Concept and Research Framework for Coordinated Situation Awareness and Active Defense of Cyber-physical Power Systems Against Cyber-attacks

Ming Ni, Manli Li, Jun'e Li, Yingjun Wu, and Qi Wang

***Abstract*—Due to the tight coupling between the cyber and physical sides of a cyber-physical power system (CPPS), the safe and reliable operation of CPPSs is being increasingly impacted by cyber security. This situation poses a challenge to traditional security defense systems, which considers the threat from only one side, i.e., cyber or physical. To cope with cyber-attacks, this paper reaches beyond the traditional one-side security defense systems and proposes the concept of cyber-physical coordinated situation awareness and active defense to improve the ability of CPPSs. An example of a regional frequency control system is used to show the validness and potential of this concept. Then, the research framework is presented for studying and implementing this concept. Finally, key technologies for cyber-physical coordinated situation awareness and active defense against cyber-attacks are introduced.**

***Index Terms*—Cyber-physical power system (CPPS), cyber security, cyber-attack, situation awareness, active defense.**

I. Introduction

WITH the development of smart grids and Internet of Things, an increasing number of information and communication techniques are being used in power grids, and this situation is driving the transition of traditional power systems into cyber-physical power systems (CPPSs) [1]-[3].

The operation of CPPS depends on the information and communication technologies. Thus, cyber security plays a vital role in ensuring the safe and reliable operation of a CPPS. Although cyber-attacks do not directly damage the physical equipment of the power grid, they can weaken or even completely destroy the normal functioning of physical power system operations, which may finally result in system instability, uneconomic operation and other issues in physical power systems [4]. The 2015 Ukraine blackout is a typical example of cyber-attacks which caused the failure of energy management system (EMS) and, eventually, a blackout [5].

Under the threat of cyber-attacks, it is urgent to improve the capabilities of CPPSs with regard to situation awareness, the identification and trace-back of cyber-attacks, and active defense.

At the cyber side, the identification of cyber-attacks is achieved mainly by two kinds of methods: deviation-based identification methods and feature-based identification methods [6]. The methods based on the distance from the statistical probability distribution [7], the deviation of the control effect [3] and the deviation between the actual and predicted data [4] can be classified as deviation-based identification methods. Feature-based identification methods include those based on features such as data messages, communication rate, signal strength, sequence number, and bit error rate [8]-[12].

The researches on identification at the physical side mainly focus on the methods of identifying bad data and malicious data in the applications of state estimation, i.e., temporal correlation identification methods and spatial correlation identification methods [13]. The main temporal correlation identification method is based on Kalman-filter [14], [15]. Spatial correlation identification is based on the electrical relationships between the measured values of the power system [16].

However, these traditional one-side identification methods are not well suited to cyber-attack scenarios. For example, deliberately constructed malicious data may invalidate traditional identification methods [17]. Nevertheless, the temporal

Manuscript received: November 20, 2018; accepted: October 16, 2019. Date of CrossCheck: October 16, 2019. Date of online publication: June 29, 2020.

This work was supported in part by the National Key Research and Development Program of China (No. 2017YFB0903000) and the Science and Technology Project of the State Grid Corporation of China (Basic Theory and Methodology for Analysis and Control of Grid Cyber Physical Systems (Supporting Projects)).

M. Ni (corresponding author) and M. Li are with the NARI Group Corporation (State Grid Electric Power Research Institute), NARI Technology Co., Ltd., and the State Key Laboratory of Smart Grid Protection and Control, Nanjing 211106, China (e-mail: ni-ming@sgepri.sgcc.com.cn; limanli@sgepri.sgcc.com.cn).

J. Li is with the School of Cyber Science and Engineering, Wuhan University, and the Key Laboratory of Aerospace Information Security and Trusted Computing of the Ministry of Education, Wuhan 430072, China (e-mail: jeli@whu.edu.cn).

Y. Wu is with the College of Energy and Electrical Engineering, Hohai University, Nanjing 211100, China (e-mail: yingjunwu@hotmail.com).

Q. Wang is with the School of Electrical Engineering, Southeast University, Nanjing 210096, China (e-mail: wangqi@seu.edu.cn).

DOI: 10.35833/MPCE.2018.000830

and spatial correlations between the cyber system and the physical system can be utilized to improve the identification performance.

The research on situation awareness of cyber security has yielded promising results in the following aspects: establishment and optimization of situation awareness models [18]-[21]; technologies for gaining a situational sense of the awareness, data fusion, early warning, situational visualization and other key technologies [22], [23]; and cyber security management platforms as well as other engineering applications [24]. By contrast, the research on situation awareness of power system is still immature. At present, it is mainly focused on the concept and framework of situation awareness [25], [26], the security and stability assessment of power system, [27]-[30] and the development of intelligent scheduling systems [31], [32].

Currently, the research on physical-side situation awareness considers only the state awareness of the power grid, and there are no related methods for the evaluation and prediction of grid failures caused by cyber faults or cyber-attacks. At the cyber side, there is a lack of research on the impact for the physical system. Consequently, cyber-side situation awareness methods cannot accurately describe the overall operation situation of the system.

The active defense of cyber systems requires the establishment of a closed-loop, active and multi-layered dynamic security protection model including the protection, detection, reaction, and recovery, i.e., the prevention, detection, and response (PDR) model, and its derived models (P2DR, PDRR, and P2DR2) [33]. The cyber network of the power system in China follows the principles of "secure partitioning, dedicated network, horizontal isolation, and vertical authentication" [34]. Security protection is implemented between secure partitions by deploying passive defense measures such as physical isolation and firewalls. The confidentiality function of the backbone network is realized through encryption and authentication [35]. A deep security protection system for the cyber network is also established based on network isolation and boundary protection.

The traditional defense system for power system security consists of three lines of defense, and plays an irreplaceable role in coping with failures of physical power system [36]. To address the problems of power system security caused by natural disasters [37], [38], the impact of natural environmental phenomena such as lightning and wildfires on the grids is considered in security defense systems of power systems.

At present, cyber security defense systems and power system security defense systems are relatively isolated. The cyber security defense system cannot estimate its impact on its associated physical power system. Similarly, the physical-side security defense system lacks the ability to deal with cyber-attacks.

Thus, the traditional one-side methods of identification, situation awareness, and defense are not sufficient to deal with cyber-attacks on CPPSs. There have been some preliminary studies on the coordination of the cyber and physical sides of such systems. For identification, [39] proposes a cyber-physical fusion approach for cyber-attack detection based on state estimation, which can effectively reduce the false positive and false negative rates. Reference [13] proposes data-based and model-based identification methods for CPPSs. With regard to situation awareness, the current research is mainly focused on security assessment. Reference [1] establishes a CPPS model and proposes a security assessment framework for CPPSs. References [40] and [41] establish a malicious attack model for supervisory control and data acquisition (SCADA), propose a security assessment framework and a quantitative evaluation method, and realize the contingency analysis for CPPSs. These security assessment researches are still preliminary, and the mechanism of cyber-physical interaction is rather simplistic. For coordinated defense, a security defense system [42] is proposed which coordinates "three lines of defense for the communication system" and "three lines of defense for the power system". Consequently, the ability of a CPPS is improved to cope with communication failures. For cyber-attacks, [43] proposes a method of attack and cyber security defense for CPPSs, but it does not coordinate the control measures at both the cyber and physical sides.

This paper proposes the research directions of cyber-physical coordinated situation awareness and active defense, which can improve the ability of a CPPS to cope with cyber-attacks. Section II validates the concept of cyber-physical coordinated situation awareness and active defense through an example of a regional frequency control system. Section III presents the research framework for studying and implementing the concept. Section IV presents key technologies for coordinated situation awareness and active defense. Finally, Section V concludes the paper.

II. Concept of Cyber-physical Coordinated Situation Awareness and Active Defense

The existing cyber-side and physical-side security defense systems are relatively isolated. For cyber-attacks, the main approaches to situation awareness and defense are executed at the cyber side, whereas the physical side has not been actively involved in these efforts. In many circumstances, state information of the physical side of the system can assist in the identification and traceback of cyber-attacks. The measures at the physical side can help prevent or reduce the risk caused by cyber-attacks. Therefore, it is necessary to systematically study a coordinated method of cyber-physical situation awareness and active defense.

A simplified diagram of a regional frequency control system is shown in Fig. 1. The master station collects state information of the power system and the controllable variables of each controllable node, and then sends control commands to the four slave stations after decision-making. The four slave stations send control commands to the DC substations, pump storage units and loads in accordance with the control commands from the master station.

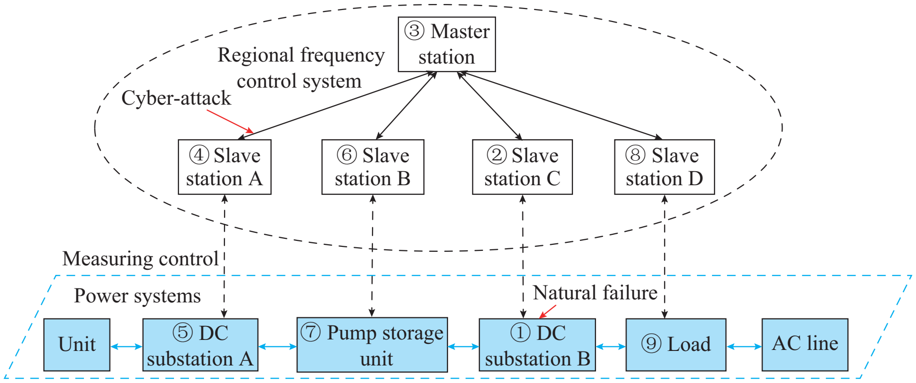

Fig. 1. Cyber-attack on a regional frequency control system.

A. Coordinated Identification and Trace-back of Cyber-attacks

The cyber-attack scenario is considered as follows: DC substation B is blocked, and slave station A is targeted by a cyber-attack, as shown in Fig. 1. The cyber-attack tampers with the control command sent from the master station to slave station A, which will cause the malfunction of DC substation A.

In this scenario, based on the information at the cyber side, slave station A cannot judge whether the received control signal has been tampered. However, it can identify the authenticity of the control signal by means of the temporal and spatial correlations between cyber events (i. e., primary equipment failure, load switching, DC adjustment) and physical events (i.e., failure identification, command transmission and reception, and device actions). The cyber and physical events in the system after a failure at the physical side and/or a cyber-attack show significant temporal and spatial correlations. Therefore, these cyber and physical events can be combined into a complete cyber-physical event chain in accordance with the specific logic of the scenario, which can be used to identify whether the system is suffering a cyber-attack.

In this scenario, after the blocking of DC substation B, to keep the frequency of the system within the specified limit, the control strategies include adjusting DC substation A, cutting the pump storage unit, and shedding the load. The whole process is described as follows:

1) Physical events: DC substation B ① fails; then, DC substation A ⑤ is adjusted; and the pump storage unit ⑦ and load ⑨ are cut in accordance with signals from their slave stations.

2) Cyber events: slave station C ② judges that DC substation B has failed based on the measured electrical quantities. Slave station C is activated. It calculates the amount of power lost in DC substation B and sends all information to the master station ③. The master station is activated. It determines the control strategy and sends control signals to slave stations A ④, B ⑥, and D ⑧. Slave stations A, B, and D act in accordance with the received control signals.

The cyber and physical events in the above scenario exhibit temporal and spatial correlations. Among them, the temporal correlations are relationships with the timing of event occurrence. For example, the master station must firstly send a command before slave station A receives it. If slave station A receives a command when the master station has not sent a command, yet it can be determined that slave station A has received a tampered command. The spatial correlations in this example are related to electrical connections. For example, if DC substation B is blocked, the quantity of electricity at DC substation A will also change. Thus, based on the temporal and spatial correlations between cyber and physical events, a cyber-physical event chain can be formed.

In this example, the cyber-physical event chain for the blocking failure of DC substation B is ①→②→③→④→⑤ (③→⑥→⑦, ③→⑧→⑨), while the cyber-physical event chain for a cyber-attack is ④→⑤. Based on the difference between these two cyber-physical event chains, a cyber-attack can be identified, and the propagation path and attack source can be traced. In this example, through the comparison of the chains, an attack at ④ can be identified.

B. Coordinated Defense

In the sample system, the original control logic of slave station A is as follows: it receives a command from the master station and then sends a command to DC substation A. If there is no blocking failure at DC substation B, slave station A should not issue a control command to adjust DC substation A. However, if the command to DC substation A has been tampered with due to an attack and slave station A cannot identify the attack, it will adjust DC substation A, which is unexpected.

Using the proposed concept of cyber-physical coordinated defense, the above-mentioned problem can be solved. This defense approach can guarantee that the slave station will not respond to the tampered control commands. At the same time, in accordance with the trace-back result, CPPS will activate the attack blocking strategy at the cyber side and notify the operation and maintenance personnel to address the source of the attack.

Under this circumstance, to implement the coordinated defense strategy, the action logic of slave station A is changed. If an action command is received by slave station A (cyber side), and at the same time, the electrical quantities measured at slave station A are consistent with the electrical characteristics expected in the case of primary equipment failure (physical side), slave station A will send the corresponding command to DC substation A. With this defense method, if the electrical quantities measured at slave station A are not changed, which indicates that there's no failure at the physical side, slave station A will not issue an action command to adjust DC substation A even if it receives an action command from the master station.

III. Framework for Cyber-physical Coordinated Situation Awareness and Active Defense

The cyber security defense system, including four phases of prediction, defense, detection and response [33], and the physical power security defense system are defined from the perspectives of pre-event, in-progress, and post-event. This serves as the theoretical basis of the cyber-physical coordinated defense system. Therefore, many problems need to be solved such as the interaction mechanism between the cyber and physical sides, and the coordinated modeling and integrated analysis of the cyber and physical sides. The proposed research framework for cyber-physical coordinated situation awareness and active defense is shown in Fig. 2, which consists of four components.

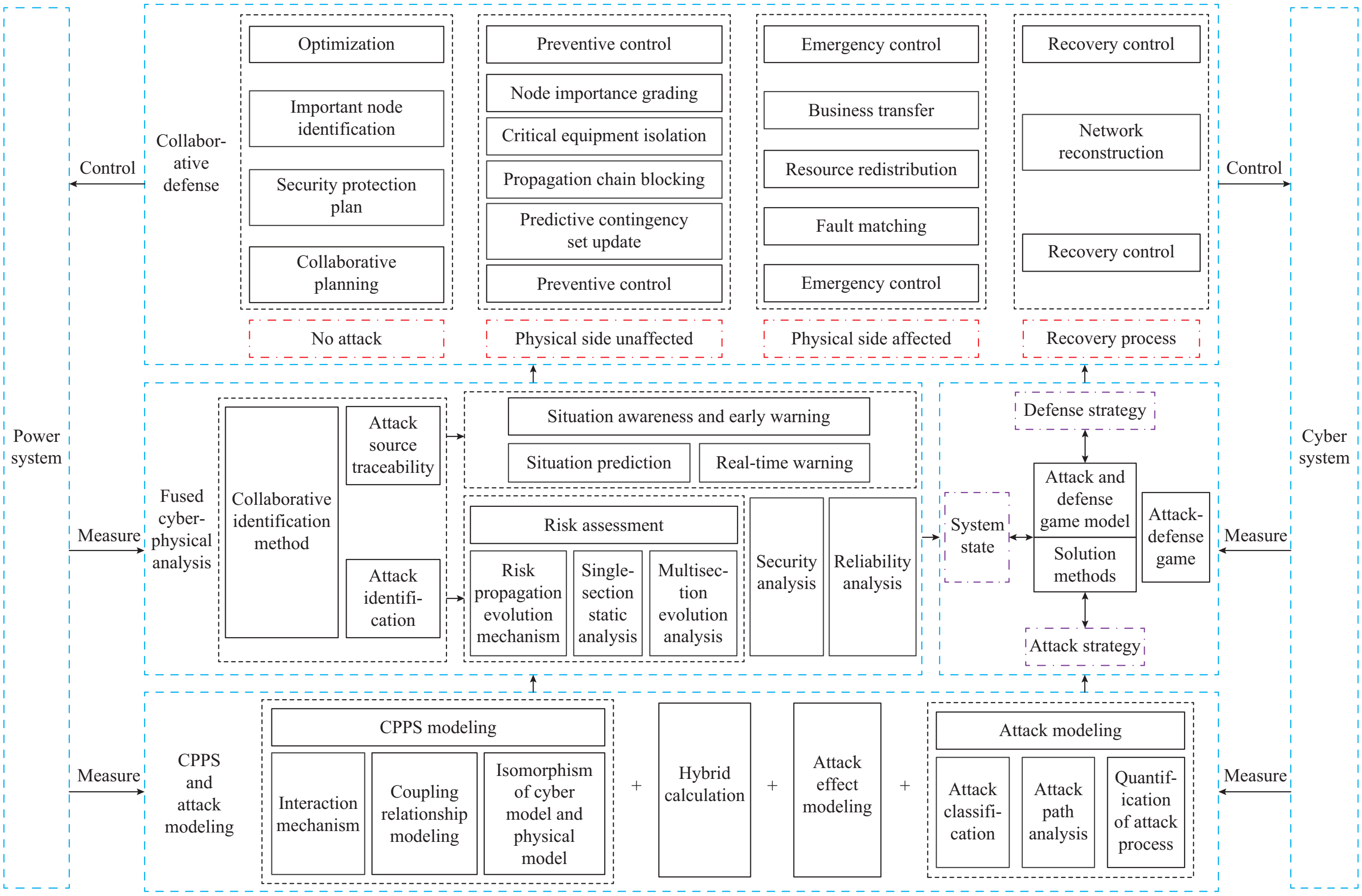

Fig. 2. Research framework for cyber-physical coordinated situation awareness and active defense.

1) CPPS model and attack model. This component considers the impact of attack behavior for each attacker, reveals the interaction mechanism between the cyber and physical sides, establishes the coordinated model of the cyber-physical system, and enables the combined calculation of the cyber-physical coordinated model.

2) Fused cyber-physical analysis. This component includes the cyber-physical coordinated identification methods, security, reliability and risk analysis methods, and coordinated situation awareness methods.

3) Cyber-physical coordinated active defense. This component extends the three lines of defense for the power system to the cyber system, establishes a four-stage coordinated defense framework, realizes cyber-physical coordinated defense, and improves the ability of CPPS to cope with cyber-attacks.

4) Attack and defense game. The nature of attack and defense confrontations can be abstracted to reflect the strategic dependence between offense and defense. By considering the system state and defense strategies of the attacker, a game model needs to be established to generate new ideas for solving cyber-attack problems.

IV. Key Technologies for Cyber-physical Coordinated Situation Awareness and Active Defense

The traditional methods of identification, trace-back and defense against cyber-attacks are based only on state information from either the physical side or cyber side. Thus, they neglect the temporal and spatial correlations between the states at physical and cyber sides. Therefore, it is difficult to accurately predict and generate warnings regarding the operation trends of CPPSs, trace the sources and paths of cyber-attacks, and coordinate the control measures at both sides.

By combining the characteristics of both the cyber and physical sides, an interactive-check-based situation awareness scheme and a coordinated-control-based cyber-attack defense scheme can be developed to effectively improve the ability of a CPPS to defend against cyber-attacks.

A. Coordinated Situation Awareness and Traceback of Cyber-attacks

An overview of the coordinated situation awareness and trace-back technology based on interactive checks between the cyber and physical sides is shown in Fig. 3.

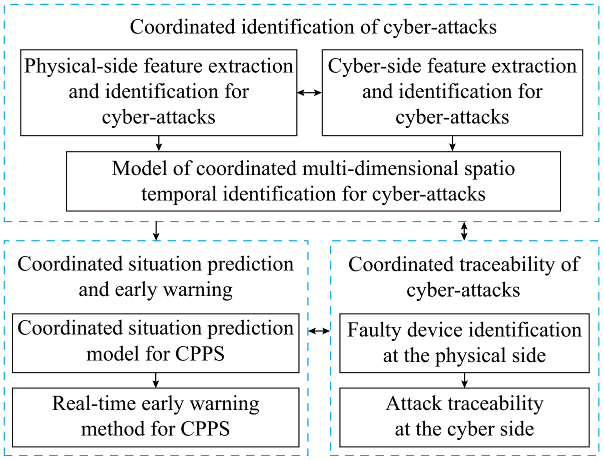
Coordinated identification of cyber-attacks
Physical-side feature extraction and identification for cyber-attacks
Cyber-side feature extraction and identification for cyber-attacks
Model of coordinated multi-dimensional spatio temporal identification for cyber-attacks
Coordinated situation prediction and early warning
Coordinated situation prediction model for CPPS
Real-time early warning method for CPPS
Coordinated traceability of cyber-attacks
Faulty device identification at the physical side
Attack traceability at the cyber side

Fig. 3. Coordinated situation awareness and trace-back of cyber-attacks.

1) Coordinated Identification of Cyber-attacks

Firstly, the method for extracting the characteristics of cyber-attacks and identifying cyber-attacks at cyber and physical sides are studied individually, along with their shortcomings. Then, the coordinated scheme for identifying cyber-attacks through interactive checks of state information at both the cyber and physical sides is addressed.

1) Characteristic extraction and identification at physical side

A time-series representation method combining the discrete Fourier transform and discrete wavelet transform approaches can be used to represent the time-series data of the operation states of the power system. Then, cluster analysis can be performed on the resulting sequence to extract the correlation characteristics of the data in the normal state under cyber-attack. Next, the critical electrical nodes under cyber-attack should be identified. Starting from two existing identification methods at the physical side, i.e., grid-topology-based method and electrical-characteristic-based method, the correlations between key electrical quantities will be analyzed. The temporal and spatial correlations of the data will then be used to establish a method for cyber-attack identification at the physical side.

2) Characteristic extraction and identification at cyber side

A time-series analysis can be performed based on information such as the logical topology of the network, network traffic, and network performance, and then cluster analysis is used to extract the characteristics of time-series of the cyber-side data under cyber-attack. Since a hidden Markov model can effectively describe the characteristics of the process in which the network security state changes, a hidden Markov data fusion model will be constructed. Comparing the processes with state changes of network security under cyber-attack and normal operation obtained from the constructed model, the abnormal cyber-side characteristics induced by a cyber-attack can be extracted.

3) Coordinated identification

Based on the cyber-attack characteristics extracted from both the physical and cyber sides, combined with an attack propagation model and an intrusion detection model, a multivariable time-series model for coordinated cyber-attack identification can be established. Based on a combination of misuse detection and anomaly detection, the attack behavior can be identified.

2) Coordinated Situation Prediction and Early Warning

1) Coordinated situation prediction

Firstly, a value representing the security situation of CPPS is extracted. Then, in combination with historical data, this value will be used to predict the security situation of CPPS via the gray prediction method, autoregressive (AR) prediction, and neural network prediction of radial basis function (RBF). A correlation analysis between the predicted and actual values will be performed to establish weight values for the three prediction methods, and the prediction results are then used in accordance with these weights to obtain the results of situation prediction.

2) Coordinated early warning

Based on the behavior model of CPPS attack, various abnormal states caused by attacks and their impacts on the physical power grid are analyzed, and early warning criteria can be formulated in combination with the early warning requirements for the power grid. By combining the interaction interface between the physical and cyber spaces with the state monitoring information of key locations, a coordinated early warning approach for both the physical and cyber sides can be established.

3) Coordinated Trace-back of Cyber-attacks

Firstly, the traceability of abnormal devices at the physical side is considered. Then, from the information obtained from cyber device directly associated with the abnormal power equipment, the attack host can be traced by means of attack source tracing at the cyber side.

1) Traceability of abnormal devices at physical side

Abnormal power devices can be identified based on the network topology and an algorithm of network fault localization combined with the regional positioning at the physical side.

2) Trace-back of attacks at cyber side

A technology integrating IP tracking, media access layer (MAC) layer tracking and device fingerprint identification can be used to trace the attack source. IP tracking is a hybrid trace-back model combining packet tracing and packet log tracing. It can be used to determine the locations of wide-area attack paths and devices with fixed IP addresses. MAC layer tracking combines the technologies of path switching and MAC address to localize devices with no fixed IP addresses or IP protocols. It can also be used as an auxiliary means of IP tracking to defend against IP forgery. Device fingerprint identification technology is used to defend against IP or/and MAC forgery and to ultimately locate the attack source.

B. Coordinated Active Defense Against Cyber-attacks

An overview of the technology for coordinated active defense against cyber-attacks at both sides is shown in Fig. 4.

1) Defense at Cyber Side

The traditional defense strategies at the cyber side include security countermeasure configuration, cyber-attack blocking, propagation chain blocking under cyber-attack and allocation of dynamic cyber resource. However, propagation chain blocking under cyber-attack depends on the security countermeasure configuration and allocation of dynamic cyber resource. Therefore, the decision-making for these defense strategies should be based on mutual coordination.

For example, traditional strategies of security countermeasure configuration and allocation of dynamic cyber resource are determined based only on the impact of cyber component failure at the cyber side and the importance of cyber services. However, in a coordinated environment, these strategies should consider the risk at both the cyber and physical sides as well as the importance of the power system functions supported by the cyber services.

2) Defense at Physical Side

In traditional physical power systems, defense is implemented on three different time scales, i.e., resource allocation, preventive control and emergency control. Accordingly, it is necessary to investigate optimal configuration strategies in allocating resources for either reserves or rapid demand response; the correction of real-time control; the self-generation of a combined contingency set; and alternative control strategies considering the impact of cyber-attacks at the physical side.

For example, traditional emergency control addresses only the failure of primary equipment. However, in a coordinated environment, equipment failures at both the physical and cyber sides need to be considered, thus a combined contingency, i.e., physical contingency plus cyber contingency set, needs to be identified. Moreover, the impact of cyber failure on the availability and effectiveness of traditional control strategies needs to be considered for comparing the control strategies.

3) Coordinated Active Defense Framework

Based on the traditional three-line defense concept of power system and the mechanism of cyber-attack cross-propagation between the cyber and physical sides, a multi-timescale multi-line cooperative active defense technology can be established as shown in Fig. 5.

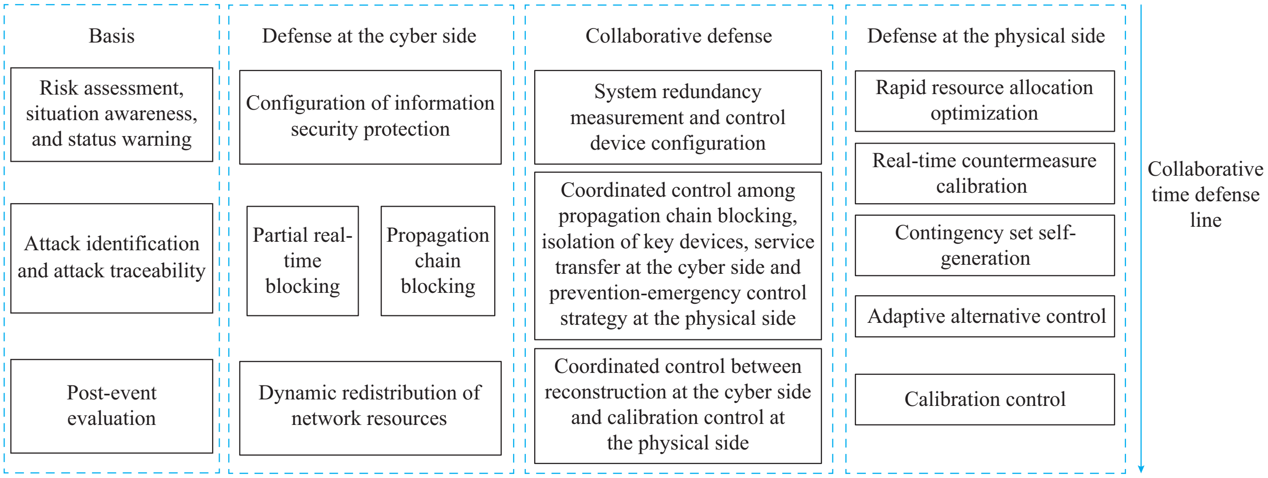
Basis
Risk assessment, situation awareness, and status warning
Attack identification and attack traceability
Post-event evaluation
Defense at the cyber side
Configuration of information security protection
Partial real-time blocking
Propagation chain blocking
Dynamic redistribution of network resources
Collaborative defense
System redundancy measurement and control device configuration
Coordinated control among propagation chain blocking, isolation of key devices, service transfer at the cyber side and prevention-emergency control strategy at the physical side
Coordinated control between reconstruction at the cyber side and calibration control at the physical side
Defense at the physical side
Rapid resource allocation optimization
Real-time countermeasure calibration
Contingency set self-generation
Adaptive alternative control
Calibration control
Collaborative time defense line

Fig. 4. Coordinated active defense against cyber-attacks between the cyber and physical sides.

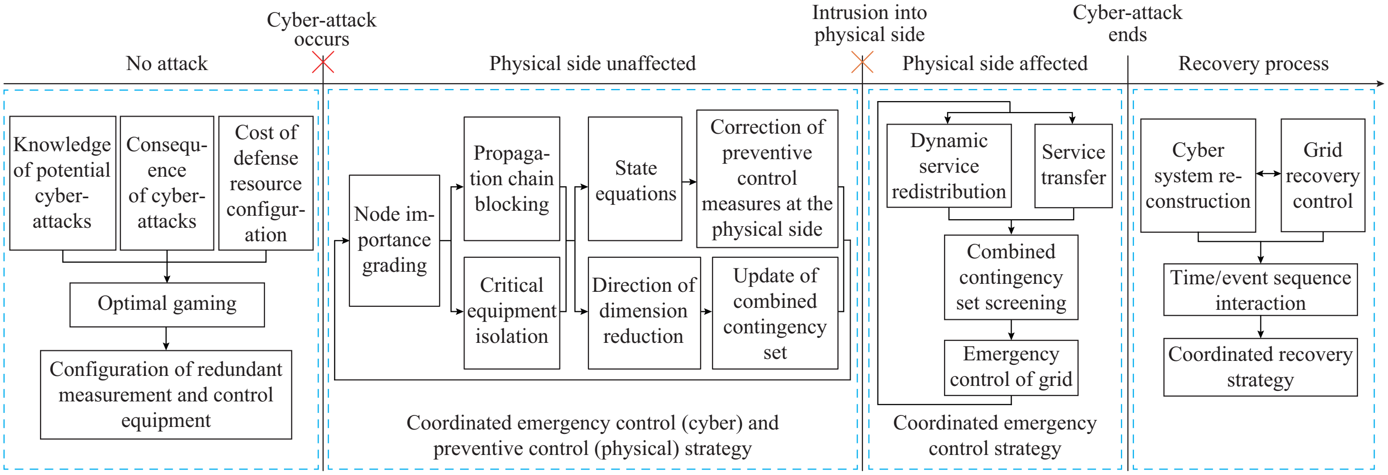
Cyber-attack occurs
Intrusion into physical side
Cyber-attack ends
No attack
Physical side unaffected
Physical side affected
Recovery process
Knowledge of potential cyber-attacks
Consequence of cyber-attacks
Cost of defense resource configuration
Optimal gaming
Configuration of redundant measurement and control equipment
Node importance grading
Propagation chain blocking
Critical equipment isolation
State equations
Direction of dimension reduction
Correction of preventive control measures at the physical side
Update of combined contingency set
Coordinated emergency control (cyber) and preventive control (physical) strategy
Dynamic service redistribution
Service transfer
Combined contingency set screening
Emergency control of grid
Coordinated emergency control strategy
Cyber system reconstruction
Grid recovery control
Time/event sequence interaction
Coordinated recovery strategy

Fig. 5. Multi-timescale multi-line cooperative active defense.

Based on the progression over time, the cyber-attack process is divided into four phases: ① phase 1: no cyber-attack; ② phase 2: physical side unaffected; ③ phase 3: physical side affected; and ④ phase 4: recovery process. For each of four phases, the interaction and coordination mechanisms between the means of defense at the cyber and physical sides need to be studied in terms of both time series and the event sequence.

1) Phase 1

Based on the possible anticipated cyber-attacks, before a cyber-attack occurs, their potential impacts at both the cyber and physical sides can be investigated. The cost of the corresponding defense resources, i. e., communication, measurement, control, and optimal gaming approach can be applied at the cyber side to determine the optimal configuration strategy for these resources.

2) Phase 2

After an attack occurs and before its impact propagates to the physical side, it is necessary to coordinate the emergency control strategy at the cyber side and the preventive control strategy at the physical side. On one hand, when performing the blocking of attack propagation chain and the allocation of dynamic cyber resource, the impacts of the attack at the physical side should be considered, along with critical functions supported by cyber services at the physical side. On the other hand, physical-side preventive control strategies need to be calculated with consideration of potential impacts of the attack at the physical side and the availability and effectiveness of the control measures at the physical side.

3) Phase 3

Once the impact of the cyber-attack has propagated to the physical side, the grid is substantially affected, and emergency control measures at the physical side are initiated. Therefore, the emergency control strategies at both sides need to be coordinated. On one hand, the implementation of emergency control at the physical side is used as an input for decision-making. It considers cyber service transfer and dynamic resource redistribution at the cyber side, and the propagation restriction strategy at the cyber side should minimize further spread of the attack at the physical side. On the other hand, the decision-making at the physical side should consider failures at both sides. Furthermore, if possible, the decision-making regarding the emergency control strategies at both sides should be implemented as a single optimization problem.

4) Phase 4

In the recovery phase, it is necessary to coordinate the reconstruction procedure in the cyber system and the recovery control strategy in the power system to quickly restore the normal operation of the CPPS. Considering the recovery control requirements for the power system, the optimal reconstruction strategy for cyber system must be based on the criticality of the nodes and functions of power system during recovery.

V. Conclusion

The tight coupling between the cyber side and the physical side in a CPPS poses a challenge to the security of the power system, but it also provides opportunities to coordinate both the cyber and physical sides to enhance power system security. This paper attempts to overcome the limitations of the traditional one-side methods by proposing a concept of cyber-physical coordinated situation awareness and active defense against cyber-attacks based on the temporal and spatial correlations between the cyber and physical sides. A regional frequency control system is used as an example to validate the effectiveness and potential of the concept. The overall theoretical architecture and the key technologies are presented.

To fully implement the coordination between the cyber and physical sides to reap the corresponding benefits, the advancements in the following areas will be critical: CPPS and cyber-attack modeling, analysis of CPPS security and risk analysis considering malicious attacks, and CPPS control theory.

As the extension of this paper, the concept of cyber-physical coordination can be further explored in other areas such as optimal control and planning for CPPSs. For example, the planning at both cyber and physical sides is currently performed by different entities. However, due to the close interaction between these two sides of smart grids, the two sides need to be designed in a coordinated manner to achieve an economic and reliable planning for CPPSs.

References

[1] Q. Guo, S. Xin, H. Sun *et al.*, “Power system cyber-physical modelling and security assessment: motivation and ideas,” *Proceeding of the CSEE*, vol. 36, no. 6, pp. 1481-1489, Mar. 2016.

[2] D. Liu, W. Sheng, Y. Wang *et al.*, “Key technologies and trends of cyber physical system for power grid,” *Proceeding of the CSEE*, vol. 35, no. 14, pp. 3522-3531, Jul. 2015.

[3] K. D. Kim and P. R. Kumar, “Cyber-physical systems: a perspective at the centennial,” *Proceedings of the IEEE*, vol. 100, pp. 1287-1308, May 2012.

[4] Y. Tang, Q. Chen, M. Li *et al.*, “Overview on cyber-attacks against cyber physical power system,” *Automation of Electric Power Systems*, vol. 40, no. 17, pp. 59-69, Sept. 2016.

[5] Q. Guo, S. Xin, J. Wang *et al.*, “Comprehensive security assessment for a cyber physical energy system: a lesson from Ukraine’s blackout,” *Automation of Electric Power Systems*, vol. 40, no. 5, pp. 145-147, Mar. 2016.

[6] Y. Tang, M. Li, Q. Wang *et al.*, “A review on research of cyber-attacks and defense in cyber physical power systems part two detection and protection,” *Automation of Electric Power Systems*, vol. 43, no. 10, pp. 1-9, May 2019.

[7] O. Salem, F. Nait-Abdesselam, and A. Mehaoua. “Anomaly detection in network traffic using Jensen-Shannon divergence,” in *Proceedings of IEEE International Conference on Communications*, Ottawa, Canada, Jun. 2012, pp. 5200-5204.

[8] L. Hui, A. Slagell, Z. T. Kalbarczyk *et al.*, “Runtime semantic security analysis to detect and mitigate control-related attacks in power grids,” *IEEE Transactions on Smart Grid*, vol. 9, no. 1, pp. 163-178, Jan. 2018.

[9] S. Sridhar and M. Govindarasu, “Model-based attack detection and mitigation for automatic generation control,” *IEEE Transactions on Smart Grid*, vol. 5, no. 2, pp. 580-591, Mar. 2014.

[10] R. Samdarshi, N. Sinha, and P. Tripathi, “A triple layer intrusion detection system for SCADA security of electric utility,” in *Proceedings of 12th IEEE International Conference Electronics, Energy, Environment, Communication, Computer, Control*, New Delhi, India, Dec. 2015, pp. 1-5.

[11] Y. J. Kwon, H. K. Kim, H. L. Yong *et al.*, “A behavior-based intrusion detection technique for smart grid infrastructure,” in *Proceedings of 2015 IEEE Eindhoven PowerTech*, Eindhoven, Netherlands, Jun.

2015, pp. 1-6.

[12] S. Wu, C. Liu, and A. Stefanov, "Distributed specification-based firewalls for power grid substations," in *Proceedings of IEEE PES Innovative Smart Grid Technologies Conference Europe*, Istanbul, Turkey, Oct. 2014, pp. 1-6.

[13] T. Liu, J. Tian, J. Wang *et al*., "Integrated security threats and defense of cyber-physical systems," *Acta Automatica Sinica*, vol. 45, no. 1, pp. 5-24, Jan. 2019.

[14] D. B. Rawat and C. Bajracharya, "Detection of false data injection attacks in smart grid communication systems," *IEEE Signal Processing Letters*, vol. 22, no. 10, pp. 1652-1656, Oct. 2015.

[15] S. Lakshminarayana, Z. T. Teo, D. Yau *et al*., "Optimal attack against cyber-physical control systems with reactive attack mitigation," in *Proceedings of 8th ACM International Conference on Future Energy Systems*, Boston, USA, May 2017, pp. 179-190.

[16] G. Liang, S. R. Weller, J. Zhao *et al*., "The 2015 Ukraine blackout: implications for false data injection attacks," *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3317-3318, Jul. 2017.

[17] M. Tian, X. Wang, Z. Dong *et al*., "Injected attack strategy for false data based on lagrange multipliers method," *Automation of Electric Power Systems*, vol. 41, no. 11, pp. 26-32, Jun. 2017.

[18] P. Xiao, M. Xian, and H. Wang, "Network security situation prediction method based on MEA-BP," in *Proceedings of 2017 3rd International Conference on Computational Intelligence & Communication Technology (CICT)*, Ghaziabad, India, Feb. 2017, pp. 1-5.

[19] X. Li and H. Zhao, "Network security situation assessment based on HMM-MPGA," *in Proceedings of 2016 2nd International Conference on Information Management (ICIM)*, London, UK, May 2016, pp. 57-63.

[20] J. Li, M. Cheng, J. Ni *et al*., "Research on the aggregation model of network security situation awareness based on analytic hierarchy process," in *Proceedings of 4th International Conference on Intelligent Systems Design and Engineering Applications*, Zhangjiajie, China, Nov. 2013, pp. 519-522.

[21] C. Li and X. Li, "Cyber performance situation awareness on fuzzy correlation analysis," in *Proceedings of 3rd IEEE International Conference on Computer and Communications*, Chengdu, China, Dec. 2017, pp. 424-428.

[22] A. Ju, Y. Guo, and T. Zhu, "Framework for big data network security situational awareness and threat warning based on open source toolset," *Computer Science*, vol. 44, no. 5, pp. 125-131, May 2017.

[23] J. Gong, X. Zang, Q. Su *et al*., "Survey of network security situation awareness," *Journal of Software*, vol. 28, no. 4, pp. 1010-1026, Nov. 2017.

[24] J. Liu, J. Liu, Y. Lu *et al*., "Application of game theory in network security situation awareness," *Computer Science*, vol. 37, no. S2, pp. 48-51, Dec. 2017.

[25] J. Zhang, H. Chen, J. Chen *et al*., "Smart grid situation awareness diagram modeling and conceptual design of situation awareness visualization," *Automation of Electric Power Systems*, vol. 38, no. 9, pp. 168-176, May 2014.

[26] J. Lin, C. Wan, Y. Song *et al*., "Situation awareness of active distribution network: roadmap, technologies, and bottlenecks," *CSEE Journal of Power & Energy Systems*, vol. 2, no. 3, pp. 35-42, Sept. 2016.

[27] H. Li, Z. Liu, and J. Song, "Real-time static security situational awareness of power systems based on relevance vector machine," *Proceedings of the CSEE*, vol. 35, no. 2, pp. 294-301, Jan. 2015.

[28] Y. Feng, Z. Yun, J. Sun *et al*., "Fast situation awareness method for distribution network coordinated with transmission grid," *Automation of Electric Power Systems*, vol. 40, no. 12, pp. 37-44, Jun. 2016.

[29] C. Basu, M. Padmanaban, S. Guillon *et al*., "Situational awareness for the electrical power grid," *IBM Journal of Research and Development*, vol. 60, no. 1, pp. 1-11, Jan. 2016.

[30] W. Zhang, S. Fu, Y. Diao *et al*., "A situation awareness and early warning method for voltage instability risk," in *Proceedings of China International Conference on Electricity Distribution*, Tianjin, China, Sept. 2018, pp. 1010-1014.

[31] S. Yang, B. Tang, J. Yao *et al*., "Architecture and key technologies for situational awareness based automatic intelligent dispatching of power grid," *Power System Technology*, vol. 38, no. 1, pp. 33-39, Jan. 2014.

[32] X. Wang, N. Chen, Y. Li *et al*., "Multi-source optimal dispatch architecture for active distribution network based on situational linkage," *Power System Technology*, vol. 41, no. 2, pp. 349-354, Feb. 2017.

[33] K. Wu, T. Zhang, and F. Chen, "Research on active controllable defense model based on zero-PDR model," in *Proceedings of Third International Symposium on Intelligent Information Technology and Security Informatics*, Jinggangshan, China, Apr. 2010, pp. 572-575.

[34] *State Electricity Regulatory Commission Regulations on Safety Protection of Secondary Power System*, The Bulletin of the State Council of the People's Republic of China, 2005.

[35] C. Zou, Z. Zheng, Z. Liu *et al*., "Application of cyber security in industrial control systems based on security protection technology for electrical secondary system," *Power System Technology*, vol. 37, no. 11, pp. 3227-3232, Nov. 2013.

[36] *Technical Guidelines for Power System Security and Stability Control*, Standards Press of China GB/T 26399—2011, 2011.

[37] X. Jin, T. Chen, G. Zou *et al*., "Application of power grid security and stability intelligent defense system self-adapting the external environment," *Power System Protection and Control*, vol. 43, no. 23, pp. 137-142, Dec. 2015.

[38] J. Luo, C. Yu, Y. Xie *et al*., "A review on risk assessment of power grid security and stability under natural disasters," *Power System Protection and Control*, vol. 46, no. 6, pp. 158-170, Mar. 2018.

[39] T. Liu, Y. Sun, Y. Liu *et al*., "Abnormal traffic-indexed state estimation: a cyber-physical fusion approach for smart grid attack detection," *Future Generation Computer Systems*, vol. 49, pp. 94-103, Aug. 2015.

[40] S. Zonouz, C. M. Davis, K. R. Davis *et al*., "SOCCA: a security-oriented cyber-physical contingency analysis in power infrastructures," *IEEE Transactions on Smart Grid*, vol. 5, no. 1, pp. 3-13, Jan. 2014.

[41] C. Vellaithurai, A. Srivastava, S. Zonouz *et al*., "CPIndex: cyber-physical vulnerability assessment for power-grid infrastructures," *IEEE Transactions on Smart Grid*, vol. 6, no. 2, pp. 566-575, Mar. 2015.

[42] Y. Xue, M. Ni, W. Yu *et al*., "Power grid blackout defense system including communication information security early warning and decision support," *Automation of Electric Power Systems*, vol. 40, no. 17, pp. 3-12, Sept. 2016.

[43] T. Li, S. Su, H. Yang *et al*., "Attacks and cyber security defense in cyber-physical power system," *Automation of Electric Power Systems*, vol. 41, no. 22, pp. 162-167, Nov. 2017.

Ming Ni received the B.S. and M.S. degrees in electrical engineering from Southeast University, Nanjing, China, in 1991 and 1996, respectively. He is currently the Chief Expert of Power System Analysis and Planning at NARI Technology Co., Ltd., Nanjing, China. His current research interests include CPPSs, stability analysis and the control of power systems.

Manli Li received the B.S. and M.S. degrees from Nanjing University of Posts and Telecommunications, Nanjing, China, in 2012 and 2015, respectively. He is currently an Engineer with NARI Technology Co., Ltd., Nanjing, China. His primary research interests include CPPSs, stability analysis and control of power systems.

Jun'e Li received the Ph.D. degree from Wuhan University, Wuhan, China, in 2004. She is currently a Professor with the School of Cyber Science and Engineering, Wuhan University, Wuhan, China. Her current research interests include CPPSs, cyber security and power industrial control security.

Yingjun Wu received the Ph.D. degree in electrical engineering from the Politecnico di Torino, Torino, Italy, in 2013. He is currently an Associate Professor with the College of Energy and Electrical Engineering, Hohai University, Nanjing, China. His current research interests include CPPSs and smart distribution systems.

Qi Wang received the Ph.D. degree from Southeast University, Nanjing, China, in 2017. He is currently a Lecturer with the School of Electrical Engineering, Southeast University, Nanjing, China. His research interests include cyber physical system, power system stability analysis and power system security.