ПРИМЕНЕНИЕ МЕТОДОВ И СРЕДСТВ МОДЕЛИРОВАНИЯ

UDC 004.056.5+620.9

H. Kravtsov, Cand. Sc. (technology)
I. Kotsiuba, I. Prytulyuk, post-graduate students
Pukhov Institute for Modeling in Energy Engineering of NAS of Ukraine
(15 General Naumov St, Kyiv, Ukraine, 03164,
(044) 4249165, email: hryhoriy.kravtsov@gmail.com, i.kotsiuba@gmail.com)

The cybersecurity modeling in critical infrastructures

The attempt to systematize modern approaches to mathematical modeling of cybersecurity of critical infrastructures was made as based on a survey of open publication argueing that modern modeling and simulation are unable to handle the complexity and inter-connectedness of such critical infrastructures as smart grid.

Предпринята попытка систематизировать современные подходы к математическому моделированию кибербезопасности критических инфраструктур на основе обзора открытых публикаций, в которых утверждается, что современное состояние математического и программного моделирования не позволяет охватить всю сложность и взаимосвязанность таких критических инфраструктур как, например, интеллектуальные сети в энергетике (смарт-грид).

K e y w o r d s: critical infrastructure, cybersecurity, smart grid, vulnerability, mathematical framework, mathematical model, agent-based simulation, game theory, algebraical approach.

Introduction. The national and financial security of country depends on reliable functioning of critical infrastructure. Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, exposing the country's security, economy, and public safety and health to risk. Similar to financial and reputational risk, cybersecurity risk affects a company's bottom line. It can drive up costs and impact revenue. It can harm organization's ability to innovate, gain and maintain customers [1].

Critical infrastructure is defined in the Executive Order 13636 (EO) "Improving Critical Infrastructure Cybersecurity" (February 12, 2013, President Obama) as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economics security, national public health or safety, or any combination of those matters". Due to the increasing pressures from external threats, organizations responsible for critical infra-

structure need to have a consistent and iterative approach to identifying, assessing, and managing cybersecurity risk.

The critical infrastructure is a term used by governments to describe assets that are essential for the society and economy functioning. Most commonly associated with the term are facilities for: (a) electricity generation, transmission and distribution; (b) gas production, transport and distribution; (c) oil and oil-products production, transport and distribution; (d) telecommunication; (e) water supply (drinking water, waste water/sewage, stemming of surface water); (f) agriculture, food production and distribution; (g) heating (e.g. natural gas, fuel oil, district heating); (h) public health (hospitals); (i) transportation systems (fuel supply, railway, airports); (j) financial services (banking, clearing); (k) security services (police, military).

The electricity generation, transmission and distribution are inalienable parts of smart grid [2] that is of high priority for each economy in the world. We will use smart grid as a basis for investigation of concerns for modeling the critical infrastructures because energy is a critical resource for everyone [3, 4].

Review of modeling problems in cybersecurity of the Smart Grid. Smart grid integrates the traditional electrical power grid with information and communication technologies (ICT). Such integration empowers the providers and consumers of electrical utilities, improves the efficiency and availability of the power system while constantly monitoring, controlling and managing the demands of customers. A smart grid is a huge complex network composed of millions of devices and entities connected with each other (for example, 22 categories of interfaces between actors of the smart grid are defined) [5]. Such a massive network comes with many cybersecurity concerns. The author [6] defines the cybersecurity of the smart grid as the urgent scientific problem. We will follow the authors of [2, 5] in our understanding of vulnerabilities, attackers and types of attacks.

The following vulnerabilities are the most serious in Smart grids:

1) Customer security: Smart meters autonomously collect massive amounts of data and transport them to the utility company, consumer, and service providers. This data includes private consumer information that might be used to infer the consumer's activities, devices being used, and times when the home is empty.

2) Greater number of intelligent devices: A smart grid has several intelligent devices that are involved in managing both the electricity supply and network demand. These intelligent devices may act as attack entry points within the network. Moreover, the massiveness of smart grid network (100 to 1000 times larger than the Internet) makes the network monitoring and management extremely difficult.

3) Physical security: Unlike the traditional power system, smart grid network includes many components, and most of them are outside of the utility's

premises. This fact increases the number of insecure physical locations and makes them vulnerable in case of physical access.

4) The lifetime of power systems: Since power systems coexist with the relatively short lived IT systems, it happens that outdated equipment is still in service. This equipment might act as weak security points and might not be thoroughly compatible with the current power system devices.

5) Implicit trust between traditional power devices: Device-to-device communication in control systems is vulnerable to data spoofing where the state of one device affects the actions of another. For instance, a device sending a false state makes other devices behave unpredictably in an unwanted way.

6) Different Team's backgrounds: Inefficient and unorganized communication between teams might cause a lot of improper decisions leading to rising vulnerability.

7) Use of Internet Protocol (IP) and commercial off-the-shelf hardware and software: The use of IP standards in smart grids offers a big advantage as it provides compatibility between the various components. However, devices using IP are inherently vulnerable to many IP-based network attacks such as IP spoofing, Tear Drop, Denial of Service, and others.

8) More stakeholders: Availability of the huge number of stakeholders leads to a very dangerous kind of attack: the insider attack.

Above mentioned vulnerabilities can be exploited by attackers with different motives and expertise and could cause different levels of damage to the network. Attackers could be script kiddies, elite hackers, terrorists, employees, competitors or customers.

The attackers can be grouped into 5 groups:

1) Non-malicious attackers who view the security and operation of the system as a puzzle to be cracked. Those attackers are normally driven by intellectual challenge and curiosity.

2) Consumers driven by vengeance and vindictiveness towards other consumers making them figure out ways to shut down their home's power.

3) Terrorists who view the smart grid as an attractive target, since it affects millions of people making the terrorists' cause more visible.

4) Employees disgruntled on the utility/customers causes unintentional errors.

5) Competitors attacking each other for the sake of financial gain.

The major known attacks are:

1) Malware spreading: An attacker can develop malware and spread it to infect smart meters or company servers. Malware can be used to replace or add any function to a device or a system such as sending sensitive information.

2) Access through database links: Control systems record their activities in a database on the control system network, then they mirror the logs into the busi-

ness network. If the underneath database management systems are not properly configured, a skilled attacker can gain access to the business network database, and then use his skills to exploit the control system network.

3) Compromising communication equipment: An attacker may compromise some of the communication equipment such as multiplexers causing a direct damage or using it as a backdoor to launch future attacks.

4) Injecting false information (Replay Attack): An attacker can send packets to inject false information in the network, such as wrong meter data, false prices, fake emergency event, etc. Fake information can have huge financial impact on the electricity markets.

5) Network Availability: Since smart grid uses IP protocol and TCP/IP stack, it becomes subject to DoS attacks and to the vulnerabilities inherent in the TCP/IP stack. DoS attacks might attempt to delay, block, or corrupt information transmission in order to make smart grid resources unavailable.

6) Eavesdropping and traffic analysis: An adversary can obtain sensitive information by monitoring network traffic. Examples of monitored information include future price information, control structure of the grid, and power usage.

7) Modbus security issue: The term SCADA refers to computer systems and protocols that monitor and control industrial, infrastructure, or facility-based processes such as smart grid processes. Modbus protocol is one piece of the SCADA system that is responsible for exchanging SCADA information needed to control industrial processes.

Given that the Modbus protocol was not designed for highly security-critical environments, several attacks are possible including:

sending fake broadcast messages to slave devices (Broadcast message spoofing);

replaying genuine recorded messages back to the master (Baseline response replay);

locking out a master and controlling one or more field devices (Direct slave control);

sending benign messages to all possible addresses to collect devices' information (Modbus network scanning);

reading Modbus messages (Passive reconnaissance);

delaying response messages intended for the masters (Response delay);

attacking a computer with the appropriate adapters (Rouge interloper).

The described above vulnerabilities and attacks may be investigated by two approaches as a result of: statistical observations on objects of real critical infrastructures, and mathematical modeling (simulation) of such infrastructures.

Obviously, research in the area of cybersecurity for the objects of real critical infrastructures is unacceptable [7]. It defines a single possible way of conducting researches — a mathematical modeling for scientific issues of cybersecurity in smart grid.

Mathematical modeling and pessimism of Massoud Admin. Massoud Admin [8] argues that modern modeling, simulation, and control paradigms are unable to handle the complexity and inter-connectedness of such critical infrastructures as smart grid. Let us enumerate the targets pertinent to the control smart system:

1) Systems Science: How to retrofit and engineer a stable, secure, robust and resilient grid with large numbers of such unpredictable power sources?

2) Modeling, Simulation, Control, and Optimization of Hybrid Systems with Uncertainty: What roles will assets optimization, novel control algorithms, increased efficiency, control/coordination of energy storage, advanced power electronics, power quality, electrification of transportation, cyber security, policies, and technologies play in the smart grid of the future?

3) How can robust controls and observers be developed that can use secure sensing to identify and build realistic models and appropriate responses? Will they be able to adapt, control, and mitigate disturbances to achieve their goals?

4) Intelligent Transmission Systems/Assets include self-monitoring and self-healing and the abilities to control real-time information for smart transmission utilization. Smart, cyber-physical secured control strategies need to be developed to handle congestions, precursors to instability or reliability problems. Information exchange among renewable resources, and locational demands from plug-in hybrids/fuel cell transport systems is to be incorporated.

5) Real time monitoring sensors, communication and control technologies will constitute a linchpin infrastructure of smart power systems. However, the increased use of electronic automation raises significant issues regarding the adequacy of operational security of the automation and control systems. In addition, the use of networked electronic systems for sending, metering, scheduling, trading, or e-commerce imposes numerous financial risks implied by the use of this technology. A timely issue is merging of sensor-enabled data-based models with derived models from first principles combined with online updating (also known as data fusion in smart grid).

The Admin's conclusion [8] is pessimistic: "Mathematical/theoretical foundation is fragmented: Computational complexity, information theory, dynamical systems and control science... need for a new science of interdependent complex networks and infrastructure security".

Mathematical modeling approaches. At the same time, many researchers attempt to create mathematical framework, which can be able to solve the above described concerns.

For example, Walid Saad together with his colleagues [9] proposes to implement game theory for smart grid modeling. Their objectives are: to provide a

comprehensive description of existing game theoretic applications in smart grid networks, to identify key open problems in smart grid networks that are bound to be addressed using game theory, and to pinpoint the main game theoretic tools that can be adopted for designing the smart grid. Clearly, game-theoretic approaches present a promising tool for the analysis of smart grid systems. Nonetheless, the advantages of applying distributed game-theoretic techniques in any complex system such as the smart grid are accompanied by key technical challenges. First, one of the underlying assumptions in classical game-theoretic designs is that the players are rational, i.e., each player makes his strategy choice so as to optimize its individual utility and, thus, conform to some notion of equilibrium play. In practical control systems such as the smart grid, as the individual system nodes interact and learn their strategies, one or more nodes might deviate from the intended play and make non-rational decisions, i.e., choose unintended strategies, due to various factors such a failure or delay in learning. These inaccurate strategy choices can eventually lead to a non-convergence to the desired equilibrium and, hence, impact the overall control system stability. The impact of such bad decisions becomes more severe in practical deployments in which the smallest perturbation of the system stability can lead to outages or other detrimental consequences. As a result, when designing game-theoretic models for the smart grid, it is imperative to emphasize robustness in the model and algorithm design.

Jurica Babic [10] sees the agent-based simulation as more appropriate approach for objectives of smart grid markets modeling. She makes a conclusion that agent-based modeling is particularly suitable for the domain of energy business since electricity markets can be defined as complex adaptive systems of interactive agents. Cybersecurity and cybernetics are strongly related fields of human knowledge. This fact helps to understand that agent-based paradigm can be successfully used for simulation of cybersecurity issues in smart grid as well.

Reinhard Laubenbacher and his co-authors [11] published a special overview of issues of agent-based simulation in 2012. They show the existing mathematical frameworks (Cellular Automata, Hopfield Networks, Communicating Finite State Machines, Interacting Particle Systems and Petri Nets) and propose to use more relevant in their opinion approach of the finite dynamic system (FDS).

They operate with the following terminology:

Agent-based simulation: an agent-based simulation of a complex system is a computer model that consists of a collection of agents/variables that can take on a typically finite collection of states. The state of an agent at a given point in time is determined through a collection of rules that describe the agent's interaction

with other agents. These rules may be deterministic or stochastic. The agent's state depends on the agent previous state and the state collections of other agents with whom it interacts.

Mathematical framework: a mathematical framework for agent-based simulation consists of a collection of mathematical objects that are considered mathematical abstractions of agent-based simulations. This collection of objects should be general enough to capture the key features of most simulations, yet specific enough to allow the development of a mathematical theory with meaningful results and algorithms.

Finite dynamical system: a finite dynamical system is a time-discrete dynamical system on a finite state set. That is, it is a mapping from a Cartesian product of finitely many copies of a finite set to itself. This finite set is often considered to be a field. Dynamics is generated by iteration of the mapping.

The approach proposed in overview [11] includes the descriptions of two kinds of FDS: parallel update systems and sequential update systems. Unfortunately, FDS has a set of disadvantages. The main disadvantage is impossibility to define "deadlock" situation in parallel processes and difficulty for theoretical evaluating of complexity of calculus that is fundamental aspect of time management in high load systems. The results [11] do not permit describing in framework such property of system elements as availability that is the major concern for cybersecurity of smart grid.

Inability to take into account the structures of the transmitted data is additional disadvantage of FDS for objectives of cybersecurity simulation.

The term "process algebra" was coined in 1982 by Jan Bergstra and Jan Willem Klop [12], originally in the sense of universal algebra, to refer to a structure satisfying a particular set of axioms [13]. Nowadays it is used in a more general sense for algebraic approaches to describe and study concurrent processes.

The system behavior generally consists of processes and data. Processes are the control mechanisms for the manipulation with data. While processes are dynamic and active, data is static and passive. The system behavior tends to be composed of several processes that are executed concurrently, where these processes exchange data in order to influence each other's behavior. Fundamental to process algebra is a parallel operator, to break down systems into their concurrent components. A set of equations is imposed to derive whether two terms are behaviorally equivalent. In this framework, non-trivial properties of systems can be established in a rigorous and elegant fashion. For example, it may be possible to equate an implementation of a system to the specification of its required input/output relation. A variety of automated tools have been developed to facilitate the derivation of such properties in a process algebraic framework. Abstract

data types offer a framework in which the data can be also specified by means of equations. μCRL [14] is a specification language, that combines process algebra with equational specification of data types. Applications of the process algebra exist in diverse fields such as safety-critical systems, network protocols, and biology.

μCRL allows investigating some problems of data fusion by the methods of Category theory [15], where data fusion [16] is a "multilevel, multifaceted process handling the automatic detection, association, correlation, estimation, and combination of data and information from several sources".

The process algebra in its different interpretations (Spy-calculus, π-calculus and others) shows more appreciate result in the field of modeling cybersecurity for distributed systems, but requires implementation of the different approaches for evaluating specific properties of smart grid. For example, for evaluating performance we should use the stochastic process algebra. The algebraic approach based on process algebra and theory of category shows very good results in formal analysis of security protocols for wireless sensor networks [18].

The correctness of different approaches usage for mathematical modeling. The first part of the author's research in the models of electronic digital signature functioning in smart grid was finished in 2014 [19]. The investigation of relevant mathematical paradigms was one of the major issues. The following known class of models was investigated and described: Protection systems that verify and supervise themselves; Kuramoto oscillators; Percolation theory (random fuse networks); evolutionary models; Markov processes; Neural networks.

The class of mathematical models of a non-stationary multidimensional random field in the process of evolution was introduced by authors [19] as a more relevant approach for evaluating the limit technical parameters during the modeling of smart grid. It requires more accuracy to solve the tasks of minimization of needs in labor and technical resources. But it may be seen as partial solution only. It was the first step of immersion into issues of cybersecurity in smart grid. The results obtained in the research allow us to see new horizons in the research and development of more universal approach which will be devoid of the previously mentioned disadvantages.

Conclusion. We have shown that the modeling problem of cybersecurity in the critical infrastructures is urgent. The algebraic approach may be a successful way for solving the problem and can help in the design of the mathematical framework of cyberspace modeling in critical infrastructures for safety evaluation and risk assessment.

Зроблено спробу систематизації сучасних підходів до математичного моделювання кібербезпеки критичних інфраструктур на підставі огляду відкритих публікацій, в яких аргументується, що сучасний стан математичного та комп'ютерного моделювання (симуляції), парадигми управління не дозволяють охопити всю складність та взаємопов'язаність таких критичних інфраструктур як, наприклад, інтелектуальні мережі в енергетиці (смарт-грід).

REFERENCES

1. National Institute of Standards and Technology (2015), "Framework for Improving Critical Infrastructure Cybersecurity", available at: http://www.nist.gov/cyberframework/upload/cybersecurityframework021214final.pdf. (accessed January 21, 2015).
2. Aloul, F.A. (2015), "Smart Grid Security: Threats, Vulnerabilities and Solutions", available at: http://www.aloul.net/Papers/faloul_ijsgce12.pdf.(accessed January 20, 2015).
3. Knapp, E.D. and Langill, J.T. (2013), Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems. Elsevier, Syngress: Amsterdam, Boston.
4. Knapp, E.D. and Samani, R. (2013), Applied Cyber Security and the Smart Grid: Implementing Security Controls into the Modern Power Infrastructure. Elsevier, Syngress: Amsterdam, Boston.
5. National Institute of Standards and Technology (2010), "Introduction to NISTIR 7628. Guidelines for Smart Grid Cyber Security. The Smart Grid Interoperability Panel, Cyber Security Working Group", available at: http://www.nist.gov/smartgrid/upload/ nistir7628_total.pdf. (accessed January 20, 2015).
6. Roberts, F. "Algorithmic Decision Theory and the Smart Grid», available at: http://dimacs.rutgers.edu/People/Staff/froberts/AlgoDecTheoryAndSmartGrid12012rev.pdf. (accessed February1, 2015).
7. Diesis, "Design of an Interoperable European federated Simulation network for critical InfraStructures, Fraunhofer IAIS", available at: http://www.iais.fraunhofer.de/ 4819. html?&L=1. (accessed February 1, 2015).
8. Massoud, A.S. (2011), "Smart Grid: Overview, Issues and Opportunities. Advances and Challenges in Sensing, Modeling, Simulation, Optimization and Control", *European Journal of Control*, no. 5-6, pp. 547-564.
9. Saad, W., Han, Z., Poor, H.V. and Basar, T. "Game Theoretic Methods for the Smart Grid", available at: http://arxiv.org/pdf/1202.0452.pdf. (accessed February 2, 2015).
10. Babic, J. "Agent-based Modeling of Electricity Markets in a Smart Grid Environment", available at: http://www.fer.unizg.hr/_download/repository/Jurica_Babic_Agentbased_Modeling_of_Electricity_Markets_in_a_Smart_Grid_Environment_%5BKDI %5D.pdf. (accessed February 2, 2015).
11. Laubenbacher, R., Jarrah, A.S., Mortveit, H.S. and Ravi, S.S. (2012), "A mathematical formalism for agent-based modeling", *Computational Complexity. Theory, Techniques, and Applications*. Springer, pp. 88-104.
12. Bergstra, J.A. and Klop, J.W. (2004), An introduction to Process Algebra. Applications of process algebra, Edited by Baeten, J.C.M., Cambridge University Press, Cambridge.
13. Fokkink, W. (2007), Introduction to Process Algebra, 2-nd edition. Springer-Verlag, Germany.
14. Fokkink, W. (2007), Modelling Distributed Systems, Springer, Germany.
15. MacLane, S. (1998), Categories for the Working Mathematician, Springer, Germany.
16. Khaleghi, B., Khamis, A. and Karray, F.O. (2015), "Multisensor data fusion: A review of the state-of-the-art", available at: http://www.alaakhamis.org/teaching/MCT200/reading/Information%20Fusion.pdf. (accessed January 20, 2015).

17. Clark, A., Gilmore, S., Hillston, J. and Tribastone, M. (2015), "Stochastic Process Algebras", available at: http://www.dcs.ed.ac.uk/pepa/stochasticprocessalgebras.pdf. (accessed January 20, 2015).
18. Novotny, M. (2010), "Formal analysis of security protocols for wireless sensor networks", *Tatra Mt. Math. Publ.*, Vol. 47, pp. 81-97.
19. Kravtsov, H. (2013), "Mathematical models of Smart Grid", *Elektronnoe modelirovanie*, Vol. 35, no. 5, pp. 27-41.

Поступила 02.06.15

КРАВЦОВ Григорий Алексеевич, канд. техн. наук, и.о. старшего науч. сотр. Ин-та проблем моделирования в энергетике им. Г.Е. Пухова НАН Украины. В 2000 г. окончил Севастопольский военно-морской институт им. П.С. Нахимова. Область научных исследований — кибербезопасность смарт-грид, криптография, разработка распределенных гетерогенных вычислительных систем.

КОЦЮБА Игорь Васильевич, аспирант Ин-та проблем моделирования в энергетике им. Г.Е. Пухова НАН Украины Директор ООО «Интегрейтед Солюшнз». В 2010 г. окончил Государственный университет информационно-комуникационных технологий. Область научных исследований — постериорные методы анализа угроз информационной безопасности.

ПРИТУЛЮК Ирина Афанасьевна, аспирант Ин-та проблем моделирования в энергетике им. Г.Е. Пухова НАН Украины. В 2011 г. окончила Открытый международный университет развития человека «Украина». Область научных исследований — моделирование финансовых систем, теория игр.