Big Data Analysis-based Security Situational Awareness for Smart Grid

Big Data Analysis-based Security Situational Awareness for Smart Grid

Jun Wu, Kaoru Ota, Mianxiong Dong, Jianhua Li, *Member, IEEE*, and Hongkai Wang

Abstract— Advanced communications and data processing technologies bring great benefits to the smart grid. However, cyber-security threats also extend from the information system to the smart grid. The existing security works for smart grid focus on traditional protection and detection methods. However, a lot of threats occur in a very short time and overlooked by exiting security components. These threats usually have huge impacts on smart gird and disturb its normal operation. Moreover, it is too late to take action to defend against the threats once they are detected, and damages could be difficult to repair. To address this issue, this paper proposes a security situational awareness mechanism based on the analysis of big data in the smart grid. Fuzzy cluster based analytical method, game theory and reinforcement learning are integrated seamlessly to perform the security situational analysis for the smart grid. The simulation and experimental results show the advantages of our scheme in terms of high efficiency and low error rate for security situational awareness.

Index Terms—Smart grid, security situation assessment, big data, game theory, association analysis

1 Introduction

As the next generation power supply system, the smart grid can achieve the reliable and effective transmission of electricity from power generators to factories or household electrical appliances with the support of recent advances in communication and information technology [1], [2]. The smart grid is constructed based on integrated, high-speed and bidirectional communication networks. By using advanced sensing, control and decision technologies, the smart grid can improve the reliability, safety, and efficiency of the power grid.

Advanced information and communication technologies bring great benefits to the smart grid. However, cyber security threats also extend from the information system to the smart grid. Various attacks can disturb the normal operation of the power system, and thus have serious impacts on the normal productivities and lives of human being. Recently, the information and communication infrastructures of the smart grid have been attacked frequently. Advanced Persistent Threats (APT), such as Stuxnet, have broken the power system and caused large losses. In fact, there are still many security flaws in the smart grid. Currently, the security of smart grid has attracted a lot of attentions. X. Wang et. al. [3] studied the security framework of wireless communications in the smart grid. In this work, the potential security attacks and possible counter-attack measures are analyzed and studied. K. C. Sou et. al. [4] focused on a smart grid cyber-security problem, which analyzes the vulnerabilities of electric power networks defending against false data attacks. To enhance the security level of the smart grid, Y. Ye et. al. [5] proposed a security protocol for advanced metering infrastructure. Different kinds of security vulnerabilities were considered for deploying advanced metering infrastructure (AMI). Also, security factors are considered which are related to confidentiality of user privacy and behavior as well as message authentication for sensing and control. To realize the refurbishment of a SCADA/EMS system, G. N. Ericsson [6] studied cyber security issues in the smart grid, especially the access points in a substation, by using information-security domain modeling. Most of the exisiting security schemes for smart grids focused on the security protection and detection. Security situational awareness is still an unresolved problem in smart grid.

In fact, many threats occur in a very short time and steer by exiting protection and detection components. These threats usually have huge impacts on power system and disturb the normal activities of cities. It is too late to take action to defend against the attacks once they are detected, and the damage may be difficult to repair. Hence, the current security schemes cannot provide sufficient protection for the smart grid, which poses a number of security challenges in smart grid. Therefore, it is very important to practice the security situation awareness which can predict the attacks on the smart grid before they can cause harm. In addition, network components (e. g. switches, routers) and security components (e. g. IDS, access control systems) of wide-area power systems in the smart grid can generate security-related big data. In fact, big data are very useful for realizing security situational awareness. Big data are generated in the processes of the security issues and in the operations of generation, transmission, transformation, distribution, consumption and dispatching of the smart grid. These big data are very

- *Jun Wu and Jianhua Li are with the School of Eletronic Information and Eletrical Engineering, Shanghai Jiao Tong University, Shanghai 200240, China. E-mail: junwuhn@sjtu.edu.cn, lijh888@sjtu.edu.cn .*
- *Mianxiong Dong and Kaoru Ota are with the Department of Physics, Department of Information and Electric Engineering, Muroran Institute of Technology, Muroran 050-8585, Japan. E-mail: {mx.dong, ota}@csse.muroran-it.ac.jp.*
- *Hongkai Wang is with the Information and Telecommunication Branch of Zhejiang Electric Power Corporation, State Grid Corporation of China, Hangzhou 310007, China. E-mail: wang_hongkai@zj.sgcc.com.cn.*

valuable resources for security situational awareness. Based on the long-term monitoring of the smart grid, security-related big data can be formed. Then security situational awareness can be realized based on the analysis of the big data.

To address the challenges described above, this paper proposes a security situational awareness mechanism for smart grid based on big data analysis. The arechitecture of the proposed mechanism is shown in Fig. 1. The security facts from e.g., the primary electrical devices, substation buses, network devices, station controllers, control centers, and engineering stations, in smart grid can be collected and reported to the security situational awareness center. Then, the data collected over the long term can be stored and analyzed. To get high accuracy for the big data analysis, fuzzy cluster based association method is used to realize the preliminary analysis, and game theory as well as reinforcement learning are introduced for security situational awareness.

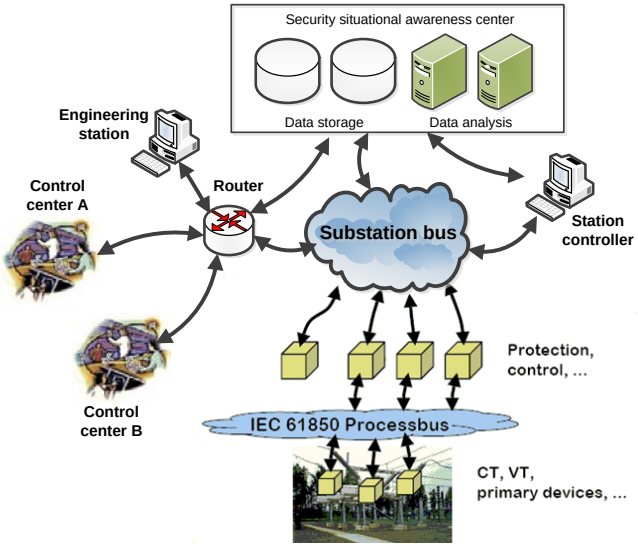


Fig. 1. Security situational awareness architecture for smart grid.

The rest of the paper is organized as follows. In Sect. 2, background and analysis about related technologies are illustrated. The preliminaries on association analysis, game theory and reinforcement learning are described in Sect. 3. Sect. 4 presents the details of the proposed security situational awareness mechanism. The evaluations of the proposed mechanism are illustrated in Sect. 5. Sect. 6 concludes this paper.

2 Background And Related Works

Situation Awareness (SA), which was clearly proposed by Endsley [7], means that the environmental factors in a certain time and space are cognized and understood, and that future development trends are predicted. The conceptual model of this definition is shown in Fig. 2. However, traditional concept of SA was not originally introduced into the field of network security in the beginning. It was only applied to considering factors in aerospace field. Next, T. Bass et. al. [8] indicated that the next generation networks' Intrusion Detection System (IDS) should fuse massive data collected by heterogeneous distributed network sensors so as to realize the cyberspace situational awareness, and they proposed the function model of network situational awareness based on multi-sensor and data fusion.

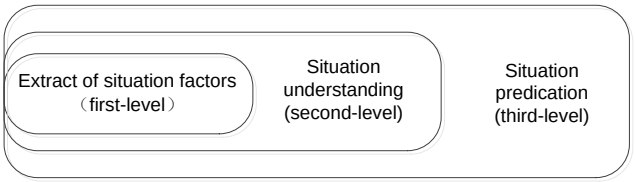


Fig. 2. The concept model of situation awareness.

The network situation can be divided into the security situation, topology situation and transmitting situation, etc. according to application areas. Currently, most existing research works focus on network security situation. M. R. Endsley [7] and T. Bass [8] gave the foundations for network security situation awareness .Based on the concept model and the function model proposed by M. R. Endsley and T. Bass respectively, other researchers also proposed a lot of models for network security situational awareness. As a matter of fact, although various network security situational awareness models have different forms, the functions of these models are similar. Existing works for network situational awareness can be divided into three types: 1) extraction of network security situation factors; 2) network situational assessment; 3) network situational predication. Most existing works generally evaluate network security situation by extracting situational factors in a certain way. S. Jajodia et. al. [9] evaluated network vulnerability situation by collecting network vulnerability information. R. Xi et. al. [10] proposed a network situational awareness tool called CNSSA (Comprehensive Network Security Situation Awareness), which can perceive network security situations comprehensively. In this work, the network security situation scheme makes a quantitative assessment on the situations of network security based on the fusion of network information. D. Kolev et. al. [11] proposed a collaborative security situation management scheme for air navigation. In this scheme, the threat prediction capability was formulated as a situational management problem mapping the concepts of situation awareness and information fusion. F. Chen et. al. [12] used the echo state networks (ESNs) with small-world property to propose a novel network security prediction method. The network security situation can be predicted after training and testing the acquired historical attack records. In addition, P. Harmer et. al. [13] proposed a situational awareness scheme for wireless security using a new set of metrics. These metrics are provided to assist administrators for identifying possible attacks as well as their impact. Moreover, J. Kim et. al. [14] presented SEAS-MR scheme which is a Security Event Aggregation System over MapReduce. This work facilitates scalable security event aggregation for comprehensive situation analysis.

Currently, there are still some open issues in the secu-

rity situation awareness. Most existing schemes do not consider the relevancy of various factors in an index architecture, thus making it difficult to fuse all information. Moreover, most of the network attacks are generated using the distributed method, which course difficulties for monitoring and controlling the whole network security situation using a simple data-fusion mechanism. In addition, in complex network enviornments, security situational awareness is a complex nonlinear process because of the randomness and uncertainty. The prediction method based on simple statistical data cannot address the above challenges. However, most existing works on security situational awareness focus on the traditional networks. The securety situational awareness of smart remains an unresolved problem. The existing security situation awareness works cannot be used in smart grid directly for the following reasons. First, the smart grid includes wide-area heterogeneous networks which based on various special standards, such as IEC 61850, ISO/IEC/IEEE 21451, WirelessHART, ISA100.11a, etc [15], [16], [17]. Second, unlike in normal communication networks, the information modelling and communications of smart grids are combined closely with the complex behaviors and smart decisions of the power system. Finally, the smart grid currently involves more new network models, such as V2G, which enhance the complexity of the smart grid and enlarge the attack surfaces of the smart grid. Although some schemes have been proposed for the situational awareness for smart grid, these works cannot address above challenges. For example, the work in [18] presented a comprehensive security monitoring and warning system implemented on the North China Grid. Although the scheme has significantly enhanced the operator's situational awareness for operating a very large power grid, it was proposed specifically for the power grid control center, and cannot cover highaly complex and smart behaviors of the entire grid. Based on above analysis, it is very important to propose a network security situational awareness scheme for smart grid.

3 PRELIMINARIES

3.1 Association Analysis

Association analysis is a very important issue for obtaining valuable underlying results from a data set [19]. According to different attributes of the data set, association rule mining can be classified as Boolean, classification and quantitative association rules. In the past, rule mining of Boolean associations has attracted a lot of attentions. However, quantitative attributes, such as integer, category and data attributions, are still the most significant association type in applications. For quantitative attribute association, existing mining algorithms of Boolean association rules cannot be applied. Therefore, there are two methods to realize the rule mining of the quantitative association: 1) transforming the quantitative attributes into Boolean attributes; and 2) proposing new association algorithms.

The attribute domain can be divided into several intervals after discretization. Then each interval is mapped as a Boolean attribute. Thus the mining algorithm of quantitative-attribute association is converted to the reasonable division problem of the quantitative attribute domain.

3.2 Game Theory

In the human society, conflict of interest is an eternal problem. When there is a conflict of interest among people, the behavior choices of the parties can be viewed as the "game". Game theory is the mathematical model that is used to study the game behavior.

There are four basic elements in a game: game players, game rules, game results and game effectiveness. A game player is a subject whose selection process can include the component's behaviors. In game theory, there are at least two game players. The game rule defines how the game runs, which is the core component of the game model. The game results can be obtained when all the allowed behaviors are finished and depend on the behaviors of all the game players. The game effectiveness is the impact on every player of the given game result. The game player usually performs the selection behaviors based on the game effectiveness. In game theory, if the players make decision at the same time, the game is called a static game. On the contrary, if the players make decisions at different times, the game is called a dynamic game.

The evolution process in biology provides a new roadmap for game theory. Evolutionary game theory was proposed by Maynard Smith, et. al., who introduced the idea of evolution into game theory. They used the game theory in economics to analyze the dependence and fight rules of biolog.

There are two basic methods for evolutionary game theory: evolutionarily stable strategy and replicator dynamics. Evolutionarily stable strategy provides the conditions under which the system is still stable when the given strategies are impacted by the variational strategies. In constrast, replicator dynamics describes the dynamic tracking of balance in evolution strategy.

When a group game uses a given strategy, the strategy can be considered an evolutionarily stable strategy, if the strategy resists the intrusion of tiny variations and allows the group game to still obtain maximum benefits.

3.3 Learning Algorithms for Game

Currently, there are two types of learning methods for game theory. The first learning model was proposed to resolve the problem of long-term convergence, which discusses how the learning model converges to Nash equilibrium. The second kind of learning model was proposed to describe the objective of players' behaviors in the repeated games, and such models can be classified as either the model based on belief or model using reinforcement learning. Here the learning model indicates the learning rules used by the individual players in the game, which can be used to check the interaction among the players. For example, a risk-dominant equilibrium will appear in some games if the long-term randomness of the learning process is considered. Some existing works have already focused on using learning technologies in game

theory [20], [21], [22], [23]. The games include Prisoner's Dilemma, Chicken Game, Game of Battle of Sex, etc. Some learning algorithms have been studied that can be used in the games, such as, Virtual action, reinforcement learning, Experience-Weighted Attraction (EWA) learning, etc. However, there are large errors between the predictions and the real practical observation results for the existing learning algorithms for game theory.

4 The Proposed Security Situational Awareness Mechanism

4.1 Basic Idea

The proposed network security situational awareness mechanism can be divided into three parts: 1) the extraction of network security situation factors; 2) network situational assessment; and 3) network situational prediction. The basica design principle is shown in Fig. 3.

Network security situation factors include static configuration information, dynamic operating information and flow information in networks, etc. Static configuration information contains the basic environmental configuration information which includes information on the network topology information, vulnerability information, and state information. Dynamic operating information consists of the basic operating information including the threat information obtained from the collection log and the analysis techniques of various protection measures. The extraction of the proposed network security situation factors has these three advantages: 1) The proposed mechanism can obtain knowledge of all collected information from multi-perspectives; 2) The proposed mechanism considers the relevancy of various factors in an index architecture reducing the difficulties in fusing all information. 3) the proposed mechanism performs effective verification of the index architecture, so we are able to verify the integrated index architecture.

Understanding the network security situation means fusing mass network security data information and analyzing their relevancy. Based on the acquisition of information described above, the general security situation of the network can be obtained. The process of understanding can also be considered a process of situation evaluation, along with data analysis for network security situation evaluation. In the proposed scheme, network security situation evaluation is not a single security event, and it considers the entire network security state in general, by evaluating the security of the entire network and assisting in decision-making.

After the association understanding, the security related data in a long time forms the big data. To realize the security situational awareness, neural networks and game theory are used to perform the big data analysis. In fact, awareness of network security situation means predicting the development trends of the network in next phase based on historical information of the network security situation. The prediction of network security situation is a primary goal of situational awareness. Because of the randomness and the uncertainty, the security situation transformation is a complex and non-linear process. This limits the applicability of traditional prediction models. To date, network security situational prediction has usually employed neural networks, time-sequence prediction methods, support vector machine (SVM), etc. Most game theory models focus on the equilibrium problem. In fact, the learning model can provide efficient methods for evaluating and optimizing traditional equilibrium concepts. Here the learning model indicates the learning rules of the game player, and checks the interaction among the players.

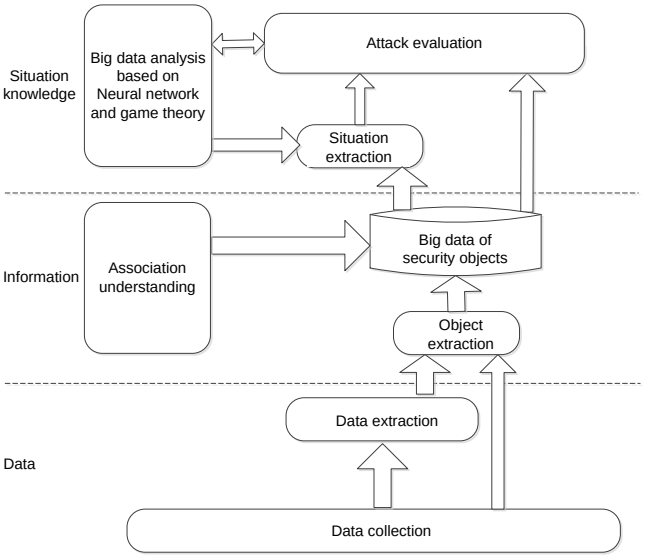


Fig. 3. Design principle of the proposed security situational awareness mechanism.

4.2 Security Situational Factor Collection and Extraction

Agent technology is used to perform the security factor collection. A collection agent executes instructions from the security awareness center. It performs the time-lapse collection of the data and reports the data to the management layer after filtration and preprocessing. Additionally, the state data from the devices on the clients can be reported to the management layer through a collection agent.

The mian principles of security situational factor collection and extraction are shown in Fig. 4. The rules of extraction are defined as limitation rules for descriptions of the users' requirements. Situational factors store the security related information and heterogeneous schemes according to the specified format. The inference machine performs the inference operations in the process of requirement parsing, decomposition and optimization. The wrapper and dispatcher perform the packaging and distribution of the task execution. The integrated engine performs the integration of the processing results of different components. In the proposed scheme, semi-structured and unstructured data will be managed uniformly.

In the proposed scheme, three types of situational factors are used to realize the basic situational factor collection: network flow, access control operations and device states. For network flow, we perform the network flow

collection based on Simple Network Management Protocol (SNMP) and the underlying package to capture the flow of the operation systems. Here, SNMP is the standard tool for managing TCP/IP network communications. In the smart grid, SNMP prevails over other commonly used technologies for network management such as common object request broker architecture (CORBA) or network configuration protocol (NETCONF), and has been implemented in most communication architectures. For device state, we also use SNMP technology to realize the situational factor collection. There are three types of components for the device-state situational factor collection including managed devices, agents and Network Management Stations (NMSs) which are deployed in the situational analysis center. A managed device is a node of the smart grid, that is used to collect and store the network status, as reported to NMS based on SNMP. Network devices in the smart grid (e. g. routers, servers, switches, network bridges, Hubs, etc.) can act as managed devices. An SNMP agent is a management software component in the managed devices. An SNMP agent collecs local information for further management, and transfers the information into compatible format for the SNMP. NMSs are located in the situational monitoring center, which can also provide storage resources for network management. For the access control operational factor, we use the previous method of ours to perform the collection of situational factors. In addtion, the features in DARPA 1998 are used as the security situational factors.

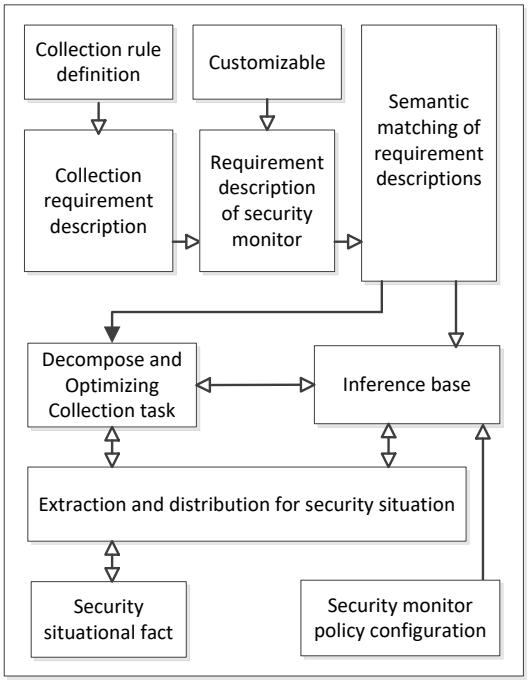


Fig. 4. Architecture of security situational factor collection and extraction.

The feature extraction of the situational factor is based on the Information Gain Ratio (IGR), which is used as a measure to determine the relevance of each feature [24].

4.3 Association Analysis for Security Situational Factors

The big data-related security in smart grids involves very complex situations. Simple and static rules cannot address the complex analysis. Moreover, the hard boundary in most attribution partitions of existing association analysis methods cannot resovle this problem. Fuzzy association is used to deal with the hard boundary problem after performing the discrete interval partition on the quantitative attributes. Currently, data analysis is a very important issue for the security situational awareness. As a matter of fact, fuzzy clustering is an efficient and appropriate tool for performing the classification, and it makes the classification results conform more to reality. We use graph theory based fuzzy cluster to realize the data association analysis [25], [26].

To perform the classification, the equivalent relation is usually applied. In the proposed scheme, we use the fuzzy equivalent relations to perform cluster analysis for the association analysis for the big data of the situational factors.

Definition I: Suppose that the fuzzy subset of the following product sets is a fuzzy relation between *M* and *N*, where *M* and *N* are two nonempty sets.

$$M \times N = \left\{ (m,n) \middle| m \in M, n \in N \right\} \tag{1}$$

In addition, for correction degree $\tilde{Z}$ of *m* and *n*, which is denoted as $\varepsilon_{\tilde{Z}}$, the function of membership is defined as follows

$$\varepsilon_{\tilde{Z}} : M \times N \to [0,1] \tag{2}$$

Definition II: Suppose there are three nonempty sets *M*, *N*, *L*. Also, $\tilde{Z}_1$ is supposed as the fuzzy relation between *M* and *N*, and $\tilde{Z}_2$ is supposed as the fuzzy relation between *N* and *L*, and $\tilde{Z}$ is the fuzzy relation between *N* and *L*. The relations among $\tilde{Z}$, $\tilde{Z}_1$ and $\tilde{Z}_2$ can be got as follows.

$$\tilde{Z} = \underset{n \in N}{\vee} [\tilde{Z}_1(m,n) \wedge \tilde{Z}_2(n,l)] \tag{3}$$

Suppose that $\tilde{Z}_1 = (z_{ij})$, $\tilde{Z}_2 = (z_{jk})$, and $\tilde{Z}_3 = (z_{ik})$ are the fuzzy matrixes of $(m \times n)$, $(n \times e)$ and $(m \times e)$order, respectively. Then the relation among z_{ij}, z_{jk} and z_{ik} can be got as

$$z_{ik} = \overset{e}{\underset{i=1}{\vee}} \left(z_{ij} \wedge z_{jk} \right), (i = 1,2,\cdots,e; k = 1,2,\cdots,y) \tag{4}$$

Specifically, $\tilde{Z}$ is supposed as the the fuzzy relation on *M*. Also, we suppose that $\tilde{Z}^2 = \tilde{Z} \circ \tilde{Z}$, where $\tilde{Z}^2$ is also the the fuzzy relation on *M*. Then $\tilde{Z}^2$ can be computed based on following equation for arbitrary $(m,l) = M \times M$.

$$\tilde{Z}^2 (m,l) = \underset{n \in M}{\vee} \left[\tilde{Z}(m,n) \wedge \tilde{Z}(n,l) \right] \tag{5}$$

Based on above method, $\tilde{Z}^k$ can be calculated.

Definition III: $\tilde{Z}$ is supposed as the fuzzy relation on *M*. If we choose randomly the values of *m* and *n*. Then $\tilde{Z}$

follows the rules as

1) Transitivity: $\tilde{Z}(m,m)=1$
2) Reflexivity: $\tilde{Z}(n,m)\geq\tilde{Z}^2(m,n)$
3) Symmetry: $\tilde{Z}(m,n)=\tilde{Z}(n,m)$

In above rules, the fuzzy relation on *M* is denoted as $\tilde{Z}$, if above symmetry and reflexivity are satisfied. The fuzzy similarity matrix and fuzzy equivalent matrix are used, respectively, to denote above issues.

In the fuzzy cluster based association analysis, according to the equivalent relations, the domain of discourse *A* can be parted into a number of non-intersecting subsets. This is based on the underlying reason that the relative features between general relations and fuzzy equivalent relations and are very valuable. The equivalent classes are the classifaction of partition of *A*, which are coursed by general equivalent relations. This classification of partition for *A* can be regarded as a cluster, which is based on the equivalent relations. For an arbitrary two-element which are denoted as *p* and *q*, the owner-member relationship cannot be applied to represent the relations between (*p*, *q*) and $\tilde{Z}$. Therefore, the situation of fuzzy equivalent relations is more complex. The degree of membership is applied to represent above situation. There is some degree on the relation between *p* and *q*, and thus, there is a fuzzy bound of η . In other words, *A* cannot be parted based on only $\tilde{Z}$. Because the fuzzy equivalent relation is denoted as $\tilde{Z}_\eta$, $\tilde{Z}$ is used denote a normal equivalent relation for arbitrary $\eta\in[0,1]$. Moreover, *A* can be divided based on η . Then, $\tilde{Z}_\eta$ depends on the value of η . Therefore, the partitions of *A* can be performed through applying fuzzy equivalent relations based on the value of η.

Clustering on the security situation factors is applying a number of similarities to evaluate the closeness degree of the factors, based on which association analysis can be performed. To enhance the efficiency of the association analysis, the construction of fuzzy equivalent relations for the attributes of the situational factors is realized based on the fuzzy cluster. The association analysis based on fuzzy cluster can be realized as follows.

- Suppose that the sample set is $M=\{m_1,m_2,\cdots,m_k\}$, where $m=\{m_{i1},m_{i2},\cdots,m_{iw}\}$, *i*={1, 2, …, *k*}. Before the process for the samples, the original factor of the indicators of m_i must be standardized. Next, the similarity factor among all of the m_i and m_j, can be calculated once applicable equation must be applied. The fuzzy relation matrix $\tilde{Z}=(z_{ij})_{k\times k}$ must be constructed. In general, according to above principle, the matrix of fuzzy relation $\tilde{Z}$ can be got.
- $g(\tilde{Z})$ is used to denote the transitive closure of $\tilde{Z}$. As the fuzzy equivalent relation of $\tilde{Z}$, $g(\tilde{Z})$ must be calculated.
- In the security big data analysis of smart grid, an applicable $\eta\in[0,1]$ must be selected based on the requirements of the real security situational question. After that, the computation of η division of $g(\tilde{Z})$ must be computed, which is denoted as $g(\tilde{Z})_\eta$. Then an association analysis result corresponding to *M* can be got.

4.4 Security Situational Awareness based on Game Theory and Reinforcement Learning

In this section, we use game theory and reinforcement learning to realize security situational awareness for smart grid. Here the legitimate users and attackers are the players in the game. As a matter of fact, equilibrium in the game theory is the long-term process for the irrational players to find the optimal results over time.

Under the given conditions, it is very important to determine when the convergence will be satisfied. Additionally, it is very important to between two different but relevant types of game models, which are used to perform the modelling of the strategies of the players in the games.

In evolutionary game theory, the most important issue for individual players is to adjust their behaviors according to the behaviours of other players in the interaction environment. To perform the security situational awareness in the smart grid, a hierarchical neural network is introduced into the game theory. According to the requirements of the security situational factors, input and output parameters are based on aforementioned factor collection and extraction rules. In addition, a number of factor values are collected as the training samples for the neural network. To establish the security situational awareness model, the real security factor data are inputed into the neural network. Next, the output results of the neural network are compared with the output results of the modelling objects, and the errors aere used to adjust the parameters of the learning model. Finally, the neural network is established to present the corresponding relations between the real input and output.

When the learning model is established, the parameters that have higher impacts on the output object should be selected, and thus, the dimension of the model can be reduced and the model can be simplified. For the process of a game, the interactive learning is different from the learning of each individual player. For given *c* players, each player changes his or her behavior strategy through learning other (*c*-1) players. In other words, there are mutual impacts between the selection of a player and the others' selections. In this state, the benefits of any individual player at least depend at least partly on the network actions of other individual players. According to the mutual interactions, the individual player can exhibit the behaviors of encouraging strategy formation.

In the proposed security situational awareness mechanism, the essence of the neural network in the game process is based on the improvement of a single neuron perceptron, in which the information process includes forward propagation and backward feedback. The learning of the network is a process that the errors propagate from input layer to output layer and corrects the right weights of network connections. The object of the learning is to make the real output of the network closed to a given expected output. The payoff actions of the payoff matrix in the Prisoner's Dilemma [27] is used to act as the input nodes, and two output nodes denote the security situations. To simplify the awareness model, the single neuron perceptron is used as the base. Meanwhile, retrospect

optimum is used to modify the feedback process. Each value of the payoff matrix in the game acts an input node d_j, and each selectable behavior of the player acts as an output node f_j. If the nodes of the input information are the payoff values of currenthyperbolic tangent game, then every input node corresponding with the output nodes is multiplied by the connection r_{ij}. Next, currenthy perbolic tangent function is used as the active function of the neural network and is computed as follows.

$$f_i = Acti\left(\lambda \times \sum_j r_{ij} x_j\right) = \frac{1}{1+e^{-\left(\lambda \times \sum_j r_{ij} z_j\right)}} \quad (6)$$

where λ is the parameter of precipitous degree to adjust the active function.

The active values of output nodes indicate the preferences of certain security behavior, which can be transformed into the real possibility of certain security behaviors through standardization. The learning process can be simulated by updating the weights.

$$r_{ij}^t = r_{ij}^{t-1} + \Delta r_{ij} \quad (7)$$

Suppose that the learning process is performed after the event. After the player knows the behaviors of other players, they change their behaviors according to the optimal strategy they regarded. They will adjust the network based on optimal strategy. In other words, a player knows the behaviors of another player in last phase, thus the player transfer his or her current behaviors as the optimal response of last phase. Assume that *k*-th player selects the *g*-th strategy, the updating rules is as follows.

$$\Delta r_{ij} = \omega^2 \times \left[t_i\left(\partial^{-k} - f_i\right)\right] \times B^k\left(\partial_g^k, \partial^{-k}\right) \times d_j \quad (8)$$

where $t_i\left(\partial^{-k}\right)$ is an optimum response of the *k*-th player according to the behaviors of other players. f_i is the tendency for the player to select *i*-th behavior. $B^k(\bullet)$ is the adjusted value based on the behaviors of the *k*-th player and other players. d_j is the strength of input nodes, which can be regarded as payoff, and ω is learning rate. The adjusted value is got by computing the difference value between the real payoff and possible maximal payoff. Compared with traditional awareness rules, the weight updating rules have the error feedback with adjusted value. Maximum payoff is added into the weight updating rules. In other words, the player can change the strategy for the direction of getting maximum payoff. Thus strategy of the proposed scheme can achieve the maximum benefits. If there is some strategy can make the system get maximum benefits comparing with the selected strategy, this weight of the strategy will be enhanced in next behavior.

The reinforcement learning for the game can be divided into two phases. In the first phase, the computation is performed from the input to the output of neural network. If the construction of the network and weights are given, the output can be computed based on Eq. (6). In the second phase, the weight should be modified, in which the computations and modifications are performed based on the feedback from the output.

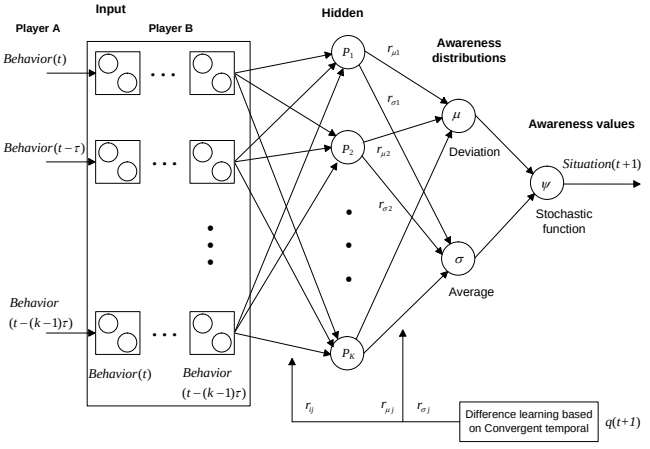


Fig. 5. Situational awareness model.

The situation factor parameter of the security situation is denoted as a vector *Situation*= [$factor_1$, $factor_2$, ..., $factor_k$], which includes the concerned node ID, node address, attack state, attack time, etc. As shown in Fig. 5, the neural network of the awareness system includes four layers: input, hidden, stochastic and output layers. The interactions among the game players are considered.

Input: A vector $S(t)$ with k dimensions denotes the inputs of awareness model on time t. $Situation(t)$ is used to denote the security situation on time t. The input vector includes k observed points with given time intervals.

$$\begin{aligned} S(t) &= (s_1(t), s_2(t), \cdots, s_k(t)) \\ &= (Situation(t), Situation(t-\tau), \cdots, Situation(t-(k-1)\tau) \end{aligned} \quad (9)$$

where time delay is denoted as τ.

Hidden: Multiple nodes accept input with weights r_{ij}, and their output is given by:

$$P_j(t) = \frac{1}{1+e^{-\xi_P \sum \partial_i(t) r_{ij}}} \quad (10)$$

where ξ_P is a constant.

Stochastic: A Gaussian distribution is considered to be used to represent the distribution of the output. For every hidden node $P_j(t)$, parameters of Gaussian distribution are connected with weight $r_{\sigma j}$ and weight $r_{\mu J}$ The output of stochastic layer can be got as follows:

$$\mu(P_j(t), r_{j\mu}) = \frac{1}{1+e^{-\xi_\mu \sum P_j(t) r_{j\mu}}} \quad (11)$$

$$\sigma(P_j(t), r_{j\sigma}) = \frac{1}{1+e^{-\xi_\sigma \sum P_j(t) r_{j\sigma}}} \quad (12)$$

Output layer: An output layer node denotes a stochastic policy of reinforcement learning. 1-dimension Gaussian function is used to describe the output layer.

$$\psi(Situation(t+1),R,S(t))=\frac{1}{\sqrt{2\pi\sigma}}e^{\frac{(Situation(t+1)-\mu)^2}{2\sigma^2}} \quad (13)$$

Temporal-difference learning is used to update the weights, which learns a linear approximation to the state-value function for a given policy and Markov decision process (MDP) from sample transitions. We use both the MDP and the policy to be stationary, so their combination determines the stochastic dynamics of a Markov chain. The state of the chain at each time t is a random variable, denoted as U_t={1, 2, …, K} . On each transition from e_t to u_{t+1}, there is also a reward b_t+1, whose distribution depends on both states. The parameter $u \in \Im^k$ of an approximate value function should be seeked, such that

$$L_\beta(u)=U^{\mathrm{T}}\theta_e \approx L(u)=E\left\{\sum_{t=1}^{\infty}\nu^t b_{t+1} \mid u_0=u\right\} \quad (14)$$

where $\beta_e \in \Im^k$ is feature vector characterizing state e. In addition, $\nu \in [0,1)$ is the discount rate, which is a constant.

Based on the temporal difference error, r can be updated as follows.

$$r_{k+1}=r_k+Q_k(\ell_k-\theta_k^{\mathrm{T}}r_k)\theta_k \quad (15)$$

where Q_k denotes the parameters of step-size.

5 Evaluations

5.1 Simulations

To implement the simulations for the proposed security situational awareness mechanism, we use the data set in DARPA Intrusion Detection Evaluation Data [28] for test and training. Eight weeks of network-based attacks of general background data are used for the training. To keep the universality of the data, the midst data of the general background data are used. On the other hand, two weeks attack and background data are used for test. The weights of the proposed awareness mechanism and the constants in the stochastic as well as hidden layers are set according to the corresponding parameters in [29] for comparisons.

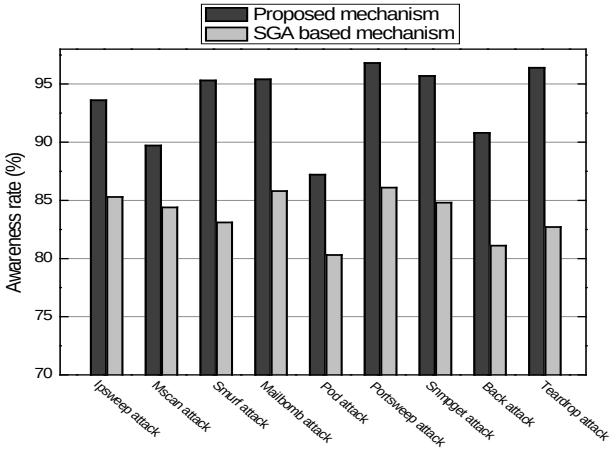


Fig. 6. Awareness rate simulation.

The evaluations and comparisons of the awareness are shown in Fig. 6. In Fig. 6, the awareness rate is denoted as the vertical coordinate. Moreover, nine types of attacks in DARPA Intrusion Detection Evaluation Data are denoted as a number of groups of columns, which are IPsweep attack, Mscan attack, Smurf attack, Mailbomb attack, Pod attack, Portsweep attack, Snmpget attack, Back attack, and Teardrop attack. As illustrated in Fig. 6, the awareness rate of the proposed mechanism is higher than that of SGA based scheme in [29], and the increment is 9.7% on average, which show the obvious advantages of the proposed mechanism on awareness rate.

5.2 Experiment

To collect the security related big data, the security situational factor data are collected from the communication network of the system in an electric power corporation. Figure 7 illustrates the network topology. The production area processes the operations of electricity generation, consumption, etc. Based on aforementioned data collection scheme, three kinds of situational factors are used to realize the basic situatinal factor collection, which are network flow, access control operations and devices states. The situational factor data are collected and stored for a long term. Then the data are analyzed based on the proposed mechanism. Security management device reorganizes the abnormal behavior and restores the potential threats in the network.

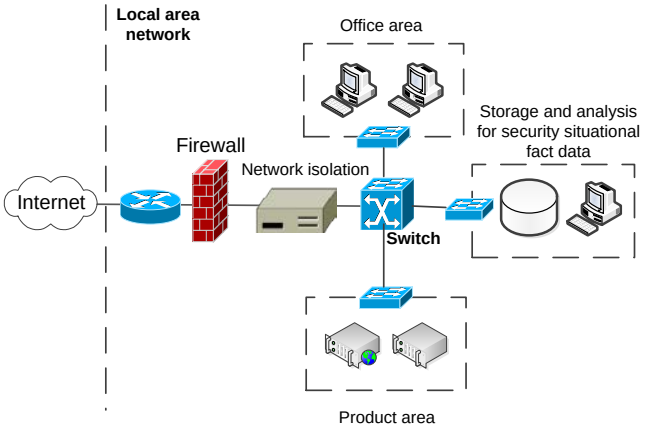


Fig. 7. The experiment network topology.

The data analysis experiment is performed on cluster computers with 25 nodes, in which every server has a 2.53 GHz Intel i5 CPU and 8GB of memory. In addition, the servers are connected based on a 1G router. We apply Hadoop-1.0.4 as the experimental tool for the data analysis.

The data are collected over half of a year. Here we use the data from the last three months of the collection period (Sept. 16, 2015 to Dec. 14, 2015) to test the awareness mechanism. The risk value *RIS* is defined to quantify the security situation. There are four intervals for the risk value, which are high risk (66<*RIS*≤100), middle risk (33<*RIS*≤66), low risk (0<*RIS*≤33), security(*RIS*≤=0). The intervals are just used to divide the section. The basic risk score of a vulnerability is 1, and the initial cumulative

value for high vulnerability, medium vulnerability and low vulnerability are 66, 33, and 0, respectively. In every interval, the scores of the vulnerabilities are cumulative untill the risk scores reach the upper limit of the interval. The accumulative risk value over a certain term is shown in Fig. 8.

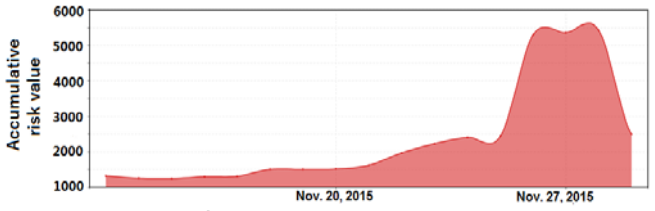


Fig. 8. Awareness of the accumulative risk.

Next, we evaluate the error of the security situational awareness. To avoid the negative effects of the large span of the original data, the security factor data are standardized for extrema. For original data $Y=(y_1, y_2, \ldots, y_k)$, the extremum standardization process is computed as follow.

$$y_i' = \frac{y_i - \min(y)}{\max(Y) - \min(Y)} \tag{16}$$

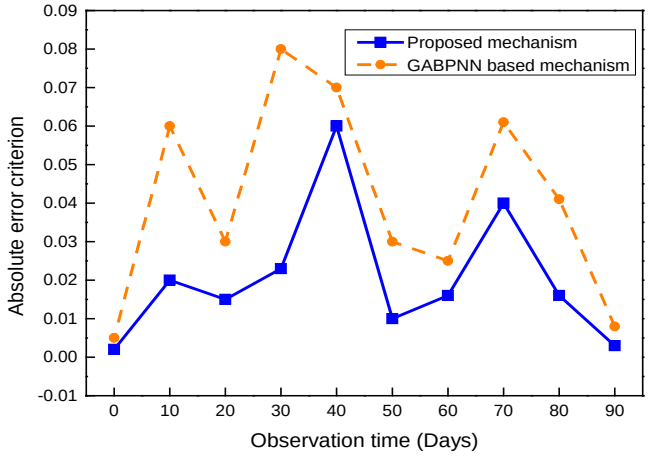


Fig. 9. Absolute error criterion of the awareness.

To evaluate the advantages of the proposed situational awareness mechanism, the GABPNN mechanism in [30] is introduced for comparison. Absolute error is used as the evluation criterion. The absolute error criterion is shown in Fig. 9. In generally, the absolute error of the proposed mechanism is lower than that of GABPNN.

6 Conclusion

Security is one of the key concerns for the smart grid. To realize the security situational awareness mechanism based on the analysis of big data in the smart grid, this paper seamlessly integrated fuzzy cluster based association analysis, game theory and reinforcement learning. Based on the proposed mechanism, the extraction of network security situation factors, network situational assessment and security situational prediction can be realized for the smart grid. The simulation and experimental results show the high awareness rate and low error rate of the proposed mechanism. The work in this paper is significant for impoving the security of the smart grid.

Acknowledgment

This work was supported in part by the National Natural Science Foundation of China under Grant 61401273, 61372049, 61431008 and in part by the Japan Society for the Promotion of Science within the Grants-in-Aid for Scientific Research through the A3 Foresight Program under Grant 15K15976 and Grant 26730056. The corresponding author of this paper is Miangxiong Dong (mx.dong @csse.muroran-it.ac.jp).

References

[1] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart Grid-The New and Improved Power Grid: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 4, pp. 944-980, Forth Quarter 2012.

[2] J. Wu, M. Dong, K. Ota, Z. Zhou, and B. Duan, "Towards Fault-Tolerant Fine-Grained Data Access Control for Smart Grid," *Wireless Personal Communications*, vol. 75, no. 3, pp. 1787-1808, Apr. 2014.

[3] X. Wang and P. Yi, "Security Framework for Wireless Communications in Smart Distribution Grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 809-818, Nov. 2015.

[4] K. C. Sou, H. Sandberg, and K. H. Johansson, "On the Exact Solution to a Smart Grid Cyber-Security Analysis Problem," *IEEE Transactions on Smart Grid*, vol. 4, no. 2, pp. 856-865, May 2013.

[5] Y. Yan, R. Q. Hu, S. K. Das, H. Sharif, and Y. Qian, "An Efficient Security Protocol for Advanced Metering Infrastructure in Smart Grid," *IEEE Network*, vol. 27, no. 4, Jul./Aug. 2013.

[6] G. N. Ericsson, "Cyber Security and Power System Communication-Essential Parts of a Smart Grid Infrastructure," *IEEE Transactions on Power Delivery*, vol. 25, no. 3, pp. 1501-1507, Jun. 2010.

[7] M. R. Endsley, "Design and Evaluation for Situation Awareness Enhancement," *Proc. 32nd Human Factors Society Annum Meeting*. pp. 97-101, 1988.

[8] T. Bass, A. Arbor, "Multisensor Data Fusion for Next Generation Distributed Intrusion Detection Systems," *Proc. of IRIS National Symposium on Sensor and Data Fusion*. pp. 24-27, 1999.

[9] S. Jajodia，S. Noel, B. O'Berry, "Topological Analysis of Network Attack Vulnerability,"*Proc. of the 2nd ACM symposium on Information, Computer and Communications Security*, pp. 2-2, 2007.

[10] R. Xi, S. Jin, X. Yun, and Y. Zhang, "CNSSA: A Comprehensive Network Security Situation Awareness System," *Proc. of 2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pp. 482-487, 2011.

[11] D. Kolev, R. Koelle, R. A. Casar Rodriguez, and P. Montefusco, "Security Situation Management-Developing a Concept of Operations and Threat Prediction Capability," *Proc. of 2015 IEEE/AIAA 34th Digital Avionics Systems Conference (DASC)*, pp. 4C2-1-4C2-11, 2015.

[12] F. Chen, Y. Shen, G. Zhang, and X. Liu, "The Network Security

Situation Predicting Technology based on the Small-World Echo State Network," *Proc. of 2013 4th IEEE International Conference on Software Engineering and Service Science (ICSESS)*, pp. 377-380, 2013.

[13] P. Harmer, R. Thomas, B. Christel, R. Martin, and C. Watson, "Wireless Security Situation Awareness with Attack Identification Decision Support," *Proc. 2011 IEEE Symposium on of Computational Intelligence in Cyber Security (CICS)*, pp. 144-151, 2011.

[14] J. Kim, I. Moon, K. Lee, S. C. Suh, and I. Kim, "Scalable Security Event Aggregation for Situation Analysis," *Proc. of 2015 IEEE First International Conference on Big Data Computing Service and Applications (BigDataService)*, pp. 14-23, 2015.

[15] R. Morello, C. De Capua, "An ISO/IEC/IEEE 21451 Compliant Algorithm for Detecting Sensor Faults: an approach based on repeatability and accuracy, " IEEE Sensors Journal, vol. 15, no. 5, pp. 2541 - 2548, May. 2015.

[16] L. Guo, J. Wu, Z. Xia, and J. Li, "Proposed Security Mechanism for XMPP-Based Communications of ISO/IEC/IEEE 21451 Sensor Networks," IEEE Sensors Journal, vol. 15, no. 5, pp. 2577-2586, May. 2015.

[17] R. Morello, "Use of TEDS to Improve Performances of Smart Biomedical Sensors and Instrumentation: an overview on advances and applications of ISO/IEC/IEEE 21451 Standard," IEEE Sensors Journal, vol. 15, no. 5, pp. 2497-2504, May 2015.

[18] X. Wang, G. Castelli, B. C. Chiu, J. Xu and D. Sun, "Comprehensive Situation Awareness in a Very Large Power Grid Control Center," *Proc. 2012 IEEE PES Transmission and Distribution Conference and Exposition (T&D)*. pp. 1-6, 2012.

[19] R. Agrawal, T. Imielinske, and A. Swami, "A Mining Association Rules between Sets of Items in Large Databases," *Proc. of the ACM SIGMOD International Conference on the Management of Data*, pp. 207-216, 1993.

[20] N. Hanaki, R. Sethi, I. Erev, A. Peterhansl, "Learning Strategies," *Journal of Economic Behavior and Organization*, vol. 56, no. 4, pp. 523-544, Apr. 2005.

[21] C. F. Camerer, "*Behavioral Game Thoery: Experiments in Strategic Interaction*," Princeton, New Jersey, Princeton University Press, 2003.

[22] Q. Sun, G. Ren, and X. Qi, "Interactive Learning Neural Networks for Predicting Game Behavior," *Proc. of Advances in Neural Networks-ISNN* 2009, pp. 774-783, 2009.

[23] R. Selten, R. Stocker, "End Behavior in Sequences of Finite Prisoner's Dilemma Supergames a Learning Theory Approach," *Journal of Economic Behavior and Organization*, vol. 7, no. 1, pp. 47-70, Mar. 1986.

[24] J. R. Quinlan, "Induction of Decision Trees," *Machine Learning*, vol. 1, pp. 81-106, 1986.

[25] S. S. Ray, "*Graph Theory with Algorithms and its Applications: In Applied Science and Technology*," Springer Publisher, 2013.

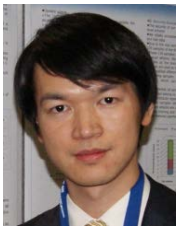
[26] O. Wolkenhauer, "*Data Engineering: Fuzzy Mathematics In Systems*," John Wiley & SonsInc Publisher, 2001.

[27] W. Poundstone, *Prisoner's Dilemma*, Anchor; Reprint edition, Jan. 1993.

[28] DARPA, "DARPA 1998 Intrusion Detection Evaluation, "http://www.ll.mit.edu/mission/communications/ist/corpora/ideval/data/1998data.html, 1998.

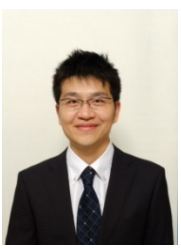
[29] T. Kuremoto, M. Obayashi, and K. Kobayashi, "Nonlinear Prediction by Reinforcement Learning," *Proc. of International Conference on Intelligent Computing (ICIC 2005)*, pp. 1-10, 2005.

[30] H. Q. Wang, J. B. Lai, and X. Wu, "A Quantitative Forecast Method of Network-Secuity-Situation—Based on the BP Neural-Network with Genetic Algorithm," *Proc. of Second International Multisymposium on Computer and Computational Sciences*, pp. 474-380, 2007.



Jun Wu is an Associate Professor of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, China. He obtained his PH.D. Degree in Information and Telecommunication Studies (GITS) at Waseda University, Japan. He was a postdoctoral researcher for the Research Institute for Secure Systems (RISEC), National Institute of Advanced Industrial Science and Technology (AIST), Japan, from 2011 to 2012. He worked as a researcher for the Global Information and Telecommunication Institute (GITI), Waseda University, Japan, from 2011 to 2013. His research interests include the advanced computation and communications techniques of smart sensors, wireless communication systems, industrial control systems, wireless sensor networks, smart grids, and more. He has hosted and participated in several research projects for the National Natural Science Foundation of China, National 863 Plan and 973 Plan projects, etc. He has been a Guest Editor for the IEEE Sensors Journal and a TPC Member of several international conferences including WINCON 2011, GLOBECOM 2015, etc. He is a member of IEEE.

Kaoru Ota (M'12) was born in Aizu Wakamatsu, Japan. She received M.S. degree in Computer Science from Oklahoma State University, USA in 2008, B.S. and Ph.D. degrees in Computer Science and Engineering from The University of Aizu, Japan in 2006, 2012, respectively. She is currently an Assistant Professor with Department of Information and Electronic Engineering, Muroran Institute of Technology, Japan. From March 2010 to March 2011, she was a visiting scholar at University of Waterloo, Canada. Also she was a Japan Society of the Promotion of Science (JSPS) research fellow with Kato-Nishiyama Lab at Graduate School of Information Sciences at Tohoku University, Japan from April 2012 to April 2013. Her research interests include Wireless Networks, Cloud Computing, and Cyber-physical Systems. She has received best paper awards from ICA3PP 2014, GPC 2015, IEEE DASC 2015 and IEEE VTC 2016. She serves as an editor for IEEE Communications Letter, Peer-to-Peer Networking and Applications (Springer), Ad Hoc & Sensor Wireless Networks, International Journal of Embedded Systems (Inderscience), as well as a guest editor for IEEE Wireless Communications, IEICE Transactions on Information and Systems. She is currently a research scientist with A3 Foresight Program (2011-2016) funded by Japan Society for the Promotion of Sciences (JSPS), NSFC of China, and NRF of Korea.



Mianxiong Dong (M'13) received B.S., M.S. and Ph.D. in Computer Science and Engineering from The University of Aizu, Japan. He is currently an Associate Professor in the Department of Information and Electronic Engineering at the Muroran Institute of Technology, Japan. Prior to joining Muroran-IT, he was a Researcher at the National Institute of Information and Communications Technology (NICT), Japan. He was a JSPS Research Fellow with School of Computer Science and Engineering, The University of Aizu, Japan and was a visiting scholar with BBCR group at University of Waterloo, Canada supported by JSPS Excellent Young Researcher Overseas Visit Program from April 2010 to August 2011. Dr. Dong was selected as a Foreigner Research Fellow (a total of 3 recipients all over Japan) by NEC C&C Foundation in 2011. His research interests include Wireless Networks, Cloud Computing, and Cyber-physical Systems. He has received best paper awards from IEEE HPCC 2008, IEEE ICESS 2008, ICA3PP 2014, GPC 2015, IEEE DASC 2015 and IEEE VTC 2016. Dr. Dong serves as an Editor for IEEE Communications Surveys and Tutorials, IEEE Network, IEEE Wireless Communications Letters, IEEE Cloud Computing,

IEEE Access, and Cyber-Physical Systems (Taylor & Francis), as well as a leading guest editor for ACM Transactions on Multimedia Computing, Communications and Applications (TOMM), IEEE Transactions on Emerging Topics in Computing (TETC), IEEE Transactions on Computational Social Systems (TCSS), Peer-to-Peer Networking and Applications (Springer) and Sensors, as well as a guest editor for IEEE Access, Peer-to-Peer Networking and Applications (Springer), IEICE Transactions on Information and Systems, and International Journal of Distributed Sensor Networks. He has been serving as the Program Chair of IEEE SmartCity 2015 and Symposium Chair of IEEE GLOBECOM 2016, 2017. Dr. Dong is currently a research scientist with A3 Foresight Program (2011-2016) funded by Japan Society for the Promotion of Sciences (JSPS), NSFC of China, and NRF of Korea..

Jianhua Li is a professor/Ph.D. supervisor and the dean of School of Information Security Engineering, Shanghai Jiao Tong University, Shanghai, China. He got his BS, MS and Ph.D. degrees from Shanghai Jiao Tong University, in 1986, 1991 and 1998, respectively. He was the chief expert in the information security committee experts of National High Technology Research and Development Program of China (863 Program) of China. His research interests include information security, signal process, computer network communication, etc.

Hongkai Wang received M.S. degree in Control Theory and Control Engineering from Zhejiang University, China in 2008. He is currently the vice director of the Information and Telecommunication Branch of Zhejiang Electric Power Corporation, State Grid Corporation of China. He is in charge of the system design and establishment of Zhejiang Electric Power Corporation, State Grid Corporation of China. Hie research interests include big data of smart grid, big data security, etc.