Management Solutions for Cyber-Physical Security in Smart Built Environment

Ping Xu[1]; Xinghua Gao, Ph.D.[2]; and Philip Agee, Ph.D.[3]

[1]Myers-Lawson School of Construction, Virginia Polytechnic Institute and State Univ. Email: pingxu90@vt.edu
[2]Myers-Lawson School of Construction, Virginia Polytechnic Institute and State Univ. (corresponding author). Email: xinghua@vt.edu
[3]School of Building Construction, Virginia Center for Housing Research, Virginia Polytechnic Institute and State Univ. Email: pragee@vt.edu

ABSTRACT

Cybersecurity risks, together with the associated physical security risks, are hindering the advancement of smart building innovations and applications. The cyber-physical (CP) security for smart built environments is an emerging, critical challenge that cannot be addressed solely by existing cybersecurity means nor traditional physical security means. Currently, because of rapid developments in smart building-related technologies, such as the Internet of Things (IoT), Cyber-physical Systems, and Artificial Intelligence (AI), researchers and industry professionals need a state-of-the-art overview of the solutions for CP security threats in smart built environments. Through a systematic literature review, this paper summarizes and discusses existing management means and methods to achieve more secured built environments. The content analysis results show that most research studies are in the area of smart grids and power systems' CP security, with focuses such as intrusion detection, cyberattack impact mitigation, system status monitoring, and system resilience improvement. The existing gaps of built-environment CP security research include human factors, coordinated attacks, preventive solutions, and the interactions between cybersecurity and physical security.

KEYWORDS: cyber-physical (CP) security, cybersecurity, smart built environments, critical infrastructure, cyberattack mitigation

INTRODUCTION

The built environment is defined as "the human-made space in which people live, work, and recreate on a day-to-day basis" (Roof and Oleru 2008). In recent two decades, with the popularization of innovative sensing, processing, and actuation (SPA) systems enabled by IoT and AI, the built environment is evolving to the envisioned smart built environment. The increased level of automation is also brings new challenges in the built environment's CP security, which is an emerging and critical challenge that cannot be addressed solely by existing cybersecurity means nor traditional physical security means (Weerakkody and Sinopoli 2019). The issues of CP security for smart built environments involve not only the cyber threats to the information systems but also the imposed physical threats to buildings and infrastructures (Clark and Hakim 2017). If used independently, many of the existing cybersecurity methods and physical security methods are not sufficient to prevent nor mitigate CP attacks (Agarwal 2021). For example, a new cyberattack that utilizing laser and voice-controllable systems (Amazon's Alexa, Apple's Siri, and Google Assistant) can obtain control of a home's physical obstructions,

such as garage doors (Sugawara et al. 2020). Therefore, a literature review on the current solutions for improving CP security for the smart built environment is in need to provide the research community and the industry an overall picture of the current developments and to identify research gaps for future research in this field.

This research summarizes and discusses management means and methods to mitigate cyberattacks in smart built environments. The scope of this research includes the academic publications on CP security for smart built environments, published within this decade. The authors have reviewed and summarized the research studies on the solutions for CP security in the built environment from a management perspective. Research gaps are also identified and suggested future directions discussed.

REVIEW APPROACH

This paper involves a literature review on publications that focus on CP security in the smart built environment. To identify related publications, a keyword search is performed on the Web of Science. Articles with the keywords "cyber-physical security", "cyber physical security", "infrastructure", "grid", "bridge", and "smart building" are identified and reviewed. 67 publications are reviewed – 61 journal articles and six book chapters. Each reviewed paper is examined in the following aspects: 1) the CP attack model, 2) the type of facility and the system that are under attack, 3) the means and methods used to achieve a more secured built environment, and 4) whether the human factor is considered.

About 84% of the reviewed articles (56 publications) have discussed the CP security of smart grids and power systems. In these 56 publications, most papers focus on the CP attacks on smart micro-grids, substations, and smart meters. Other than the 56 papers, five papers have studied the CP security of the critical infrastructure. Another five discussed the CP security of the cyber-physical system (CPS) applied in buildings. Two of them focus on the industrial control system, and one focuses on the additive manufacturing system. There is one paper discussing the CP security of the smart-world system. In the reviewed papers, three papers have discussed the importance of the human factor for CP security of smart built environments.

MANAGEMENT SOLUTIONS FOR CP SECURITY

The authors have reviewed and summarized the research studies on the solutions for CP security in the built environment from a management perspective. The studies are categorized into six major groups: 1) increasing human awareness, 2) intelligently detecting intrusions, 3) improving system resilience, 4) optimizing attack mitigation strategy, 5) real-time monitoring system status and assessing system vulnerability, and 6) modeling and simulating attack and defense. The major studies reviewed and discussed are summarized in Table 1.

Increasing human awareness for CP security

The human factor is a major source of CP security threats to critical infrastructures (Symantec Corporation 2014). Malicious insiders may utilize their knowledge and access of the control system to attack the electric power infrastructure (Weerakkody and Sinopoli 2019). Weerakkody and Sinopoli (2019) have suggested that human factors should not be underestimated and special care should be taken when permissions to employees are granted.

Table 1. The major research studies reviewed and discussed

Management solutions	Study	Summary
Increasing human awareness	Backhaus et al. (2013) Caviglione et al. (2015) Clark and Hakim (2017) Jiow (2017) Weerakkody and Sinopoli (2019)	Improving the CP security of the facilities and their systems with the human factor considered.
Intelligently detecting intrusions	Čeleda et al. (2012) Krejčí et al. (2012) Lo and Ansari (2013) Zhang et al. (2020)	Proposing intrusion detection approaches with different data sources such as data flow in the building system, sensor and meter reading, and time-series signals.
Improving system resilience	Venkataramanan et al. (2020) Zhu (2019) Zonouz et al. (2014)	Improving system resilience by methods such as creating assessment metrics, proposing layered control systems for the smart grid, and providing predictive capabilities of situational awareness to the power grid security officers.
Optimizing attack mitigation strategy	Ashok et al. (2017) Bretas et al. (2017) Hong et al. (2019) Weerakkody and Sinopoli (2019)	Proposing mitigation methods by methods such as creating a framework to address the security issues of the facility lifecycle, and modeling cyberattacks and defense.
Real-time monitoring system status and assessing system vulnerability	Stefanov et al. (2015) Srivastava et al. (2018) Vellaithurai et al. (2015)	Proposing status monitoring and vulnerability assessment models through methods such as 1) calculating the supervisory control and data acquisition performance, 2) using topology-based performance indices, and 3) applying automated and proactive CP contingency analysis tools.
Modeling and simulating attack and defense	He et al. (2018) Rao et al. (2018) Shan and Zhuang (2020)	Modeling and simulating attacks and defenses by using Game theory.

Backhaus et al. (2013) have presented an approach to develop a predictive model of a human-in-the-loop control system that is required to design an attack-resilient system. This model is based on game theory and semi-networks. The interaction between system intruders and operators (defenders) is modeled, and a guide for resilience is provided through contingency analysis.

Caviglione et al. (2015) have studied human awareness of security and privacy threats in smart environments based on an agent-based approach. They describe three roles – vendors, customers, and operators – and explain how their lack of security awareness leads to threats to smart built environments. They suggest that proper and effective countermeasures should be

developed as soon as possible, and countermeasures can be stimulated by the efforts made in other fields, such as peer-to-peer and ad-hoc networks.

Jiow (2017) has highlighted human factors and has studied the involvement of the public in CP security from two aspects – educational efforts and cultivating safe online practices. This study discusses two kinds of efforts in Singapore and Australia, and concludes that Singapore has more related education programs than Australia. The researcher suggests that Singapore should put more effort into education programs about CPS security to help the public watch out for deceptive practices, and Australia should provide more education programs for the general public. Clark and Hakim (2017) have also proposed that education is an important aspect of cybersecurity and a key to protect critical infrastructures from cyber threats. They suggest that more education programs should be provided to "the general public, including the need for secure passwords and awareness of malicious spam". They propose a public-private partnerships (PPPs) solution for cybersecurity, which may be applicable to solving some of the constitutional and political barriers in the US.

Intelligently detecting intrusions

Čeleda et al. (2012) have studied the specific Building Automation and Control System (BACS) networks and utilized network traffic flow information for monitoring BACS networks. They use a tool named *BACnetFlow* proposed by Krejčí et al. (2012) to identify and describe network traffic flows related to the BACnet protocol. Specifically, they apply an approach used in IP networks to the BACS network environment. This approach is based on entropy, which is a measure of the randomness of data. Through this approach, one type of Telnet attack that infecting ordinary computers with Microsoft Windows can be detected by comparing the entropy in the network.

Lo and Ansari (2013) have formulated an attack model, CONSUMER, which demonstrates that an illegal customer ''can steal'' electricity via compromised smart meters by lowering the reading of its energy consumption and raising others' in a neighborhood distribution network. They develop a novel hybrid intrusion detection system framework incorporating power information and sensor placement to detect malicious attacks that are undetectable by the traditional measurement. This framework includes power grid information and sensor placement. An algorithm for placing grid sensors throughout a distribution network is proposed to provide sufficient network observability to enhance detection performance.

Transactive energy system (TES) is a new paradigm for power system operation and control. TESs are vulnerable to cyberattacks because of the financial interest motives of stakeholders (Zhang et al. 2020). Zhang et al. (2020) have modeled and simulated the components of TES and have proposed a deep learning approach called deep-stacked autoencoder (SAE) to detect potential anomalies in the market and physical system measurements. SAE can "extract the baseline of the time series signals" and use domain knowledge (for example, "outage has more impacts on generators, and the attack has more impacts on the market behaviors") and can discover which signal contributes most to the reconstruction error. This approach can detect unobserved attacks and apply optimized domain expertise.

The approach that Čeleda et al. (2012) proposed can detect intrusions within the BACS networks by identifying network traffic flows. The intrusion detection approach proposed by Lo and Ansari (2013) is augmented by some sensors to monitor the whole system. They have also provided algorithms for optimizing the sensor deployment to improve observability and detection rate with a limited number of sensors.

Improving system resilience

Zonouz et al. (2014) have proposed a security-oriented CP contingency analysis (SOCCA) framework to identify contingencies through cyberattacks, considering the current state of cybersecurity in the power system control network. SOCCA can provide predictive capabilities of situational awareness for the power grid security officers by assessing the global impacts of different cyberattacks on the power grid, and thus, help operators decide on the proper deployment of preventive solutions for intrusion.

Smart grid consists of physical power systems and cyber information systems. Although the physical systems and cyber components separately can be resilient or enhanced by some measures (Moslehi and Kumar 2010, Zhu 2019), the interaction between these two environments can create new challenges for the resilience of the smart grid (Zhu 2019). To cope with these challenges, Zhu (2019) has hierarchically organized the smart grid into six layers, which are physical layers, control layers, data communication layer, network layer, supervisory layer, and management layer. Based on the multilayer architecture of the smart grid, the researcher identifies the security challenges from each layer and proposes a holistic viewpoint for security solutions in the smart grid. This study proposes a conceptual control system with layering for facilitating the understanding of the cross-layer interactions between the physical world and the cyber world, which can be a foundation for a framework of resilient power system design.

Based on some quantitative factors that can affect resiliency, Venkataramanan et al. (2020) have proposed a CP security assessment metric, CP-SAM, by using "concepts from graph-theoretic analysis, probabilistic model of availability, attack graph metrics, and vulnerabilities across different layers of the microgrid system". This metric can help monitor microgrid resiliency and select the best possible mitigation strategies for microgrid system resilience. CP-SAM can be applied in active distribution systems and has been validated in a testbed.

The SOCCA proposed by Zonouz et al. (2014) has complemented the traditional power contingency analysis methods by providing operators with predictive situational awareness and enabling them to propose preventive solutions for proactive intrusion. It can be used for accidental contingencies and malicious compromises to help the grid to continue operating in the case of failure. The conceptual layered control system proposed by Zhu (2019) is generally applicable to resilient power system design. The CP-SAM metric proposed by Venkataramanan et al. (2020) can be applied in active distribution systems but it becomes less reliable when considering more than 15 factors.

Optimizing attack mitigation strategy

Using the Weighted Least Square state estimation formulation, Bretas et al. (2017) have presented an analytical method for smart grids CP security. This method can "detect, identify, and correct malicious data attacks in smart grids". In this research, "malicious data attacks are modeled as bad data, and the power system is modeled as a set of non-linear equations". The researchers utilize the χ^2 Hypothesis Testing with the random variable Composed Measurement Error to detect the attack. This method can be applied widely even without the knowledge of the cyberattack model. As long as the method "is restricted to a change of measurements, parameters, or topology, the error can be estimated, and then the bad data get corrected".

"Attacks that impact the integrity and availability of measurement-and-control data have a direct impact on the reliability and security of the bulk power system" (Ashok et al. 2017). Ashok et al. (2017) have focused on the types of attacks and have proposed an end-to-end attack-

resilient CP security framework for wide-area monitoring, protection, and control (WAMPAC) applications in the power grid. This framework can address the security issues of the entire life cycle including "risk assessment, attack prevention, attack detection, attack mitigation, and attack resilience". They have described a defense-in-depth architecture for WAMPAC that incorporates infrastructure and application-layer reliance.

Hong et al. (2019) have used the attack tree to model cyberattacks. Impact analysis is applied in analyzing the consequences of a cyberattack on the substation and the power system as a whole. They propose novel mitigation methods based on the power system domain. These mitigation methods can be applied even though ICT-based solutions (such as firewall, or intrusion detection system) are compromised. With the mitigation methods, the accuracy of traditional intrusion detection and anomaly detection can be improved, and human errors can be lowered by preventing operators from incorrect commands before they enforce the control actions.

The method proposed by Bretas et al. (2017) is generally applicable even without the knowledge of the cyberattack model. The CP security framework for WAMPAC proposed by Ashok et al. (2017) has provided a method to generate the conceptual solution under a specific attack scenario. The mitigation method proposed by Hong et al. (2019) is mainly applied in the remote attack to substations.

Real-time monitoring system status and assessing system vulnerability

Vellaithurai et al. (2015) have proposed an automated and proactive CP contingency analysis tool called CPINDEX to monitor the current status of the power system. This tool can calculate a CP contingency ranking by inputting the network configurations, the power system topology, and the current intrusion detection systems alert. The CP contingency ranking is an indication of the current status of the power system.

Stefanov et al. (2015) have presented a model and simulation platform for the supervisory control and data acquisition (SCADA) system of an integrated CPS. The SCADA performance is calculated based on communication time delays. The researchers calculate the latencies of packets to identify the communication congestions. They also compute the success rates of cyberattacks and the dynamic impacts of cyberattacks on the grid. Besides that, they have proposed methods to model cyber intrusions and assess the vulnerability of an integrated CPS.

Srivastava et al. (2018) have presented centrality indices based on graph theory for vulnerability assessment in the power system in terms of various bus and branch contingencies by using limited system information. They provide defensive mechanisms by utilizing topology-based performance indices to prevent such an attack.

Modeling and simulating attack and defense

Game theory is applied widely in capturing the strategic interactions between the attacker and the defender on securing critical infrastructure (Xu and Zhuang 2019). Based on the game theory, the measurement of the infrastructure performance has been formulated as a game by Rao et al. (2018), "using composite utility functions that generalize the sum-form and product-form utility functions". Rao et al. (2018) have derived Nash equilibrium conditions. The equilibrium conditions can provide expressions for "individual system survival probabilities and the expected capacity specified by the total number of operational components in terms of composite gain-cost and composite multiplier".

"Coalitional attacks can be launched by multiple adversaries cooperatively against the smart-world system such as smart cities" (He et al. 2018). To deal with them, He et al. (2018) have proposed a model based on game theory to capture the interactions among multiple adversaries and have quantified the capacity of the defender based on the extended Iterated Public Goods Game model. With the proposed game model, the defender can analyze the behavior of the adversaries and deploy the defensive strategies properly to inspire competition among them to reduce the impacts caused by coalitional attacks.

Shan and Zhuang (2020) have formulated a game-theoretic model to study the strategic interactions between a defender and an attack at the three-level networks – power plants, transmissions, and distribution networks. They find that the attacker's best responses are not affected by the interdependent relations between the networks. "The defender's best responses at power plants and transmissions networks are not only a function of the number of nodes attacked at that particular level of the network, but also the attack strategy at its parent or child network (above the transmission network level)" because of the interdependent relations between the networks.

DISCUSSIONS AND RECOMMENDATIONS FOR FUTURE RESEARCH

According to the content analysis on the literature, there are only three papers of all the reviewed publications studying human factors for CP security of the built environment. One of them is emphasizing the importance of improving human awareness. Another is proposing solutions such as providing general education for the public. The last one is considering human factors when designing a system for CP resilience. More studies are still in need to investigate human factors in CP security for smart built environments.

Most of the reviewed research studies are focused on one particular type of cyberattack, while coordinated attacks are not sufficiently studied. A few research studies are focusing on coordinated attacks with two cyberattacks (Xiang et al. 2017, He et al. 2018) but more research on coordinated attacks with two or more cyberattacks should be conducted.

Many studies investigate the means and methods for detecting cyberattacks after they have occurred and for mitigating the attack damage. Current research on preventive solutions mainly relies on making standards by the institutes such as NIST and industry associations, which requires a long process to accomplish and may not be as effective as expected (Cardenas et al. 2009). Therefore, more research on preventive solutions for CP security for smart built environments is still in need.

Most studies are only focused on cybersecurity instead of the interactions between cybersecurity and physical security. Cybersecurity issues and physical security issues are mingling in smart built environments. Although the current research has studied solutions to detect and mitigate cyberattacks, there are still unknown cyber-physical threats in a whole system. Thus, more studies on the interactions between cybersecurity and physical security should be conducted.

CONCLUSION

This paper aims to provide an overall picture of management solutions for CP security in smart built environments. It contributes to the body of knowledge by summarizing and discussing six types of management solutions for building CP security. Through a

comprehensive literature review, we have found that most research studies are focused on CP security of smart grids and power systems. These studies have proposed methods or frameworks to detect intrusions, mitigate impacts of cyberattacks, monitor the system status, and improve the resilience of the systems. Some research gaps in this field are identified: 1) human factors should be further investigated when designing systems for CP resilience, 2) the effects of coordinated attacks with the combination of different cyberattacks should be further studied, 3) preventive solutions other than standards and guidelines are in need, and 4) the interactions between cybersecurity and physical security need to be further investigated.

REFERENCES

Agarwal, R. (2021). *Graph-based Simulation for Cyber-physical Attacks on Smart Buildings*. Master of Science in Computer Science.

Ashok, A., Govindarasu, M., and Wang, J. (2017). "Cyber-Physical Attack-Resilient Wide-Area Monitoring, Protection, and Control for the Power Grid." *Proceedings of the IEEE*, 105(7), 1389-1407.

Backhaus, S., Bent, R., Bono, J., Lee, R., Tracey, B., Wolpert, D., Xie, D., and Yildiz, Y. (2013). "Cyber-Physical Security: A Game Theory Model of Humans Interacting Over Control Systems." *IEEE Transactions on Smart Grid*, 4(4), 2320-2327.

Bretas, A. S., Bretas, N. G., Carvalho, B., Baeyens, E., and Khargonekar, P. P. (2017). "Smart grids cyber-physical security as a malicious data attack: An innovation approach." *Electric Power Systems Research*, 149, 210-219.

Cardenas, A. A., Amin, S., Sinopoli, B., Giani, A., Perrig, A., and Sastry, S. (2009). "Challenges for Securing Cyber Physical Systems." *Workshop on Future Directions in Cyber-physical Systems Security, DHS, 23, July, 2009*.

Caviglione, L., Lalande, J.-F., Mazurczyk, W., and Wendzel, S. (2015). "Analysis of Human Awareness of Security and Privacy Threats in Smart Environments." *Human Aspects of Information Security, Privacy, and Trust. HAS 2015. Lecture Notes in Computer Science*, Springer.

Čeleda, P., Krejčí, R., and Krmíček, V. (2012). "Flow-Based Security Issue Detection in Building Automation and Control Networks." *18th European Conference on Information and Communications Technologies (EUNICE) 2012*, Springer, Budapest, Hungary.

Clark, R. M., and Hakim, S. (2017). "Protecting Critical Infrastructure at the State, Provincial, and Local Level: Issues in Cyber-Physical Security." *Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level*, Springer-Verlag Berlin, Berlin, 1-17.

He, X., Yang, X., Yu, W., Lin, J., and Yang, Q. (2018). "Towards an Iterated Game Model with Multiple Adversaries in Smart-World Systems." *Sensors (Basel)*, 18(2).

Hong, J., Nuqui, R. F., Kondabathini, A., Ishchenko, D., and Martin, A. (2019). "Cyber Attack Resilient Distance Protection and Circuit Breaker Control for Digital Substations." *IEEE Transactions on Industrial Informatics*, 15(7), 4332-4341.

Jiow, H. J. (2017). "Efforts to Get People Involved in Cyber-Physical Security: Case Studies of Australia and Singapore." *Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level*, Springer-Verlag Berlin, Berlin, 221-232.

Krejčí, R., Čeleda, P., and Dobrovolný, J. (2012). "Traffic measurement and analysis of building automation and control networks." *IFIP International Conference on Autonomous Infrastructure, Management and Security*, Springer, 62-73.

Lo, C.-H., and Ansari, N. (2013). "CONSUMER: A Novel Hybrid Intrusion Detection System for Distribution Networks in Smart Grid." *IEEE Transactions on Emerging Topics in Computing*, 1(1), 33-44.

Moslehi, K., and Kumar, R. "Smart Grid - A Reliability Perspective." *Proc., IEEE PES Conference on "Innovative Smart Grid Technologies" January 19-20, 2010*.

Rao, N. S. V., Ma, C. Y. T., Hausken, K., He, F., Yau, D. K. Y., and Zhuang, J. (2018). "Defense Strategies for Asymmetric Networked Systems with Discrete Components." *Sensors (Basel)*, 18(5).

Roof, K., and Oleru, N. (2008). "Public Health: Seattle and King County's Push for the Built Environment." *Journal of Environmental Health*, 71(1), 24-27.

Shan, X. G., and Zhuang, J. (2020). "A game-theoretic approach to modeling attacks and defenses of smart grids at three levels." *Reliability Engineering & System Safety*, 195.

Sjelin, N., and White, G. (2017). "The Community Cyber Security Maturity Model." *Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level*, 161-183.

Srivastava, A. K., Ernster, T. A., Liu, R., and Krishnan, V. G. (2018). "Graph-theoretic algorithms for cyber-physical vulnerability analysis of power grid with incomplete information." *Journal of Modern Power Systems and Clean Energy*, 6(5), 887-899.

Stefanov, A., Liu, C.-C., Govindarasu, M., and Wu, S.-S. (2015). "SCADA modeling for performance and vulnerability assessment of integrated cyber-physical systems." *International Transactions on Electrical Energy Systems*, 25(3), 498-519.

Sugawara, T., Cyr, B., Rampazzi, S., Genkin, D., and Fu, K. "Light Commands: Laser-Based Audio Injection Attacks on Voice-Controllable Systems." *Proc., the 29th USENIX Security Symposium*, 2631-2648.

Symantec Corporation. (2014). *Internet security threat report 2014* (Vol. 19).

Vellaithurai, C., Srivastava, A., Zonouz, S., and Berthier, R. (2015). "CPIndex: Cyber-Physical Vulnerability Assessment for Power-Grid Infrastructures." *IEEE Transactions on Smart Grid*, 6(2), 566-575.

Venkataramanan, V., Hahn, A., and Srivastava, A. (2020). "CP-SAM: Cyber-Physical Security Assessment Metric for Monitoring Microgrid Resiliency." *IEEE Transactions on Smart Grid*, 11(2), 11.

Weerakkody, S., and Sinopoli, B. (2019). "Challenges and Opportunities: Cyber-Physical Security in the Smart Grid." *Smart Grid Control: Overview and Research Opportunities*, Springer, New York, 257-273.

Zhang, Y., Krishnan, V. V. G., Pi, J., Kaur, K., Srivastava, A., Hahn, A., and Suresh, S. (2020). "Cyber Physical Security Analytics for Transactive Energy Systems." *IEEE Transactions on Smart Grid*.

Zonouz, S., Davis, C. M., Davis, K. R., Berthier, R., Bobba, R. B., and Sanders, W. H. (2014). "SOCCA: A Security-Oriented Cyber-Physical Contingency Analysis in Power Infrastructures." *IEEE Transactions on Smart Grid*, 5(1), 3-13.

Xiang, Y., Wang, L., and Liu, N. (2017). "Coordinated attacks on electric power systems in a cyber-physical environment." *Electric Power Systems Research*, 149, 156-168.

Xu, Z., and Zhuang, J. (2019). "A Study on a Sequential One-Defender-N-Attacker Game." *Risk Analysis*, 39(6), 1414-1432.

Zhu, Q. (2019). "Multilayer Cyber-Physical Security and Resilience for Smart Grid." *Smart Grid Control: Overview and Research Opportunities*, Springer, New York, 225-239.