An Active Security Defense Strategy for Wind Farm Based on Automated Decision

Jun Lai,Bin Duan,Yongxin Su
College of Information Engineering, Xiangtan University
Xiangtan 411105, Hunan, China
793242374@qq.com

Lan Li,Qiaoxuan Yin
Collaborative Innovation Center of Wind Power Equipment and Energy Conversion
Xiangtan, China

***Abstract*—With the development of smart grid, information and energy integrate deeply. For remote monitoring and cluster management, SCADA system of wind farm should be connected to Internet. However, communication security and operation risk put forward a challenge to data network of the wind farm. To address this problem, an active security defense strategy combined whitelist and security situation assessment is proposed. Firstly, the whitelist is designed by analyzing the legitimate packet of Modbus on communication of SCADA servers and PLCs. Then Knowledge Automation is applied to establish the Decision Requirements Diagram (DRD) for wind farm security. The D-S evidence theory is adopted to assess operation situation of wind farm and it together with whitelist offer the security decision for wind turbine. This strategy helps to eliminate the wind farm owners' security concerns of data networking, and improves the integrity of the cyber security defense for wind farm.**

***Index Terms*-- Cyber-Physical Systems, Knowledge Automation, SCADA system, Security, Whitelist.**

I. INTRODUCTION

With the development of smart grid and operation and maintenance service of wind power, the operation data should be transmitted to the remote monitoring center of wind farm through the Internet for large-scale cluster monitoring and fine scheduling in real-time [1], [2]. However, the current wind power monitoring and control network is very fragile [3]. Power system accidents, such as Stuxnet, and Ukraine power outage, caused by malicious network attacks also make wind farm owners worried about data network of wind farm [4], [5].

Wind power SCADA network has the characteristics of simple and reliable communication protocol, fixed control flow, long update cycle of system code and stable network topology as well as the general industrial control network [6]. In recent years, the domestic and foreign scholars have made a lot of research, but there are still many problems in SCADA security defense. Reference [7] illustrated protection techniques of the SCADA system which communicate by FTP and MODBUS protocol, but it didn't analyze SCADA traffic or classify the flow arrival process. Reference [8] presented an innovative approach to the design of filtering systems based on the state analysis of the system being monitored. It referred to MODBUS and DNP3 protocols, but didn't analyze them in-depth. Reference [9] designed a set of intrusion prevention system for SCADA, which can effectively defense the common intrusion, but it didn't filter the non-sensitive packet, and would extend the response time and reduce the flexibility of SCADA system. Reference [10] developed a model-based scheme for detection and isolation of a wide class of faults and attacks in automated canal systems, but it was too abstract and complex to be transplanted and applied to the SCADA network of wind power.

Therefore, we analyze the Modbus protocol which is used in communication between the SCADA system and PLCs, and designs the whitelist according to the characteristics of the packet in traffic. Furthermore, we design the situation assessment to evaluate the security of commands, and present a DRD to integrate the two methods. The paper is organized as following; In the Methodology, the DRD is shown in the forepart, the Whitelist mechanism and the situation assessment is shown in part A and part B separately. In the Case study, the method demonstrated. And the Conclusions are drawn in section IV.

II. METHODOLOGY

Whitelist detection is a kind of excellent industrial network security defense method, and it can effectively filter out malicious command and the threat of abnormal communication. But, it will increase the rate of missing report if used singly. So, we add the situation awareness, which is aimed at provide advice for security decision by integrate dispatch plan, wind speed and the fault warning of equipment, is to improve the accuracy rate of defense.

We used the DRD (Decision Requirement Diagram) to demonstrate the relationship of the two methods in this paper. DRD is a key method in the field of Knowledge Automation. It represents the decision process through a network consisted of knowledge domain, data domain and decision [11]. As shown in Fig.1, the security decision for wind farm security is depend on two sub-decision, operation situation and whitelist. The detail of sub-decision is show in phase B and phase C.

This research was supported by National Natural Science Foundation of China (NSFC) (No.61170191, 61379063)

978-1-5386-2212-4/17/$31.00 ©2017 IEEE

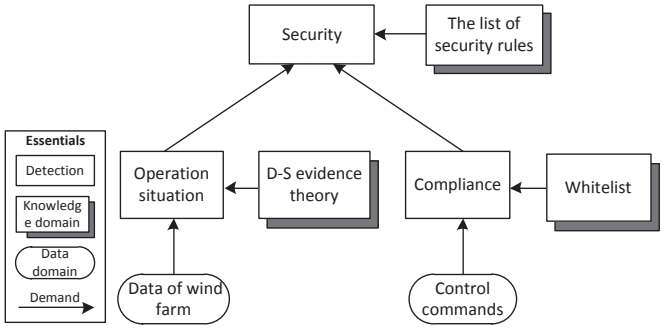

Figure 1. DRD of wind farm security

A. *Whitelist Detection for Control commands*

1) *Control commands based on Modbus TCP*

Modbus is an application layer messaging protocol which provides client/server communication between intelligent devices in SCADA systems. It has the characteristics of standardization, openness, transmission reliability, and widely applied to the current industrial network. There are two ways to implement Modbus. One is based on the serial link called Modbus RTU/ASCII, and the other is based on Ethernet called Modbus TCP/IP.

In the megawatt wind turbine control system, the communication between the SCADA system and the PLC is mainly based on Modbus TCP/IP, whose massage format is shown in Fig.2.

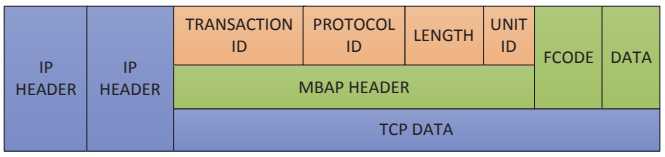

Figure 2. Massage format of Modbus TCP

The MBAP (Modbus Application Protocol) HEADER is used to recognize the data units of MBAP, and the FCODE (Function Codes) indicates to the server (slave) which kind of action to perform [12]. Through packet capture and analysis of the two headers, the control commands of SCADA system to PLCs can be clearly recognized.

2) *Process of Whitelist Detection*

The whitelist can defend against 0 day malware and targeted attacks, and is widely used in information security. Its main idea is to establish a list of legitimate commands, and intercept or alert which out of the list. As shown in Fig.3, the process of whitelist detection includes two parts, automatic whitelist detecting and static whitelist detecting. Automatic whitelist detecting contains two modules for training and testing, and filters the commands of SCADA system to field devices initially.

In the training module, the Modbus TCP packets are captured and resolved. Then based on data mining algorithm, the whitelist is generated automatically by extracting the characteristics of the packets within sensitive commands. In the testing module, we compare the resolved packets with the whitelist, if match, the control command would be marked ALLOW and pass. Otherwise, it would be marked ALERT and wait for a further detecting by static whitelist detection. Combined with automatic and static detection, whitelist filter increases little redundancy of communication system, and effectively reduces the missing and false positives in detection procession.

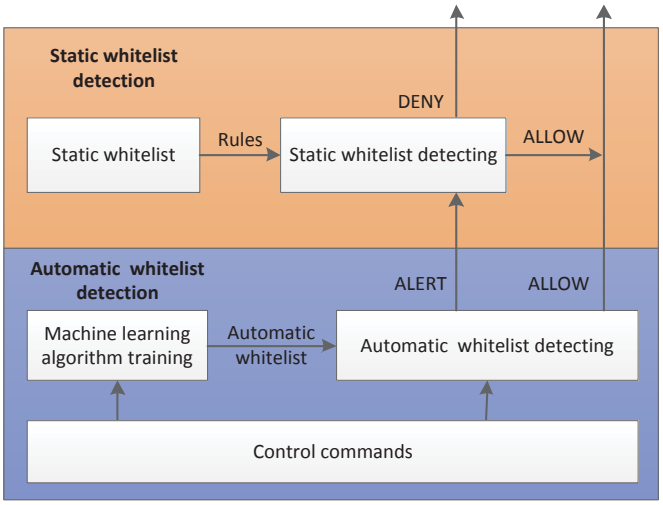

Figure 3. Process of whitelist detection

3) *Static whitelist detection*

In the static whitelist detection, three kinds of whitelists are proposed, as shown in Fig.4. The captured packets from SCADA are filtered through whitelist firstly, which includes Host Whitelist, Header Whitelist and Function Code Whitelist. If the packet passes all the three kinds of whitelist, it would be sent to PLCs; otherwise, it would be intercepted.

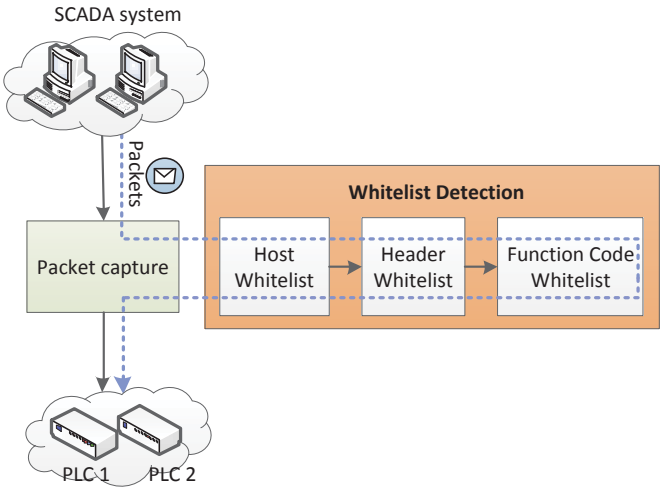

Figure 4. Static whitelist detection of wind turbine command

a) *Host detection*

The MAC and IP of each host of SCADA system in wind farm network are recorded in the Host Whitelist. Due to the low security, the terminal devices, such as backup host,

engineer station and HMI (Human Machine Interface), are easily exploited by attackers. So the Host Whitelist stipulates that only the specified host can send control commands to a certain PLC. As the case is shown in Fig.5, since the Host Whitelist only allows SCADA server 1, whose MAC is 11.11.11.11.11.11 and IP is 10.128.99.101, send commands to PLCs, command sent by SCADA server 2 is regarded as a threat, and would be filtered and denied.

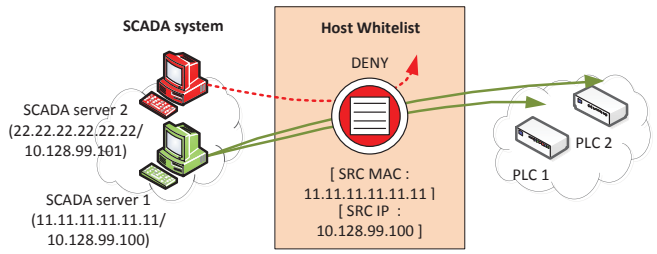

Figure 5. Host Whitelist detection

b) Header detection

Header whitelist includes Modbus TCP header detection and source/destination port detection. Modbus TCP header detection is aimed at the transaction identifier, the protocol identifier, and the length and unit processing. The protocol identifier is used to determine whether the massage is based on Modbus. The length identifier recognizes the unit identifier and the total length of the data, and we can determine whether the packet is randomly constructed by attackers after listening to traffic.

As shown in Fig.6, SCADA server 1 attempts sent a packet with Shutdown command to the PLC 1. Although it has the legality of IP, the protocol identifier and the port, but the length identifier of the suspicious packet is 0x0014, which is obviously not in conformity with the Header Whitelist (assuming normal length identifier of Shutdown command is 0x0006). So this packet is regarded as a suspicious packet, and denied.

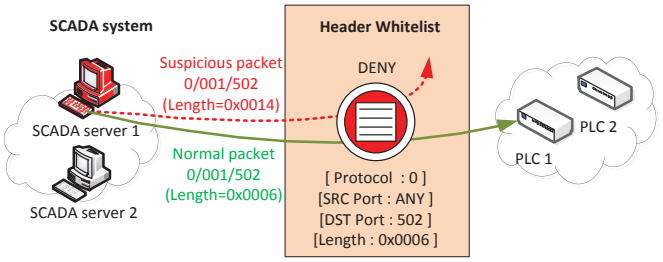

Figure 6. Header Whitelist detection

c) Function code detection

Function code describes the function of the packet, so that we can recognize the kind of command. According to the operation experience to the wind farm, the host (SCADA server) with specific IP address can only send packets with some specific function codes. This mapping is defined in the header whitelist, so that the suspicious packets can be distinguished and filtered out. As the case is shown in Fig.7, the Function Code Whitelist define that the function code of the packet sent from SCADA sever 1, can only be 0x01, 0x02, 0x03, 0x04, 0x05. If the function code of a resolved packet is 0x09, which is not included in the Function Code Whitelist, the packet would be regarded as a suspicious packet, and denied.

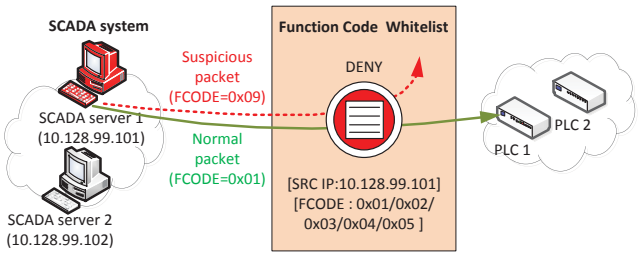

Figure 7. Function Code Whitelist detection

B. *Situation Assessment and Security Decision*

1) Operation situation assessment

Operation situation assessment is a sub-decision in DRD of wind farm security. It is used to perceptive data of the wind farm and to assess the probability of various commands issued. The assessment is based on DS evidence theory, which is widely used in many fields, such as information fusion, expert system, and information analysis. There are two concepts related to DS evidence theory.

Denote by Ω the universal set, and let 2^{Ω} be its power set. A function $M: 2^{\Omega} \to [0,1]$ named basic probability assignment (BPA) is defined to quantify the candidate proposition as follows [13]:

$$M(\Phi)=0, \sum M(A)=1, A \subseteq 2^{\Omega} \quad (1)$$

A peculiar property for the DS evidence theory consists in the capability to combine multiple distinct sources. If we express by M_1, M_2 two BPAs on the same power set 2^{Ω}, a joint BPA m can be obtained by Dempster's rule of combination as follows[13]:

$$M(A)=c^{-1} \sum_{A1 \cap A2=A} M_1(A_1)M_2(A_2), A \neq \Phi \quad (2)$$

$$c=1-\sum_{A1 \cap A2=\Phi} M_1(A_1)M_2(A_2)=\sum_{A1 \cap A2 \neq \Phi} M_1(A_1)M_2(A_2)$$

From (2) to general $M=M_1+M_2+\cdots+M_n$ is defined as following:

$$M(A)=c^{-1} \sum_{\cap A_i=A} \prod_{1 \le i \le n} M_i(A_i), A \neq \Phi \quad \ldots\ldots\ldots\ldots (3)$$

$$c=1-\sum_{\cap A_i=\Phi} \prod_{1 \le i \le n} M_i(A_i)=\sum_{\cap A_i=\Phi} \prod_{1 \le i \le n} M_i(A_i)$$

In operation situation assessment, the dispatch plan, wind speed and the fault warning of equipment are regard as the source of decision. The probability of various command are fused and calculated based on DS evidence theory. When the PLC of wind turbine received a command, we can make the synthesized decision from the probability and the result of the whitelist.

2) Security decision

In order to implement the security decision in DRD, we design the Decision Management Cycle, which includes four structured components, Decision Process, Knowledge Base,

Data Warehouse and Discovery Analysis Module. Decision Process calls the decision service, which is supported by security rules stored in the Knowledge Base, for security decision. Discovery Analysis Module is designed to find, generate and modify the security rules. In the decision process, security decision is made by calling the decision service and input data, which include the operation situation and the whitelist result. The outputs and the logs of the process are stored in the Data Base and will be used to Discovery Analysis Module.

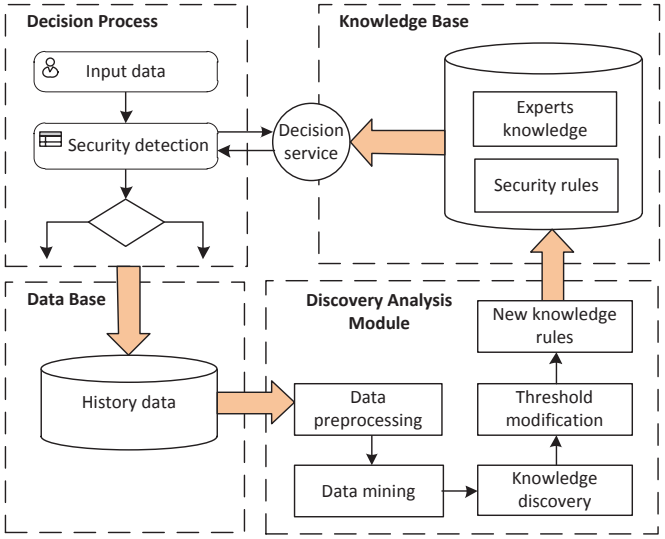

Figure 8. The Decision Management Cycle of security

The security rules mentioned before is packaged in the List of Security Rule as shown in Table1. The probability of the command is divided into four sections and the threshold value is default. In the practical, the threshold is based on expert experience and history data. ALLOW and DENY represent the result of whitelist detection. The level of security state is denoted by A, B, C and D in the table, where A to D indicates that the danger class is increasing successively.

TABLE I. LIST OF SECURITY RULES

Probability interval	Whitelisting result	Security state	Security decision
(0, 25%)	ALLOW	C	Intercept &Alert
	DENY	D	Intercept
(25%, 50%]	ALLOW	B	Pass &Alert
	DENY	D	Intercept
(50%, 75%]	ALLOW	A	Pass
	DENY	C	Intercept &Alert
(75%, 100%)	ALLOW	A	Pass
	DENY	B	Pass &Alert

The list of security rules is used for the security decision, and it is generated and modified by Discovery Analysis Module. As shown in Fig.9, according to the data of input and output, we calculate the rate of missing report and false report based on the Machine learning. And the result will be used to modify the threshold value of probability interval.

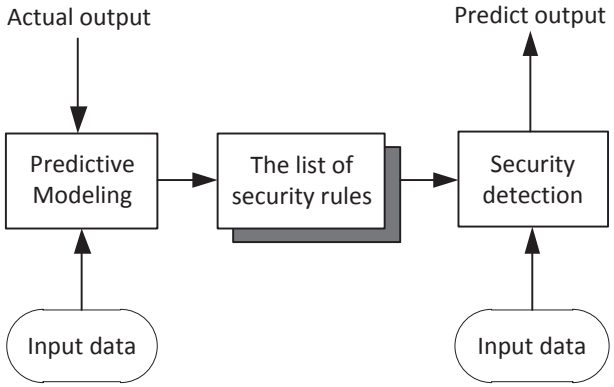

Figure 9. Discovering Analytic Module of security rules

III. CASE STUDY

In order to simplify the calculation, in this example, we select three kinds of evidence sources , the grid-connected wind speed, the fault alarm signal of the key component and the dispatching plan of power grid, and each of them respectively comes from two wind turbines, $1^{\#}$ and $2^{\#}$.

Assuming all evidence sources are positive, that average wind speed over the critical value of grid-connection, no fault alarm for the key components of wind turbine and the period in the dispatch plan. Under the influence of evidences, the probabilities for SCADA system sends Start/Shutdown commands are shown in Table 2. In the practical, the probabilities are arrived at statistical data of the wind farm in a certain time scale, and here only for demonstration.

TABLE II. THE PROBABILITY OF COMMAND UNDER EVIDENCE SOURCE

Evidence Source	Wind turbine $1^{\#}$		Wind turbine $2^{\#}$	
	Start	Shutdown	Start	Shutdown
Standard wind speed	0.6	0.4	0.65	0.35
No fault alarm	0.8	0.2	0.75	0.25
In the dispatch plan	0.85	0.15	0.8	0.2

Next, we fuse the probability under all kinds of evidences. For the jth (j=1, 2)wind turbine, the probability distribution function of a certain command caused by sth(s=1, 2, 3) evidence source, that the wind speed, fault alarm signal and dispatching plan are denoted as 1th, 2nd, 3rd respectively, is noted as M_{sj}. According to (3), for event A:

$$M_s(A_k) = c_s^{-1} \sum_{\bigcap A_m = A_k} \prod_{1 \le j \le J} M_{\mathrm{sj}}(A_m), m = 1, \cdots, k \quad (4)$$

$$c_s = 1 - \sum_{\bigcap A_m = \Phi} \prod_{1 \le i \le J} M_{\mathrm{sj}}(A_m) = \sum_{\bigcap A_i \ne \Phi} \prod_{1 \le i \le J} M_{\mathrm{sj}}(A_m)$$

From (3) and Table II, the computing process of $M_1(\mathit{Start})$ are as following:

$$M_1(Start)=1^{-1}[M_{11}(Start)\cdot M_{12}(Start)+M_{11}(Start)\cdot M_{12}(Shutdown)+M_{11}(Shutdown)\cdot M_{12}(Start)]$$
$$=0.6*0.65+0.6*0.35+0.4*0.65$$
$$=0.86$$
$$M_1(Shutdown)=1-M_1(Start)=0.14$$

The others can be calculated by the same way:

$$M_2(Start)=0.40 \qquad M_2(Shutdown)=0.60$$
$$M_3(Start)=0.97 \qquad M_3(Shutdown)=0.03$$

Then, the fusion results of Start command under each evidence are fused again based on wind turbine $1^{\#}$ and wind turbine $2^{\#}$, as shown in (5):

$$M(A_k)=c^{-1}\sum_{\cap A_m=A_k}\prod_{1\le s\le S}M_s(A_m), m=1,\cdots,K \qquad (5)$$

We can get:

$$M(Start)=0.33368=33.37\%$$
$$M(Shutdown)=0.66632=66.63\%$$

It means, in the current situation, the probability of sending Start command from SCADA system to the PLC is 33.37%, and of sending Shutdown command is 66.63%. Contrast Table I, the two probabilities respectively dropped in (25%, 50%] and (50%, 75%]. For the Start command, if the result of whitelist filtering is DENY, the packet would be intercepted, but if it is ALLOW, the packet would be passed and alerted. For the Shutdown command, if the result of whitelist filtering is DENY, the packet would be intercepted and alerted, but if it is ALLOW, the packet would be passed.

IV. CONCLUSION

The entire work focused on the topic of Cyber security of wind farm. An active defense strategy based on automated decision is designed, which is combined whitelist detection for the control commands and the situation assessment of the wind farm. This strategy can insure the security of the control commands and avoid the impact of the intrusion for the wind farm. Next, we will apply this strategy to the wind farm, and improve the scheme according to the actual effect.

ACKNOWLEDGMENT

The authors would like to show great thanks for the Collaborative Innovation Center of Wind Power Equipment and Energy of China.

REFERENCES

[1] Qinyin Chen, Y. Hu, J. N. Davies and P. Excell, "Wind farm communication system research based on Ethernet," Automatic Control and Artificial Intelligence (ACAI 2012), International Conference on, Xiamen, 2012, pp. 2268-2271.

[2] H. Long, L. Wang, Z. Zhang, Z. Song and J. Xu, "Data-Driven Wind Turbine Power Generation Performance Monitoring," in IEEE Transactions on Industrial Electronics, vol. 62, no. 10, pp. 6627-6635, Oct. 2015.

[3] D. G. Krishna, "Preventive maintenance of wind turbines using Remote Instrument Monitoring System," Power India Conference, 2012 IEEE Fifth, Murthal, 2012, pp. 1-4.

[4] A. Nourian; S. Madnick, "A Systems Theoretic Approach to the Security Threats in Cyber Physical Systems Applied to Stuxnet," in IEEE Transactions on Dependable and Secure Computing , vol.PP, no.99, pp.1-1.

[5] P. Zavarsky, "High assurance cybersecurity plan templates for nuclear facilities: Two-dimensional layering of mutually orthogonal security controls for a high-assurance cybersecurity protection of critical computer-based systems in the post-Stuxnet era," Information Society (i-Society), 2014 International Conference on, London, 2014, pp. 40-44.

[6] X. Fan, K. Fan, Y. Wang and R. Zhou, "Overview of cyber-security of industrial control system," Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC), 2015 International Conference on, Shanghai, 2015, pp. 1-7.

[7] I. Stoian, S. Ignat, D. Capatina and O. Ghiran, "Security and intrusion detection on critical SCADA systems for water management," Automation, Quality and Testing, Robotics, 2014 IEEE International Conference on, Cluj-Napoca, 2014, pp. 1-6.

[8] I. Nai Fovino, A. Coletta, A. Carcano and M. Masera, "Critical State-Based Filtering System for Securing SCADA Network Protocols," in IEEE Transactions on Industrial Electronics, vol. 59, no. 10, pp. 3943-3950, Oct. 2012.

[9] Y. Yang et al., "Multiattribute SCADA-Specific Intrusion Detection System for Power Networks," in IEEE Transactions on Power Delivery, vol. 29, no. 3, pp. 1092-1102, June 2014.

[10] S. Amin, X. Litrico, S. S. Sastry and A. M. Bayen, "Cyber Security of Water SCADA Systems—Part II: Attack Detection Using Enhanced Hydrodynamic Models," in IEEE Transactions on Control Systems Technology, vol. 21, no. 5, pp. 1679-1693, Sept. 2013.

[11] A.N.Fish, Knowledge automation: how to implement decision management in business processes. Wiley, 2012.

[12] D.H.Kang, B.K.Kim, Byoung-Koo Kim, J.C.Na, and K.S.Jhang, Whitelist Generation Technique for Industrial Firewall in SCADA Networks. In Frontier and Innovation in Future Computing and Communications, pp. 525-534. Springer Netherlands, 2014.

[13] G. Dong and G. Kuang, "Target Recognition via Information Aggregation Through Dempster–Shafer's Evidence Theory," in IEEE Geoscience and Remote Sensing Letters, vol. 12, no. 6, pp. 1247-1251, June 2015.