-Lera, and V. Matellán, "Empirical analysis of cyber-attacks to an indoor real time localization system for autonomous robots", *Computers & Secur.*, vol. 70, pp. 422–435, 2017 (doi: 10.1016/j.cose.2017.06.013).

[31] Á. M. Guerrero-Higueras, N. DeCastro-García, and V. Matellán, "Detection of cyber-attacks to indoor real time localization systems for autonomous robots", *Robot. and Auton. Syst.*, vol. 99, pp. 75–83, 2018 (doi: 10.1016/j.robot.2017.10.006).

[32] P. Guo, H. Kim, N. Virani, J. Xu, M. Zhu, and P. Liu, "Exploiting physical dynamics to detect actuator and sensor attacks in mobile robots", *arXiv preprint arXiv:1708.01834*, 2017.

[33] B. Dieber *et al.*, "Security for the robot operating system", *Robot. and Auton. Syst.*, vol. 98, pp. 192–203, 2017 (doi: 10.1016/j.robot.2017.09.017).

[34] N. Bezzo et *al.*, "Attack resilient state estimation for autonomous robotic systems", in *Proc. IEEE/RSJ Int. Conf. on Intell. Robots and Syst. IROS 2014*, Chicago, IL, USA, 2014, pp. 3692–3698 (doi: 10.1109/IROS.2014.6943080).

[35] R. White, G. Caiazza, H. Christensen, and A. Cortesi, "Procedurally provisioned access control for robotic systems", in *Proc. IEEE/RSJ Int. Conf. on Intell. Robots and Syst. IROS 2018*, Madrid, Spain, 2018, arXiv:1810.08125 [cs.RO].

Wojciech Dudek received his B.Sc. and M.Sc. degrees in Automation and Robotics from WUT and is currently a Research Assistant at Warsaw University of Technology (WUT), Institute of Control and Computation Engineering. His M.Sc. thesis has been recognized with the 1st place in the 2017 Young Innovators' Competition organized by the Industrial Research Institute for Automation and Measurements (PIAP). He is a contributor to international projects i.a. RAPP (European Commission – FP 7) and INCARE (European Commission AAL Joint Programme). His scientific interests focus on mobile robot control systems, their localization and navigation and harmonization of their tasks.

https://orcid.org/0000-0001-5326-1034
E-mail: wojciech.dudek@pw.edu.pl
Institute of Control and Computation Engineering
Warsaw University of Technology
Nowowiejska 15/19
00-665 Warsaw, Poland

Wojciech Szynkiewicz received his Ph.D. and D.Sc. (habilitation) degrees in Control and Robotics both from the Warsaw University of Technology (WUT). He works at WUT's Institute of Control and Computation Engineering. His research activities concentrate on multi-robot systems, sensor based motion planning, autonomous navigation of mobile robots, robot controller structures and robot cybersecurity. He is the author and co-author of over 90 papers published in conference proceedings, journals and books concerned with the above mentioned research subjects.

https://orcid.org/0000-0001-6348-1129
E-mail: W.Szynkiewicz@elka.pw.edu.pl
Institute of Control and Computation Engineering
Warsaw University of Technology
Nowowiejska 15/19
00-665 Warsaw, Poland