Analysis Of Attacks In Modern Cyberphysical Systems

Yurii Shcherbyna
Dept. Automated Systems and Cybersecurity
Odesa State Academy of Technical Regulation and Quality
Odesa, Ukraine
shcherbinayura53@gmail.com

Nadiia Kazakova
Dept. Information Technologies
Odesa State Environmental University
Odesa, Ukraine
kaz2003@ukr.net

Oleksii Fraze-Frazenko
Dept. Information Technologies
Odesa State Environmental University
Odesa, Ukraine
frazenko@gmail.com

Lubomir Parchuts
dep. protection of information
Lviv Polytechnic National University
Lviv, Ukraine
par7@i.ua

Sergey Schneider
dep. Information Security
Lviv Polytechnic National University
Lviv, Ukraine
shnapi007@gmail.com

***Abstract*—Cyber-physical systems, representing the integration of computing, network and physical processes, are increasingly being implemented into critical infrastructure, processes of community management and private life of people. Due to their excessive complexity, the number of vulnerabilities in both the software and the physical part of the equipment significantly increases, which in turn leads to increased risks from the implementation of possible threats. Implementation of the overwhelming part of cyber threats occurs through intelligent telecommunication networks, attacks on data transmission protocols, intellectual part of data sources in executive mechanisms of systems, as well as local control centers of the system. The construction of adequate requirements for the system of cybernetic protection implies a careful approach to the study of the architecture and technical features of the cyberphysical system to be protected. As in any real engineering system, in systems of protection of cyber-physics systems, modeling of internal processes plays a key role in the analysis of their dynamic behavior. It is shown that the only model of the cyberphysical system is to describe at the formal level in spatial and temporal measure all possible connections between the cybernetic and physical parts of the functioning environment and to substantiate the characteristics that determine the quality of its functioning. This analysis of published works shows that the most dangerous attacks used by security breachers in cybernetic space are divided into attacks such as DoS attacks, Replay attacks and Deception attacks. It is against the attacks of this type that the efforts of specialists in the field of cybernetic defense are concentrated. It is shown that ensuring stability, security and reliability of protection is based on solving the problem of multi-purpose optimization.**

***Keywords*—Cyber-physical system, Cyber-security, Cyber-Attack, DoS attack, Replay attack, Deception attacks, Wormhole attack, cyberspace, physical space.**

I. INTRODUCTION

The use of cyberphysical systems to improve the management of society and complex technological processes, lead to radical changes in society itself. Such systems are based on intelligent networks (Smart Grid), which can significantly increase the efficiency of automation of power infrastructure management, telecommunications and defense systems and other objects of strategic importance. Smart Grid first appeared as a term in the West to use a description of everything related to the automation, control and management of power supply systems components [1]. Today, the term Smart Grid is used in those areas where information collection and processing systems are implemented, and equipment condition monitoring in large complex systems [2]. Along with the benefits of public life = , production and business digitalization, the threat of using digital systems to interfere in the sphere of other people's interests with malicious purposes is growing. As a result, there is a growing need to explore issues related to responding to operational events related to resource recovery, security control, and automation.

The use of cyberphysical systems involves the implementation of appropriate infrastructure, which should increase the reliability and security of all aspects of its operation. Due to its complexity and the fact that the basis of such infrastructure is intelligent information and telecommunications networks, increases the probability of attacks from the external environment on critical management procedures, the implementation of which may allow attackers to manipulate measurements, load conditions and other critical system parameters [3]. Thus, the importance of constant monitoring of risks in the operating environment of the system and timely prevention of illegal interference is obvious. It follows that the cybersecurity system is one of the main components of any modern cyberphysical system [4].

II. FORMULATION OF THE PROBLEM

With the cyberphysical systems development , security problems arise in both their physical and cyber spaces [5]. The modern cyberphysical systems architecture allows the violator to carry out parallel coordinated attacks from external cyberspace on elements of their infrastructure and management. The consequences of such attacks can be events that pose a threat to human life, man-made disasters and large material losses.

The cybersecurity system should reduce the risks of threats, detect and identify abnormal system behavior, respond to intrusions, and initiate countermeasures to mitigate the effects of such threats and quickly restore normal operation.

Extensive security research on modern cyberphysical systems has identified a significant number of attack scenarios based on specific vulnerabilities, their targets, and the resources required to implement them. The results of such an analysis form the basis for the organization of appropriate protection [6].

The security systems reliability is determined by careful analysis of physical and cyber environments for the presence of intentional and unintentional events that lead to threats, so the purpose of this work is to review the current state of the most common cyber attacks and defense strategies scenarios.

III. MAIN PART

The appear of cyberphysical systems does not require a fundamental revision of the protection theory. Its main part is still network protection, and the main attacks type are attacks on communication protocols, identification and authentication mechanisms, as well as key distribution mechanisms. At the same time, the features of cyberphysical systems and their gradual improvement give rise to new scenarios and types of attacks. In relation to traditional security systems, cyberspace protection systems are still in their infancy, and studies have already identified a large number of vulnerabilities that could lead to catastrophic attacks. Although a strategy for protection and detection or mitigation already exists for most of the detected attacks, this problem is far from being resolved.

Given the vulnerabilities of cyberphysical systems, attacks can be implemented covertly and unpredictably [7]. Thus, an attacker could alter control information by forging packets intercepted in the control loop using viral software, illegally accessing process monitoring centers to disrupt their normal operation. Thus, the dynamics of the system can be disrupted if its protection is not provided at the appropriate level and, therefore, cyber attacks are considered the main type of threats in cyberspace.

Effective defense can be organized if it is based on mathematical models of attacks. Modeling plays a key role in analyzing and understanding the violators' behavior dynamics . From a practical and theoretical point of view, it is important to build a model of a single system before any analysis. An example of a model that considers a cyberphysical system as a dynamic system with distributed parameters and a high degree of automation and is used by specialists in various fields is the model described in [8]. It makes it possible to formally determine such system characteristics as asynchrony of measurements in time and control, network packet delays and the state of coherence of processes in the system. Within modeling-based analysis, it is important that attacks be formally described at the mathematical level. Currently, the most popular and described in scientific journals attacks can be divided into the following categories: attacks such as "denial of service" (DoS attacks), Replay attacks and Deception attacks.

The most common attack type is DoS attack. With their help, violators manage to make system resources inaccessible. Typically, they constantly send "empty" messages to the smart network domain buffers and thus block them by overloading. This allows you to block one or another of its resources and make it impossible to exchange data between system entities or change the routing protocol. For quantitative analysis of the reduction of system performance from such attacks use queuing models, and also Markov and Bernoulli models.

Attacks build on queuing models can be described as time-delayed systems, which will effectively solve the problem of stability [9]. In [10], based on the analysis of the schedule of DoS-attacks, the substantiation of the method of calculating the average error in the operation of the intrusion detection system is given. DoS-attack models based on the Bernoulli scheme, although describing different mechanisms, are the same, which makes it possible to effectively analyze the performance of cyberphysical systems, using typical approaches for missed measurements.

The next type of dangerous that is common in cyberspace are Replay attacks. This is an attack on the authentication system by recording and then playing the correct message or part of it [11]. Any immutable information, such as a password or biometric data, is used to simulate authenticity. Such an attack makes it possible to gain unauthorized access to resources or transmit false data to disrupt the system.

An example of a Replay attack is an attack on cyberphysical system actuators, where packets that were previously transmitted are transmitted instead of packets containing control commands. Such an attack is not easy to identify due to the possibility of authentication procedures and, as a consequence, the normal functioning of the cyberphysical system may be disrupted.

Using a wormhole attack, attackers intercept information between two endpoints and pass it on to other attackers, thus creating a "tunnel" of control. Using this Replay-attack, violators have the ability to control management processes. Obviously, violators do not need any system information to carry out attacks.

A cryptographic authentication system is required to fight Replay attacks. It should provide for the availability of original keys for each session. In addition to the password, the packages must include timestamps and other additional control data that limit the capabilities of potential violators. The presence of such parameters makes the packets retransmission less effective.

The most common and dangerous in cyberspace is the Deception attacks. This is a type of cyber attack, the purpose of which is to intervene in physical and cybernetic processes through telecommunications systems to gain control over certain parts of the cyberphysical system [12]. In principle, deception can be defined as the interaction between two subjects - the attacker and the target of deception, in which the deceiver tries to force the target to accept the false version of reality desired by the deceiver.

Cyberspace is very different from the natural environment. First, it is much easier to hide personal information or identification data in cyberspace than in the usual interaction of subjects. Second, information in cyberspace is subject to constant change. Both of these factors contribute to the implementation of fraudulent activities in cyberspace. Therefore, deception attacks do not have a separate typical model. Their scenarios are determined depending on the goals, vulnerabilities and available resources of security violators [13].

In the case of an attack on technological systems, the main purposes of fraud attacks are sensor readings manipulation, control information forgery and access to system resources.

Over time, the fraud attacks technical complexity will increase, due to improved countermeasures. Today, there are a large number of methods to detect and stop attacks of this type. Success is based on the study of vulnerabilities and attack scenarios that have been used in the past, their assessment and finding ways to effectively counter [14]. As the attacks intensity increases, so should the variety of protection means.

IV. CONCLUSION

The main tasks of cybersecurity are to ensure the sustainable operation of cyberphysical systems by creating their mathematical models that formally take into account the smallest features of the architecture and processes of measurement, control and data exchange protocols. The presence of such models makes it possible to analyze the detected attacks, on the basis of which counteraction mechanisms are built.

Given the complexity of such systems and their components dynamic behavior, it is almost impossible to predict all possible scenarios of attacks in cyberspace. At the moment, this problem is still far from being finally solved. The published literature assumes that violators have all the necessary system information, and defenders - possible scenarios of attacks. For the most part this is the case, but not always. It follows that the main problem is the openness of intelligent networks on which cyberphysical systems are built.

The design of cyberphysical systems requires simultaneous consideration of security tasks with limited resources and compliance with the requirements of the quality of their operation. At the same time, to ensure stability, security and reliability, it is necessary to solve the problem of multi-purpose optimization.

REFERENCES

[1] Janssen M.C. The Smart Grid Drivers, PAC World, 2010, 77 p.

[2] Amin S.M., Wollenberg B.F. Toward a Smart Grid, IEEE P&E Magazine, 2005, No. 3, pp. 34-41.

[3] MoY.KimT.H.J.BrancikK. et al.: ‘Cyber–physical security of a smart grid infrastructure’, Proc. IEEE, 2012, 100, (1), pp. 195–209 (doi: 10.1109/JPROC.2011.2161428).

[4] National Institute of Standards and Technologies (NIST): ‘Guidelines for smart grid cybersecurity’ (NIST Special Publication, Gaithersburg, MD, 2014). Available at url: http://www.dx.doi.org/10.6028/NIST.IR.7628r1.

[5] SridharS.HahnA.GovindarasuM.: ‘Cyber–physical system security for the electric power grid’, Proc. IEEE, 2012, 100, (1), pp. 210–224 (doi: 10.1109/JPROC.2011.2165269).

[6] The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT): ‘Cyber-attack against Ukrainian critical infrastructure’. Alert (IR-ALERT-H-16-056-01), 2016. Available at url: https://www.ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

[7] A. D’Innocenzo, F. Smarra, M. Benedetto, Resilient stabilization of multi-hop control networks subject to malicious attacks, Automatica 71 (2016) 1–9.

[8] X. Guan, B. Yang, C. Chen, W. Dai, Y. Wang, A comprehensive overview of cyber-physical systems: from perspective of feedback system, IEEE/CAA J. Autom. Sin. 3 (1) (2016) 1–14.

[9] X.-M. Zhang, Q.-L. Han, A. Seuret, F. Gouaisbaut, An improved reciprocally convex inequality and an augmented Lyapunov — Krasovskii functional for stability of linear systems with time-varying delay, Automatica 84 (2017) 221–226.

[10] H. Zhang, P. Cheng, L. Shi, J. Chen, Optimal denial-of-service attack scheduling in cyber-physical systems, Technical Report, Zhejiang University, 2015. (Online). http://www.sensornet.cn/heng/HengestimationFull.pdf.

[11] Dutt, V., Ahn, Y. S., & Gonzalez, C.: Cyber situation awareness modeling detection of cyber-attacks with instance-based learning theory. Human Factors: The Journal of the Human Factors and Ergonomics Society, 55(3), 605-618 (2013).

[12] D. Ding, Z. Wang, Q.-L. Han, G. Wei, Security control for a class of discretetime stochastic nonlinear systems subject to deception attacks, IEEE Trans. Syst. Man Cybern.Syst. doi:10.1109/TSMC.2016.2616544.

[13] [20] D. Ding, Z. Wang, D.W.C. Ho, G. Wei, Observer-based event-triggering consensus control for multi-agent systems with lossy sensors and cyber attacks, IEEE Trans. Cybern. 47 (8) (2017) 1936–1947.

[14] Sridhar, S., Govindarasu, M.: ‘Model-based attack detection and mitigation for automatic generation control’, IEEE Trans. Smart Grid, 2014, 5, (2), pp. 580–591.