ATLANTIS PRESS

Advances in Intelligent Systems Research, volume 166

7th Scientific Conference on Information Technologies for Intelligent Decision Making Support (ITIDS 2019)

Semantic modeling of cyber threats in the energy sector using Dynamic Cognitive Maps and Bayesian Belief Network

Daria A. Gaskova
Melentiev Energy Systems Institute of Siberian Branch of the Russian Academy of Sciences
Irkutsk, Russia
gaskovada@gmail.com

Aleksei G. Massel
Melentiev Energy Systems Institute of Siberian Branch of the Russian Academy of Sciences
Irkutsk, Russia
amassel@gmail.com

***Abstract*— The article discusses the use of semantic modeling in the analysis of threats to energy security (ES). Semantic modeling is proposed to be applied at a qualitative level, followed by quantitative assessment of the ES level in studies of energy security. Exercise of traditional software systems provides a quantitative assessment, which is characterized by the duration of information preparation, and the formation and adjustment of large enough models for computational experiments. At the first level, a decision maker selects options for which a detailed rationale is required based on the results of semantic modeling. These options are calculated at the second level. The article presents basic notions of Dynamic Cognitive Maps (DCM) and Bayesian Belief Network (BBN). The paper presents the information model that is suggested to use in analyzing cyber threats in the energy sector. Exemplification of the impact of cyber threats on an energy facility carried out under Dynamic Cognitive Maps and Bayesian Belief Network is given in this article. The advantages of each tool and their role in analyzing cyber threats in the energy sector are presented.**

Keywords*— *semantic modeling methods, cyber security, energy security, extreme situations in the energy sector, energy sector, cyber threat analysis

I. INTRODUCTION

The energy sector is one of the main critical infrastructures, in which more and more system-level breakdowns are observed, which emerge from small perturbations that cascade to large-scale consequences. Analysis of recent incidents have shown that information technology systems can be vulnerable to cyber-attacks and that such attacks can lead to disruption of physical systems and networks [1]. The issue of the using advanced information and communication technologies in the Smart Grid was considered in [2]. This will have potential devastating effects since the growing scale and complexity of Smart Grid also increase the threat of cyber-attacks due to unforeseen loopholes and unexpected weaknesses in the system.

Abnormal situations such as critical or emergency situations in the energy sector are the subject of energy security studies [3]. Semantic Modeling [4], which involve Cognitive Maps, Bayesian networks, Markov processes, Petri Nets and Ontology-based Modeling [5], is applied in research of energy security.

The possibility of applying Fuzzy Cognitive Maps in Decision Making Support System was considered, for example, in [6]. Bayesian Belief Networks (BBN) were previously used to model the risks of critical situations in the energy sector when implementing strategic threats to the energy security (ES) [7]. The study like [8] proposes to use this tool to compute the probability of the compromise of cyber components of the Smart Grid system. Bayesian Networks are also used in information security risk management. For instance, the article [9] explains using this tool to establish the relationship between the attributes (such as skills, time, and attitude) for attacker profiles (such as hackers, opportunists, and explorer behavior) and risks to analyse network penetration.

II. MODELING CYBER THREATS IN THE ENERGY SECTOR

Energy security studies address the impact of energy security threats on the state of energy systems. With regard to energy security, threats to the energy facility are the shortage of resource needs of acceptable quality under normal conditions and in extreme situations, the violation of stability and continuity of energy supply [3].

The ES threats list was supplemented with the cybersecurity threats [10], whose implementation could provoke serious emergency situations in the energy sector fraught with a drastic reduction of energy resources to be provided to consumers [11].

In the present work, the modeling of extreme situations (ExS) caused by the implementation of cyber threats in the energy sector is performed by building scenarios. As part of the research, the authors identified 4 main groups of concepts:

- ***factors (F)*** affecting the occurrence of an extreme situation;
- ***vulnerability (V)*** of the assets of the information and communication system of an energy facility (EF);
- ***threats (T)***;
- ***consequences (C)***.

The factors could be the following: lack of reserve capacity; natural conditions; untimely measures to eliminate threats; and other negative or positive processes.

Threats (T) are divided conditionally into 1) classical threats to energy security (T^E) and 2) cyber threats (T^C), which initiate events for threats of the first group.

Consequences from the realization of threats are considered as the probability of power loss and forced load shedding. Any extreme situation is estimated through the probability of consequence concept on the scale "norm" (normal functioning), "pre-crisis" (critical situation), "crisis" (emergency situation) [12].

The interrelation between these concepts can be described by Semantic Methods as a probabilistic dependence (Bayesian Networks), and functional dependence (Dynamic Cognitive Maps (DCM)).

Let's consider a generic example. Let's assume that a vulnerability "Remote Code Execution" with a high degree of criticality was found on the server (asset) at the level of the operator (dispatching) control of some subsystem of the Automated Control System (ACS) at an energy facility. Such vulnerabilities can be caused by the lack of timely updating, ports unpatching and / or insufficient protection. Using this vulnerability can lead to cyber threats such as DoS attacks, which are exacerbated by a delay or communication failure on the server. This in turn can cause such threats to the ES as loss of power and eventually disconnection of consumers (loss of load). Threat states can vary depending on the duration and target attack asset. The occurrence of an extreme situation in the example is estimated by the indicator "Loss of load" on the scale "norm" (normal functioning), "pre-crisis" (critical situation), "crisis" (emergency situation). Figure 1 shows the relationship of vulnerability, cyber threats, and energy security threats.

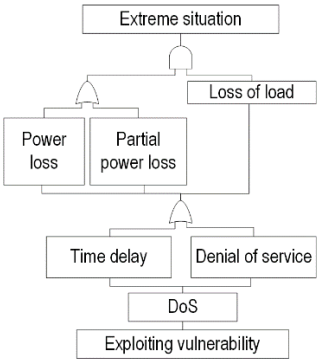

Fig. 1. The fault tree illustrating DoS cyber threat in energy facility

Further implementation of this example will be shown using Dynamic Cognitive Maps and Bayesian Network.

III. Dynamic Cognitive Maps

Cognitive maps are oriented graphs in which vertices correspond to factors (concepts), and arcs describe the relationships between factors. Relationships can be positive or negative, depending on the nature of the cause-effect relationship.

$$D_{t_i} = \{P, R\}, \quad (1)$$

where P are concepts; R are relationships.

The Dynamic Cognitive Map differs from the conventional cognitive map in that it is a set of cognitive maps presented at different point of time, that is [13]:

$$\{D\} = \{D_{t_0}, D_{t_1} \dots D_{t_n}\}, \quad (2)$$

where {D} is a set of dynamic cognitive maps; $\{D_{t_0}, D_{t_1} \dots D_{t_n}\}$ are sets of cognitive maps at time instants t_0, t_1, and t_n.

As a result, it becomes necessary to include in the DCM the weights of the relationships that would reflect the influence of factors (and / or objects) on each other as a function of time. It can be represented by the relationship weight as some function W(t). In most cases, the relationship weights in DCM can be represented by simple functions. [14].

Dynamic Cognitive Maps are offered as a tool for analyzing threats to ES. They maintain the possibility to identify causal relationships of concepts, implemented in ordinary cognitive maps (CM). The difference from Fuzzy Cognitive Maps, which were used in ES research earlier, is that an expert can see and evaluate the effect of relationships with respect to the time scale. Furthermore, expert can consider individual factors in the simulation.

Three types of concepts are considered in the model depending on the established relationships:

- ***independent concepts (N)*** can have outgoing arcs, but do not have incoming arcs;
- ***intermediate concepts (M)*** have both incoming and outgoing arcs;
- ***dependent concepts (R)*** have only incoming arcs.

Set of concepts types is represented as:

$$P \in \{P_N, P_M, P_R\}, \quad (3)$$

Factors (concepts) change over time. This internal change is described by the function F(t). The change in the concepts is fixed by the boundary values on a scale: "norm", "pre-crisis", or "crisis". Figure 2 presents an example of the use of Dynamic Cognitive Maps in simulating cyber threats in the energy sector, discussed in the previous section. Table 1 presents concepts descriptions of a DCM.

TABLE I. DESCRIPTION OF THE CONCEPTS OF DCM

№	Concept	F(t) type	Boundary values			P type
			Norm	*Pre-crisis*	*Crisis*	
P_1	Remote code execution on the server	Boolean function	F1(t) = 0	-	F1(t) = 1 V - vulnerability	P_N
P_2	DoS	Boolean function	F2(t) = 0	-	F2(t) = 1 T_1^c – cyber threat	P_M
P_3	Server operation, rps	Interval function	F3(t)={A-A1} rps	F3(t)={A1-A2} rps T_2^c – cyber threat	F3(t) > A2 rps	P_N
P_4	Power, kWh	Interval function	F4(t)={B1-B2} kWh	F4(t) ={B2-B3} kWh T_1^E - ES threat	F4(t) < B3 kWh	P_N
P_5	Loss of load, kWh	Interval function	F5(t)={C1-C2} kWh	F5(t)={C2-C3} kWh T_2^E – ES threat	F5(t) > C3 kWh	P_R

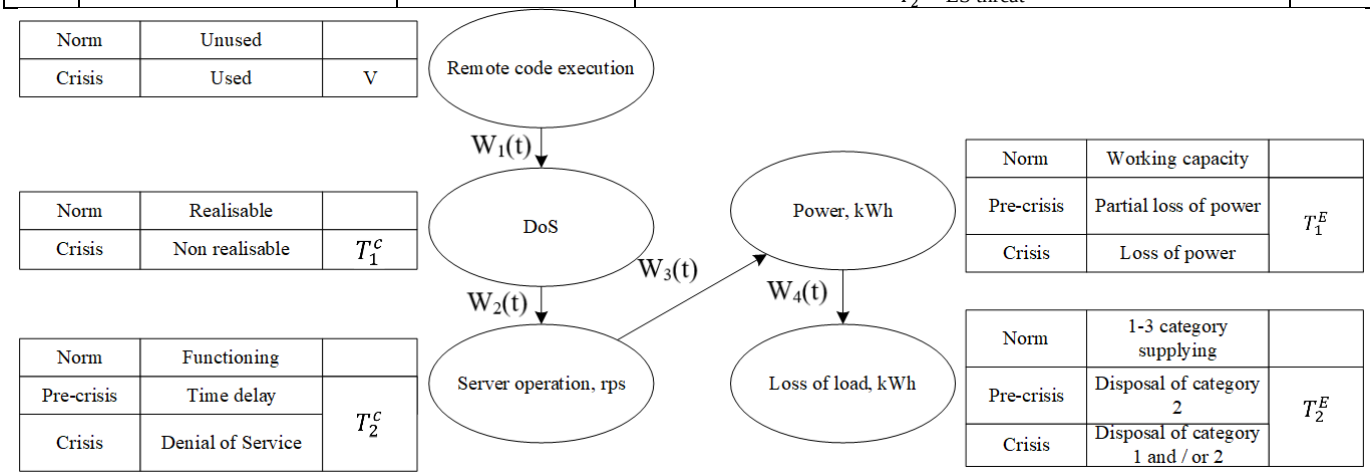

Fig. 2. Fragment of a DCM describing Dos attack in energy sector

In the example above, the weight of the relationships weight W(t) is given conditionally in the form of a Boolean function (T-true, F-false), which reflects the influence of the concepts on each other when reaching boundary values in time t_i. Table 2 describes the relationships of concepts and their states with regard to the boundary values.

TABLE II. DESCRIPTION OF THE RELATIONSHIPS OF THE CONCEPTS OF DCM

t	*P1*	*P2*	*P3*	*P4*	*P5*
t_1		$W_1(t)$=T	$W_2(t)$=F	$W_3(t)$=F	$W_4(t)$=F
t_2		$W_1(t)$=T	$W_2(t)$=T	$W_3(t)$=F	$W_4(t)$=F
t_3		$W_1(t)$=T	$W_2(t)$=T	$W_3(t)$=T	$W_4(t)$=F
t_4		$W_1(t)$=T	$W_2(t)$=T	$W_3(t)$=T	$W_4(t)$=T

Exemplification of the DCM represents step by step the impact of cyber threat “Dos attack” on the ES threat “Loss of load” while points of time t_i correspond to the transition of concept states from “norm” to “crisis”.

Points of time t_1 and t_2 correspond to the state “norm” of the concept “Loss of load” that is normal functioning of the energy facility and the absence of an extreme situation. At point of time t_3, a “pre-crisis” is observed that means critical situation at the energy facility, requiring urgent measures. There is a “crisis” at point of time t_4 at which point that is emergency situation requiring liquidation measures.

Cognitive maps allow ones to trace the causal relationships of concepts depending on time and their influence on each other. DCM permit to visually analyse threats. In the course of such an analysis, the main concepts for probabilistic modeling of cyber threats in the energy sector were highlighted: vulnerability (V), cyber threats (T^C), and other threats to ES (T^E).

IV. BAYESIAN BELIEF NETWORK

The Bayesian network is a graphical model of probabilistic and cause-effect relations between sets of variables, which is a directed acyclic graph whose vertices represent variables, and the edges show conditional dependencies between variables [12].

The following definition of BBN is given in [12]. The Bayesian network for the variable set consists of:

- network structure *S*, which reflects the set of assumptions about the conditional independence of the set of variables X;
- The *P* probability distribution sets for each variable in *X*.

Extreme situation in the energy sector caused by cyber threats implementation is defined by probability in the course of reasoning on the network constructed in accordance with the types of concepts described in the second section. In this case, the state of concepts is estimated by Bayesian probabilities based on the knowledge and experience of an expert.

Figure 3 represents the same example using the BBN tool, which was considered earlier.

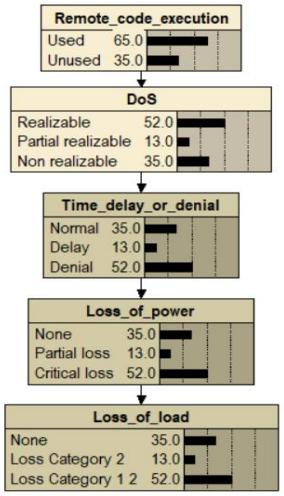

Fig. 3. Fragment of a BBN describing Dos attack in energy sector

In the example in Figure 3, in accordance with Table 2, conditional probabilities for each state in a network node are determined.

This exemplification illustrates that a preliminary analysis using the DCM allows ones to identify the main states of network variables and their relationships. In future, the authors propose to introduce conditional probabilities based on the relationship weights W(t) constraints, given by a mathematical function.

The determination of the ExS probability is based on the posteriori probability of the nodes. In this example, there are concepts of the loss of power and the disconnection of consumers (by categories).

The risk of ExS from the point of view of ES includes the probability of the occurrence of a negative event with consequences for the consumer. The risk of ExS is determined based on the posteriori probability obtained when modeling the "Loss of load" node, taking into account the probabilities of exploiting vulnerability, the threat and the consequences. Risk is determined as:

$$R = \{V, T, C\}, \quad (4)$$

where R are risks; V are vulnerabilities; C means consequences.

Threats determine the probability of event occurrence in extreme situations. Cyber threats could cause subsequent implementation of the other ES threats. Cyber threats might initiate scenario events; and final events are responsible for the consequences and determine the damage.

V. Conclusion

The study of strategic threats to ES is characterized by the diversity of the considered states of energy facility systems and disturbance scenarios, and also the criticality of the consequences. The joint use of DCM and BBN in modeling cyber threats in the energy sector contributes to the visual presentation of the concepts changes and their influence on each other, highlighting the threats of ES, including cyber threats, as well as calculating the probability of an ExS occurring during the implementation of cyber threats. The use of semantic modeling in energy security studies is considered to be a preliminary stage of qualitative expert analysis before choosing a calculation option in a complex computational experiment conducted on the different level of detail, using the mathematical model of the energy sector as a whole, energy systems or a set of energy facilities.

Acknowledgment

This work was performed within the framework of project according to state assignment MESI SB RAS №AAAA-A17-117030310444-2. The studying of separated aspects was supported by RFBR grants № 19-07-00351, № 19-57-04003, № 18-07-00714, № 18-37-00271, № 18-57-81001, № 17-07-01341.

References

[1] Z. Enrico, "Challenges in the vulnerability and risk analysis of critical infrastructures", Reliability Engineering and System Safety. Vol. 152, pp. 137–150, 2016.

[2] C.C. Fung, A.R. Mehrnaz, K.P. Wong, "A proposed study on economic impacts due to cyber attacks in Smart Grid: A risk based assessment", IEEE Power & Energy Society General Meeting. 2013. doi:10.1109/pesmg.2013.6672302

[3] N.I. Pyatkova, V.I. Rabchuk, S.M. Senderov, M.B. Cheltsov, "Energy Security in Russia: Problems and Solutions", Novosibirsk: SB RAS, 2011, p. 211 (in Russian).

[4] L.V. Massel, A.G. Massel, "Semantic technologies based on the integration of Ontological, Cognitive and Event modeling", III International Science and Technology Conference "OSTIS-2013" Minsk, pp. 247-250, 2013, (in Russian).

[5] M. Rybnicek, R. Poisel, M. Ruzicka and S. Tjoa, "A Generic Approach to Critical Infrastructure Modeling and Simulation", International Conference on Cyber Security "CyberSecurity" Alexandria, VA, USA, 2012, pp. 144-151.

[6] P.P. Groumpos, I.E. Karagiannis, "Mathematical Modelling of Decision Making Support Systems Using Fuzzy Cognitive Maps", Business Process Management. 2013, pp. 299–337. doi:10.1007/978-3-642-28409-0_12.

[7] L.V. Massel, E.V. Pyatkova, "Application of Bayesian Networks for the intelligent support of Energy Security problem researches", Proceedings of Irkutsk State Technical University. No. 2, pp.8-13, 2012, (in Russian).

[8] Y. Wadhawan, A. AlMajali, C.A. Neuman, "Comprehensive Analysis of Smart Grid Systems against Cyber-Physical Attacks", Electronics. 2018, 7 (10). doi:10.3390/electronics7100249.

[9] R. Dantu, P. Kolan, "Risk management using behavior based Bayesian networks", Intelligence and Security Informatics, pp. 165-184, 2005.

[10] L.V. Massel, N.I. Voropai, S.M. Senderov, A.G. Massel, "Cyber Danger as one of the strategic threats to energy security", Cybersecurity issues, No. 4 (17), 2016, pp. 2-10 (in Russian).

[11] S. Nazir, S. Patel, D. Patel ,"Assessing and augmenting SCADA cyber security: A survey of techniques", Comput. Secur. Vol. 70, 2017, pp. 436–454.

[12] L.V. Massel, A.G. Massel, "Technologies and tools for intelligent decision-making support in extreme situations in the energy sector", Computational Technologies, Vol. 18, № S1, 2013, pp. 37-44 (in Russian).

[13] A.G. Massel, "Dynamic Cognitive Maps for decision making on strategic management of energy sector development", Proceedings of the XIX International Conference "Complex Systems: Control and Modeling Problems". Samara: Ofort. 2016, pp. 253-257 (in Russian).

[14] A.G. Massel, "Dynamic cognitive maps for the substantiation of strategic decisions on management of energy sector development", Industry 4.0. Publisher: Scientific Technical Union of Mechanical Engineering "Industry 4.0", Issue 4, 2018, pp. 190-193.

[15] D. Heckerman, "A Tutorial on Learning with Bayesian Networks", Technical Report MSR-TR-95-06, Microsoft Research. 1995. 57 p.