Synthesis of Controlled Parameters of Cyber-Physical-Social Systems for Monitoring of Security Incidents in Conditions of Uncertainty

Igor Kotenko 1,2 and Igor Parashchuk 2

1St.Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS), 39, 14 Liniya, St. Petersburg, Russia.
Email: {ivkote, parashchuk}@comsec.spb.ru
2Saint-Petersburg National Research University of Information Technologies (ITMO University), 49, Kronverksky Prospect, St. Petersburg, Russia.

Abstract. A methodological approaches aimed at obtaining the optimal set of controlled parameters of cyber-physical-social systems for monitoring of security events and incidents is suggested. Synthesis of the optimal parameters is carried out not only on the basis of known and approved methods of decomposition (structural, parametric and evolitional) and dynamic reduction, but also taking into account uncertainty, ambiguity and unreliability (inadequacy, incompleteness) of the initial information. The paper considers the mechanisms to formalize different stages of synthesizing a set of controlled parameters. The proposed set of controlled parameters claims to be optimal by the criteria of reliability (completeness, depth), informativeness (the value of the information) and operativeness of data collection and processing. The results of computational experiments on synthesizing the optimal set of controlled parameters based on fuzzy sets and neural networks are outlined.

1. Introduction
Modern Cyber-Physical-Social Systems (CPSSs)- cars, drones, factories, smart homes, etc. - are interconnected aggregates of various social and natural objects, artificial subsystems and controllers [1]. CPSSs are based on information processing, and a separate area of modern research is monitoring of security incidents in such systems [2, 3]. The task of synthesizing the elements of the optimal set of controlled parameters (SCP) for monitoring of security incidents in CPSSs is very important and hard to solve. For the systems of this class a set of traditional methodological and theoretical approaches exist. It is focused on the joint step-by-step decomposition procedure (structural, parametric and evolitional) and the dynamic reduction of the vectors of parameters [4]. They allow one to synthesize the elements of SCP for complex CPSSs. The relevance of this topic is determined by the fact that often the problem of synthesizing such elements has to be solved in conditions of various kinds of uncertainty. This significantly affects the reliability of decision-making.

The theoretical significance of the main idea of the paper is to consider a new methodological and mathematical approach aimed to synthesize the elements of the optimal SCP for CPSSs. This synthesis takes into account two key types of uncertainty: ambiguity (fuzziness) and unreliability (inadequacy, incompleteness) of the initial information. The paper is organized as follows. Second section analyzes the related works. Third section considers an approach for solving the SCP synthesis problem. It includes the formulation of the synthesis problem and outlines the stages of synthesizing the optimal set of controlled parameters in uncertainty conditions. Fourth section describes the experiments. Fifth
section is the discussion of the experimental results. Sixth section presents conclusion and directions of further work.

2. Related Work
The main decisions on optimizing the volume and nomenclature of the controlled and evaluated parameters of complex systems are considered in many works. But they, basically, are aimed at algorithms of decomposition, reduction and evolutionary optimization.

In [4] these approaches are classified according to the different levels and criteria of decomposition. Various simple heuristic algorithms based on combinatorial solutions are proposed for object recognition [5]. In [6], it is suggested to use the tensor approximation and the ranking of tensors, for example, in signal processing problems. However, tensor models in the application to problems of optimal sets synthesis do not guarantee the high accuracy of the solution. An approach, based on the reduction method, is proposed in [7]. However, such an approach requires to considerer the auxiliary parameters that characterize multidimensional sampling and the agreement of moments for approximation, which is not always possible. In [8] an approach to reduction based on a step-by-step scaling is outlined. But this method is applicable only to the standard symmetric model of systems, which narrows the field of application. The paper [9] is devoted to a method that allows one to reduce the set of controlled parameters using affine spaces. But this approach is complex for the mathematical description and laborious. The paper [10] outlines the modern mechanisms for managing the complex systems. It justifies the need to construct an optimal set of controlled parameters. At the same time, it is possible to synthesize the optimal global SCP (GSCP), as well as the local SCP (LSCP) to manage security incidents. This approach is suggested in this paper. It is the basis for formulation of the problem and is taken into account in determining the SCP composition. The admissibility of considering not absolute SCP values, but deviations of the parameters from the required values, was proved in [11]. The analysis of the relevant papers [4-11] shows that the direct application of the results obtained in these papers is impossible for the task of monitoring of security incidents in CPSSs. The reason is that the actual security monitoring proceeds in the conditions of uncertainty. This is due to a large number of different factors, including the impact of complex multi-step attacks of various categories of malefactors [12]. Thus, the unified approach proposed in the paper for synthesizing the optimal SCP under uncertainty is topical and important, and can be used for security information and event management systems of the next generation.

3. The Approach to Solve the SCP Synthesis Problem

3.1. The Problem Formulation
The global SCP of the IT-infrastructure of CPSS can contain the following parameters:

\[ \Delta \text{acc}_{\text{avg/thr}}(k) \] deviation of the average time of accessing to the protected information resource by the legal (authorized) users at the k-th step of CPSS functioning, characterizing such an integral (across the list of services and corresponding threats) property as accessibility;

\[ \Delta \text{con IPP}_{\text{avg/thr}}(k) \] deviation of the average time of continuous ( uninterrupted) realization of the information protection process (IPP), characterizing the property of protection continuity;

\[ \Delta K_{\text{inf loss}}(k) \] deviation of the information loss coefficient, and \[ \Delta K_{\text{dist}}(k) \] deviation of the distortion coefficient; both of these coefficients characterize the property of integrity, i.e. the ability to keep information in a reliable and undistorted form, despite the presence of threats and vulnerabilities;

\[ \Delta K_{\text{inf conf}}(k) \] deviation of the information confidentiality coefficient at the k-th step of the CPSS operation, characterizing the property to keep information in secret from entities that do not have authority to access it;

\[ \Delta \text{R}_{\text{cost}}(k) \] deviation of the resource cost vector on the construction of security monitoring subsystem.

Thus, the CPSS functioning at the k-th step is characterized by the following vector of global SCP:
\[ \Delta \bar{Y}_{\text{CPSS}}(k) = [\Delta \bar{Y}_{\text{acc/thr}}(k); \Delta \bar{Y}_{\text{infIP}}(k); \Delta \bar{Y}_{\text{infloss}}(k); \Delta \bar{Y}_{\text{dist}}(k); \Delta \bar{Y}_{\text{infcont}}(k); \Delta \bar{Y}_{\text{cont}}(k)]^\top. \]  

*The local SCP*, characterizing the quality of security incident monitoring, may include the following parameters: \( \Delta \bar{Y}_{\text{scp}}(k) \) – *deviation of the average recovery time* from the required values for normal operation of the control loop (CL) at the \( \xi^k \)-th exposures and at the \( k \)-th control stages of the \( k \)-th step of the CPSS operation; \( \Delta \bar{Y}_{\text{cc}}(k) \) – *deviation of the average time of continuous operation* of CL from the required values due to security incidents; \( \Delta \bar{Y}_{\text{cc}}(k) \) – *deviation of the control cycle (CC) time* from the required values due to security incidents; \( \Delta \bar{Y}_{\text{open}}(k) \) – *deviation of the average breaking (hacking) time* for incidents occurring in CL.

Thus, the CPSS functioning at the \( k \) step is characterized by the following vector of local SCP:

\[ \Delta \bar{Y}_{\text{man/acc}}(k) = [\Delta \bar{Y}_{\text{res/cont}}(k); \Delta \bar{Y}_{\text{cl}}(k); \Delta \bar{Y}_{\text{cc}}(k); \Delta \bar{Y}_{\text{open}}(k)]^\top. \]

Expressions (1) and (2) are the initial data in the problem formulation. On their basis, taking into account the volume and nomenclature of these vectors, further optimization can be carried out. As the synthesis result, the optimal space of controlled parameters should be formed in uncertainty conditions.

3.2. Stages of Synthesizing the Optimal Set of Controlled Parameters in Uncertainty Conditions

3.2.1. The approach based on fuzzy sets

It is known that monitoring of security incidents in complex systems is realized in conditions of uncertainty, including aspects of ambiguity (fuzziness) and insufficiency (incompleteness) of the initial information. The first stage of synthesis is oriented to the presence of uncertainty of the initial data, which has the character of ambiguity (fuzziness). Such problems are traditionally solved on the basis of fuzzy sets [13, 14]. The following steps are proposed for SCP synthesizing: (1) the formulation of the key elements of synthesis - the fuzzy membership functions, characterizing the preliminary, ambiguously (fuzzy) predetermined composition of the SCP; (2) the construction of matrices of the fuzzy membership functions; (3) formation of fuzzy intersection relation; (4) building a Boolean matrix for the ratio of fuzzy sets; (5) the definition of similarity classes - the number and composition of the SCP; (6) the definition of ordinal function of the ratio of fuzzy sets; (7) search for disjoint subsets of the local SCP and the formulation of the results of fuzzy synthesis, i.e. the similarity classes of SCP and the resulting system of disjoint subsets of controlled parameters. At the same time, it is proposed to use one of the simplest operations on fuzzy sets. The use of disjunctive summation is used for combining the opinions of experts on the volume and nomenclature of the SCP [13]. The application of union and intersection operations of two fuzzy sets will allow us to formulate a combined fuzzy metric. This metric characterizes the degree of confidence of experts in the correctness of the inclusion of deviations of a particular parameter \( \Delta x \) in the set of controlled CPSS security parameters.

3.2.2. The approach based on extrapolating neural networks

The second stage of the synthesis is realized, taking into account the uncertainty of the initial data, which has the character of insufficiency (incompleteness) of the initial information. It is suggested to solve this task on the basis of extrapolating neural networks (ENN) [15, 16].

The mathematical mechanism of transformations, the logic and physical meaning of functioning of single-layer neural networks with insufficient (incomplete) information are described in detail in [15].

The suggested synthesis technique, based on neural network methods, includes the following steps: (1) definition of data for the ENN and determination the values of the initial states (synaptic weights) of the ENN input layer; (2) activation of the ENN entrance layer and bringing the neurons of the input layer to initial states; (3) initialization of neurons of the ENN output layer; (4) bringing the neurons of the input layer to the state of the output layer neurons; (5) calculation of new states of the ENN output layer neurons; (6) development of the ENN to the stabilization state (the actual process of neural
computing); (7) analysis of the obtained states of the output layer neurons and inclusion of relevant parameters in the SCP in the interest of security monitoring.

4. Experiments

4.1. Synthesis of the Optimal Set of Controlled Parameters on the Basis of Fuzzy Sets

We performed computational experiments on the synthesis of the optimal SCP based on the fuzzy sets. Let us consider an example of using the technique for computing a disjunctive sum. As an example for a computational experiment, we define a fuzzy vector of deviations of security parameters that need to be monitored at the k-th step of the CPSS operation. It consists of ten parameters:

\[ \Delta Y_{p_{ai}}(k) = [\Delta \tilde{x}_{i}(k)| \mu(\Delta x_{i}); \Delta \tilde{x}_{2}(k)| \mu(\Delta x_{2}); \ldots; \Delta \tilde{x}_{9}(k)| \mu(\Delta x_{9}); \Delta \tilde{x}_{10}(k)| \mu(\Delta x_{10})]^T, \]

where \( \Delta \tilde{x}_{i}, \ i = 1\ldots10, \) is a fuzzy preference for including the deviation of i-th parameter into the SCP structure, and \( \mu(\Delta x_{i}), \ i = 1\ldots10, \) is a value of the membership function of the preference. Then the opinion of the first (A) of two (A and B) experts on including the deviation, for example, of the first parameter in the SCP structure, can be represented as a fuzzy set:

\[ \vec{\tilde{A}}_{A_{i1}} = \{p_0|0; \ p_1|0; \ p_2|0,3; \ p_3|0,9; \ldots; p_{10}|0\}; \]

As a result, the cumulative opinion of experts to include the first parameter (\( \Delta x_1 \)) in the SCP is finally determined by the disjunctive summation of fuzzy sets:

\[ \vec{\tilde{C}}_{i} = \vec{\tilde{A}}_{A_{i1}} \oplus \vec{\tilde{B}}_{A_{i1}} = \{p_0|0; \ p_1|0; \ p_2|0,4; \ p_3|0,2; \ p_4|0; \ldots; p_{10}|0\}. \]

Similarly, the fuzzy sets, specifying the need to include other parameters, for example, the second and third parameters (\( \Delta x_2 \) and \( \Delta x_3 \)), are defined in the same way. For the final selection of the \( \Delta x_i \) deviations of the security parameters, that are to be included in the SCP, the function \( \Delta x'_i = F((\Delta x_i | \max \mu(\Delta x_i))) \) is used.

4.2. Synthesis of the Optimal Set of Controlled Parameters Based on Extrapolating Neural Networks

Let us consider an experiment on using the neural network based technique of synthesis of the optimal SCP in conditions of insufficiency (incompleteness) of the initial information. Namely, we consider the operations of forming cognitive maps and obtaining a forecast. As an example for the computational experiment, a cognitive map is formed that characterizes the cause-effect relationships between some conditional security parameters. For example, the 1-st and 2-nd, i.e. \( \Delta x_1 \) and \( \Delta x_2 \). Dependencies are determined from the point of view of the consequences of an incomprehensible situation (0), inclusion (+1) or not inclusion (−1) of these parameters in the SCP composition. This cognitive map is completely defined by its matrix of links.

Within the framework of our experiment, the input vector of a neural network is \( \vec{U} = [0, 0, 1, 0, 0] \). In this case, the output vector \( \vec{B} = [b_1, \ b_2, \ldots, b_5] \) successively takes a number of state values. They are defined on the basis of the expression:

\[ b_i(k + 1) = f \left( \sum_{j=1}^{n} a_{i}(k) \ w_{ij} \right) = f \left( \sum_{j=1}^{n} b_{i}(k) \ w_{ij} \right), \]

The results of the experimental calculation show that the ENN, built in the interest of synthesizing the optimal set of controlled parameters, stabilized after the third clock. The network status can be interpreted as a forecast in case of guaranteed inclusion of the security parameter \( \Delta x_3 \) in the final SCP composition. This state is characterized by a decrease in the influence of the parameter \( \Delta x_2 \), the parameter \( \Delta x_3 \), and the increase in the weight of the parameter \( \Delta x_1 \). There was a tendency to reduce the dependence between the parameter \( \Delta x_3 \) and the parameter \( \Delta x_4 \). As a result of sequential realization of
the stages of SCP synthesis, taking into account the uncertainty, a number of security parameters can be obtained. The inclusion of these parameters in the SCP, according to the experts, is desirable. This will increase the objectivity (accuracy, in formativeness) for monitoring of security incidents.

5. Discussion
In experiments, as the result of the optimal SCP synthesis, taking into account the uncertainty, different variants of disjoint sets of controlled parameters were obtained. These parameters are considered as important for monitoring of security incidents.

Analysis of the results of fuzzy and neural network synthesis allows us to say that it is necessary to include in the final optimal global SCP a parameter of user service – the deviation of the number of services to prevent security threats ($\Delta N_{\text{ser}}^{\text{acc}}(k)$). In addition, the results of the experiments show that it is necessary to exclude from the final optimal local SCP a parameter $\Delta T_{\text{open CL}}(k)$, since this parameter is logically inseparable from (correlated to) the existing parameter of CPSS functioning – the deviation of the average time of continuous (uninterrupted) realization of the information protection process or inverse parameters - the deviation of the average time of break-in (hacking) the entire system.

Thus, the vector of the optimal global SCP can be represented as:

$$
\Delta \vec{Y}_{\text{CPSS}}(k) = [\Delta T_{\text{acc}}^{\text{thr}}(k); \Delta T_{\text{con BP}}^{\text{thr}}(k); \Delta K_{\text{inf loss}}(k); \Delta K_{\text{dist}}(k); \Delta K_{\text{inf cont}}(k); \Delta R_{\text{cont}}(k); \Delta N_{\text{ser}}^{\text{acc}}(k)]^T
$$

And the vector of optimal local SCP is as follows:

$$
\Delta \vec{Y}_{\text{loc inc}}^{\text{acc}}(k) = [\Delta T_{\text{res CL}}^{\text{CC}}(k); \Delta T_{\text{com CL}}^{\text{CC}}(k); \Delta T_{\text{CC}}^{\text{CC}}(k)]^T.
$$

The components of the global SCP for servicing CPSS users and the local SCP of incident monitoring are described in expressions (1) and (2) and supplemented with the results of synthesizing the security parameters in conditions of ambiguity (fuzzy) and insufficiency (incompleteness) of the initial information.

6. Conclusion
The paper proposed a comprehensive approach to the synthesis of SCP for security monitoring. It is based on both known methods of decomposition and reduction, and on methods (stages) of synthesis under conditions of uncertainty. This makes it possible to synthesize SCP, which is optimal according to the criteria of reliability (completeness, depth), in formativeness (the value of information), and the promptness of collecting and processing observation data. Computational experiments were performed to synthesize the optimal SCP based on fuzzy sets and neural networks. The results of the experimental calculation demonstrated that techniques for synthesizing SCP with fuzzy sets and ENN were stabilized already after the third clock cycle. It allows us to speak about high operational efficiency and small computational complexity of solving the synthesis problems by the suggested approach. The proposed methods and results of the experimental calculation can be widely used for security information and event management (SIEM) [17-18] and are used in the current SIEM implementations developed by the authors [2, 19]. Future research will be devoted to the further practical implementation of the suggested approach and comprehensive experiments.

7. Acknowledgments
This research was partially supported by grants of RFBR (projects No. 16-29-09482 and 18-07-01488), by the budget (project No. AAAA - A16-116033110102-5), and by Government of the Russian Federation, Grant 08-08.

8. References
[1] Xiong G, Zhu F, Liu X, Dong X, Wuling H, Songhang C and Kai Z 2015 Cyber-physical-social System in Intelligent Transportation IEEE/CAA Journal of Automatica Sinica 2 pp 67-69
[2] Kotenko I, Levshun D and Chechulin A 2016 Event correlation in the integrated cyber-physicalsecurity system Proceedings of the 2016 XIX IEEE International Conference on Computing and Measurements (SCM-2016) (St. Petersburg, Russia) pp 484 - 486

[3] Kotenko I, Chechulin A 2012 Common Framework for Attack Modeling and Security Evaluation in SIEM Systems Proceedings of the 2012 IEEE International Conference on Green Computing and Communications, Conference on Internet of Things, and Conference on Cyber, Physical and Social Computing (California: IEEE Computer Society) pp 94-101

[4] Lu Y, Gadh R and Tautges T 1998 Volume decomposition and feature recognition for hexahedral mesh generation I-CARVE Lab, University of Wisconsin-Madison (Madison Wisconsin, USA)

[5] Sakurai H and Dave P 1996 Volume Decomposition and Feature Recognition, Part II: Curved Objects Computer-Aided Design 28 (6/7) pp 519-537

[6] Sidiroopoulos N, Lathauwer L, Fu X, Huang K, Papalexakis E and Faloutsos C 2017 Tensor Decomposition for Signal Processing and Machine Learning IEEE Transactions on Signal Processing 65(13) pp 3551-3582

[7] Ciuprina G, Fernandez J, Ioan Z and Ilievski S 2015 Parameterized model order reduction CASA-Report. Eindhoven University of Technology (Netherlands)

[8] AbdusSalam S, Burgess C and Quevedo F 2015 MFV reductions of MSSM parameter space Journal of High Energy Physics (Cambridge University, Cambridge, UK)

[9] Hubert E and Labahn G 2010 Scaling Invariants and Symmetry Reduction of Dynamical Systems Cheriton School of Computer Science (University of Waterloo, Waterloo ON, Canada)

[10] Golnaraghi F and Kuo B 2017 Automatic Control Systems (London: Tenth Edition) p 1160

[11] Hemink G, Meijer B and Kerkhoff H 1990 Testability Analysis of Analog Systems IEEE Transactions on Computer-Aided Design 9(6) pp 573-583

[12] Kotenko I 2003 Active Vulnerability Assessment of Computer Networks by Simulation of Complex Remote Attacks Proceedings of the International Conference on Computer Networks and Mobile Computing. ICCNMC-03 (IEEE Computer Society) pp 40-47

[13] Zadeh L 1965 Fuzzy Sets Information and Control 8 pp 338-353

[14] Kotenko I, Saenko I, Ageev S and Kopchak Y 2015 Abnormal Traffic Detection in networks of the Internet of things based on fuzzy logical inference XVIII International Conference on Soft Computing and Measurements (SCM'2015) IEEE Xplore pp 5-8

[15] Rojas R 1996 Neural Networks (Berlin: Springer-Verlag) p 453

[16] Parashchuk I 2002 System Formation Algorithm of Communication Network Quality Factors using Artificial Neural Networks 1st IEEE International Conference on Circuits and System for Communications (ICCSC’02). Proceedings. (St. Petersburg: SPbGTU) pp 263-266

[17] Kotenko I, Chechulin A and Novikova E 2012 Attack Modelling and Security Evaluation for Security Information and Event Management Proceedings of the International Conference on Security and Cryptography (SECRIPT 2012) pp 391-394

[18] Kotenko I 2005 Agent-Based Modeling and Simulation of Cyber-Warfare between Malefactors and Security Agents in Internet Proceedings of the 19th European Simulation Multiconference “Simulation in wider Europe” (ESM’05) pp 533-543

[19] Fedorchenko A, Kotenko I, Chechulin A 2015 Integrated repository of security information for network security evaluation Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications 6(2) pp 41-57