Smart Attacks in Smart Grid Communication Networks

Pin-Yu Chen, University of Michigan
Shin-Ming Cheng, and Kwang-Cheng Chen, National Taiwan University

ABSTRACT

The operations of a smart grid heavily rely on the support of communication infrastructures for efficient electricity management and reliable power distribution. Due to the strong dependency, the robustness of a smart grid communication network against attack is of the utmost importance for the deployment of the smart grid. Notably, the large scale and autonomous features of a smart grid render its cyber security quite vulnerable to adversaries. In this article, we introduce several intelligent attacks and countermeasures in smart grid communication networks, which aim for maximal damage or benefits by taking advantage of the network structure as well as the protocol functionality. We adopt the percolation-based connectivity in statistic mechanics to quantitatively analyze the network robustness. If the attack and defense strategies are involved, the attack can be further smart and complicated. Consequently, a two-player zero-sum game is introduced between the adversary and the defender, and the outcome of the game equilibrium is used to evaluate the performance of defense mechanisms with different network configurations. This article therefore offers novel insights and comprehensive analysis on the cyber security of a smart grid.

INTRODUCTION

The emergence of the smart grid is to expand the current capabilities of the grid's generation, transmission, and distribution systems for autonomous power distribution and efficient electricity management. Loosely speaking, a smart grid is composed of a power grid and a communication network atop the power grid for data retrieval to fully facilitate its functionality [1]. To achieve timely control in the smart grid, reliable information exchange is essential for identifying the demands and status of each device, and a smart grid communication network is thus formed on top of the power grid for communication supports as shown in Fig. 1. Each node (e.g., smart meter) in the communication network feeds back the information (e.g., phasor measurements) to a fusion center (control center) for data analysis and decision making. However, the tight coupling and strong dependence between the power grid and smart grid communication networks induce new threats on this cyber-physical system, as the adversaries are able to make use of the vulnerabilities in cyber security to disrupt the operations of the smart grid by paralyzing or manipulating the communication network. As a matter of fact, while cyber security is closely related to the viability of the entire system, it is an ever increasing concern over the physical reliability due to the accessibility of the communication protocols and the autonomous features of the smart grid. The U.S. Department of Energy (DOE) has identified attack resistance to be one of the seven major properties required for the operation of a smart grid [2].

Although a layered approach is introduced in great depth in [1] to evaluate the risk of cyber-physical security of the electric power grid, the attack capabilities, and the interactions between adversary and defender in a smart grid communication network are far from realized. An analytical model to evaluate the network robustness regarding the attack and defense mechanisms, and, most important, the network topological features, is still lacking. This article focuses on the emerging smart attacks and state-of-the-art countermeasures in smart grid communication networks, where the adversaries possess intelligent capabilities to launch attacks based on the cyber-physical dependency and network vulnerabilities. Three main attack categories and countermeasures are specified based on the purpose of the adversary. In addition, as the inherent network resilience protocols in the communication infrastructures provide innate attack resistance, we integrate the large-scale feature of the smart grid communication network with concepts in statistic mechanics to investigate the network robustness under attack. Due to the network resilience to temporal disconnection or malfunctioning, a network can maintain its fundamental operations as long as a majority of nodes are still connected, which offers new avenues and solid theoretic approaches to network robustness assessment.

With the theoretic analysis of network robustness, one is able to evaluate the performance of a defense mechanism against attacks in a smart grid communication network. Since there is a fusion center in a smart grid communication net-

0163-6804/12/$25.00 © 2012 IEEE

work in charge of data analysis and decision making, it is natural to presume that the defense mechanism is employed in a similar manner, to which we refer as the fusion-based defense mechanism. The fusion center uses the collected information or previous data from each node to infer the malicious activities in smart grid communication network. More interestingly, knowing the existence of the defense mechanism, a smart adversary should manage to disguise its intention while accomplishing its attack. Conversely, the fusion center attempts to make the precision of attack inference as high as possible to reduce the network damage. These interactions lead to a two-player game where its attack and defense approaches refer to its strategy profiles, and the network robustness refers to its corresponding payoff. The outcome of the game equilibrium plays an important role in understanding the cyber security of a smart grid communication network because at the game equilibrium no player's payoff can be improved via unilateral change of its own strategy. Consequently, this article offers a novel game-theoretic framework to evaluate the cyber security when the attack and defense strategy are involved.

This article also elucidates the impacts of topological features on the network robustness in a smart grid communication network. The results on both synthetic network models and empirical network data show that smart attacks could cause fatal destruction to the network if the detection capabilities are insufficient or the network possesses an inherently fragile network structure such that the network is prone to be disintegrated when a small fraction of nodes are targeted by the adversary. These theoretic analyses on network robustness and performance evaluations can serve as future system security design guidelines and future research directions on cyber security in the smart grid.

The rest of this article is organized as follows. The categories of smart attacks in a smart grid communication network and their countermeasures are elucidated. The concepts of network resilience and network robustness are introduced. The fusion-based defense mechanism is specified. A game-theoretic analysis of the two-player attack and defense game is demonstrated. The performance evaluations are shown. Finally, we conclude this article.

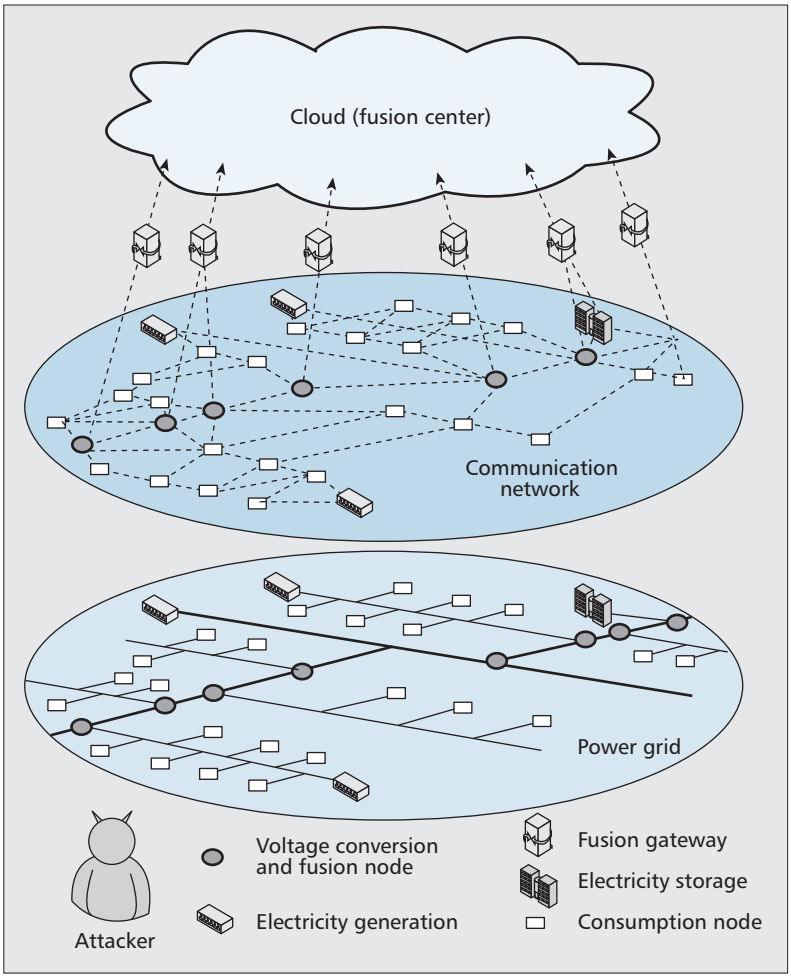

Figure 1. *A smart grid is composed of a power grid and a communication network for information exchange and timely control. Each node feeds back information to the fusion center for data analysis and decision making. This system model can be extended to a multistage hierarchical network structure composed of several fusion centers when the distributed computation mechanisms and network scalability are considered. In reality, the fusion center can be a gateway, a data aggregator, or an intelligent machine.*

Attack Category

This section introduces three main attack categories and their countermeasures in smart grid communication networks as follows.

• **Vulnerability attack:** This type of attack is induced by the malfunction of a device or communication channel, or the desynchronization of feedback information. Feedback information may be deteriorated by erroneous data delivery or unreliable channel conditions, which leads to an incorrect control process at the control center. The vulnerability attack is mainly caused by the inherent reliability in the communication network instead of malicious attacks with specific attempts, and it can be prevented by introducing the fault diagnosis scheme [3] to infer the fault detection and localization.

• **Data injection attack:** This type of attack is first proposed in [4] to alter the measurements of some meters in order to manipulate the operations of the smart grid. Although the integrity of meter data and commands is important, their damage is mostly limited to revenue loss. The impacts of the number of meters under manipulation on the attack observability are investigated, and the smallest set of meters sufficient for the adversary to control the smart grid are specified in [5]. In addition, countermeasures are demonstrated in [6] with which it is possible to defend against malicious data injection if a small subset of measurements can be made immune to the data injection attacks.

• **Intentional attack:** If an adversary is able to have full understanding of the network topology, it can fully utilize the network structure to disrupt the network operations by paralyzing some fraction of nodes with the highest degree, known as intentional attack [7]. Intentional attack can be implemented via coordinated denial-of-service (DoS) attack and contributes to network disruption due to node disconnections in the

By relating the network robustness to percolation-based connectivity, we are able to determine the defense cost and infer the presence of the attack in a smart grid communication network based on the feedback information from each node, known as the fusion-based defense mechanism.

communication network. From a graph-theoretic point of view, an intentional attack on a specific node is identical to node removal on the corresponding network graph [8]. Intentional attack is quite effective in disintegrating the network and it is relatively difficult to be detected since the adversary attacks only some central but not all nodes in the network [9]. A fusion-based defense mechanism is proposed in [10] to defend intentional attack by utilizing the feedback information from each node for attack inference and defense reaction.

Network Resilience and Network Robustness

Current research on network robustness mainly follows the graph-based connectivity (i.e., a network is connected if there is a path between any arbitrarily chosen node pair in order to maintain network operations). Nonetheless, it is worth mentioning that due to advances in network resilience protocols [11], a network is able to sustain from temporal node failures or disconnections as long as a giant connected component still exists in the network. Interesting is that the notions of network resilience coincide with the percolation phenomenon in statistic mechanics as it describes the behavior of connected clusters in a random graph [12]. We therefore refer to the network robustness regarding network resilience protocols as percolation-based connectivity. The network is expected to transit from the connected phase to the disconnected phase when the fraction of nodes removed exceeds the critical point q_c. In other words, the phase transition of percolation-based connectivity occurs at the critical value q_c since the network is decomposed into several small components, and the giant connected component vanishes when more than q_c fraction of nodes are removed from the network.

With the aid of statistic mechanics, the critical value q_c can be solved given the degree distribution of a randomly selected node in the network, which is relatively simple and analytically tractable compared with the exhaustive numerical computations due to the large-scale nature of the smart grid. More important, by acquiring the critical value of the percolation-based connectivity, the network robustness can be quantitatively defined regarding the network resilience for defense assessment and performance evaluation. Without loss of generality, we define the network robustness to be 1 if the network is connected in percolation sense; otherwise, the network robustness is –1. In the smart grid communication network, the goal of the adversary is to disintegrate the network while the defender attempts to maintain its network connectivity in the percolation sense. We demonstrate how to utilize the network robustness for attack inference and game-theoretic analysis, respectively.

Fusion-Based Defense Strategy

By relating the network robustness to the percolation-based connectivity, we are able to determine the defense cost and infer the presence of the attack in a smart grid communication network based on the feedback information from each node, known as the fusion-based defense mechanism. For instance, in order to alleviate the damage of intentional attack on the smart grid communication network, every node needs to individually employ local detection on the occurrence of attack and feedback the local decision to the fusion center with the aid of communication protocol supports. It is worth noting that this defense mechanism is quite distinct from traditional distributed detection schemes [13]. Distributed detection schemes determine the occurrence of a common event based on the feedback information of each node, whereas intentional attack only targets some particular nodes instead of a uniform attack such that it is not a common event for all nodes. This unique attribute renders intentional attack difficult to be detected via traditional distributed detection schemes since the null attack decision of untargeted nodes may deteriorate the precision of attack inference at the fusion center.

To bridge this gap, it is suggested in [10] that the fusion center should infer the feedback information from only the S nodes with the highest degree, where S is determined according to the detection sensitivity to the attack, and $S = N$ degenerates to traditional distributed detection schemes, where N is the number of nodes in the network. Moreover, due to the fact that intentional attack is capable of sabotaging all nodes simultaneously and the prior information of launching such an attack is unknown at the defender side, the Neyman-Pearson criterion is employed for the node-level defense to maximize the detection precision while confining its false alarm probability. At the network level, with the network robustness discussed earlier, the minimax criterion is employed by the fusion center to minimize the damage caused by the adversary. The attack is considered to be in vain if it is detected by the fusion center, and the false alarm from a node is assumed to play an identical role as being attacked since erroneous feedback also leads to immediate defense reactions and temporal node quarantine.

Game-Theoretic Analysis

Intuitively, if the smart grid communication network is equipped with certain defense mechanisms against attacks in the smart grid, the ultimate goal of the adversary is to sabotage or manipulate as many nodes as possible without being detected, while the defender attempts to improve the precision of the attack inference based on the feedback information to enhance the network robustness. As a result, a two-player game is formed among the adversary and the defender, where both the adversary and the defender hold their own strategy profiles, and the corresponding payoff matrix can be uniquely specified by the percolation-based connectivity discussed earlier. Due to the fact that there is at least one (mixed-strategy) Nash equilibrium in a finite matrix game, the outcome of the game equilibrium can be regarded as the network robustness at the stable stage, as no player's payoff can be improved via unilateral change of its own strategy. Furthermore, with the network

robustness defined previously, this attack and defense game can be simplified to a zero-sum game since the attack is either successful or in vain, and the Nash equilibria are equivalent in the sense that the payoffs are identical. Consequently, the outcomes of the game equilibrium serve as the performance measure of the cyber security in smart grid communication network.

Without loss of generality, we consider the worst-case scenario that the adversary can make the most use of the network topology to launch an attack, while prior information of the attack is unknown at the defender side. We choose intentional attack and the fusion-based defense mechanism as a motivating example. As shown in Fig. 2, N nodes in a smart grid communication network are labeled in descending degree order with one additional fusion center for attack inference. The adversary's strategy is to sabotage $T \in \{1, \ldots, N\}$ nodes with the highest degree, while the defender's strategy is to keep surveillance on the feedback information of $S \in \{1, \ldots, N\}$ nodes with the highest degree. Clearly, there are trade-offs between the strategy of the adversary and the defender. Given a defense strategy, the adversary tends to sabotage the most essential nodes to paralyze the entire network without being detected. Conversely, given an attack strategy, the defender tends to adjust the number of nodes under surveillance for better inference. The complicated interactions render the outcomes of the game highly nontrivial, and the game can be even more sophisticated when uncertainties such as incomplete network information are involved. Nonetheless, for the two-player zero-sum game, the outcomes of the game equilibrium can be efficiently solved via linear programming approaches [14], which tremendously reduces the computational complexity of analyzing the network robustness and avoids cumbersome numerical computations in a smart grid communication network since the dimension of the network (i.e., N) is in general quite large.

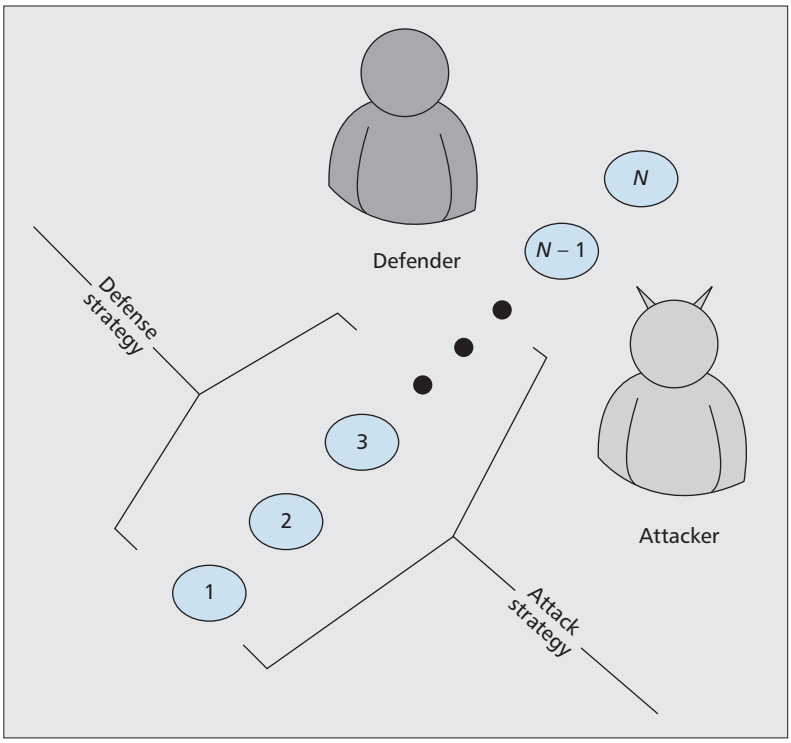

Figure 2. *Illustration of the attack and defense game. The* N *nodes are sorted in descending degree order. The attack strategy is to sabotage* $T \in \{1, \ldots, N\}$ *nodes with the highest degree, while the defender's strategy is to keep surveillance on the feedback information of* $S \in \{1, \ldots, N\}$ *nodes with the highest degree. The outcome of the game equilibrium states that no player's payoff can be improved via unilateral change of its own strategy.*

Performance Evaluation

With the notions of percolation-based connectivity and game-theoretic analysis on network robustness, we are able to investigate the performance of the fusion-based defense mechanisms against smart attacks in smart grid communication networks. Furthermore, to emphasize the impacts of topological features on network robustness, both synthetic network models and empirical data from real-world networks are used to evaluate the cyber security of the smart grid communication network. Consistent with the previous sections, we use intentional attack as an example as it is considered to be more fatal to network robustness than other attacks in a smart grid communication network.

Fusion-based Defense

Consider the fusion-based defense strategy where the fusion center keeps surveillance on the feedback information of $S \in \{1, \ldots, N\}$ nodes for attack inference. We assume that each node feedbacks one-bit information to the fusion center on behalf of its current status (i.e., 1 being attacked and 0 otherwise) to minimize the additional communication overheads. For simplicity, each node is assumed to have identical detection probability P_D and false alarm probability P_F. Based on the detection techniques [10, 13], there is an optimal detection threshold under a given defense strategy S such that the fusion center confirms the presence of an attack when the collected information exceeds the detection threshold. As shown in Fig. 3, it is straightforward that the detection threshold increases with S since it indicates that the fusion center requires more feedback information for attack inference. Moreover, the detection threshold will be enhanced if the network possesses a higher false alarm probability as the fusion center needs to compensate the damage caused by erroneous reports and false defense reactions.

Synthetic Network Model

As different network structures possess distinct topological features and therefore different critical values q_c for percolation-based connectivity, it is more tractable to conduct defense mechanisms on synthetic network models for thorough analysis and performance evaluation. In addition, since the network topology of the smart grid communication network is not visible at this point, we consider the Internet-oriented and power-grid-oriented synthetic network configurations as the performance metric of cyber security in the smart grid due to their maturity and well developed communication protocols.

For an Internet-oriented network, the degree

distribution follows a power-law distribution $P(d) \sim d^{-\alpha}$, where d is the degree of a randomly selected node in the network and $\alpha > 0$ is the power exponent. The power-law distribution reflects the fact there exists a few number of nodes (hub nodes) with extremely high degree compared with other nodes in the network. While the Internet-oriented network is quite sustainable to vulnerability attack [7], this feature results in an inherent fragility of the network, especially under intentional attack [9], by paralyzing the hub nodes to disrupt the entire system. For a power-grid-oriented network, the degree distribution follows an exponential distribution $P(d) \sim 1/\beta\ e^{d/\beta}$, where $\beta > 0$ can be approximated as the mean degree of the network when the network size is large enough. It is shown in [7] that the power-grid-oriented network is more robust against intentional attack than the Internet-oriented network due to the lack of hub nodes in the network.

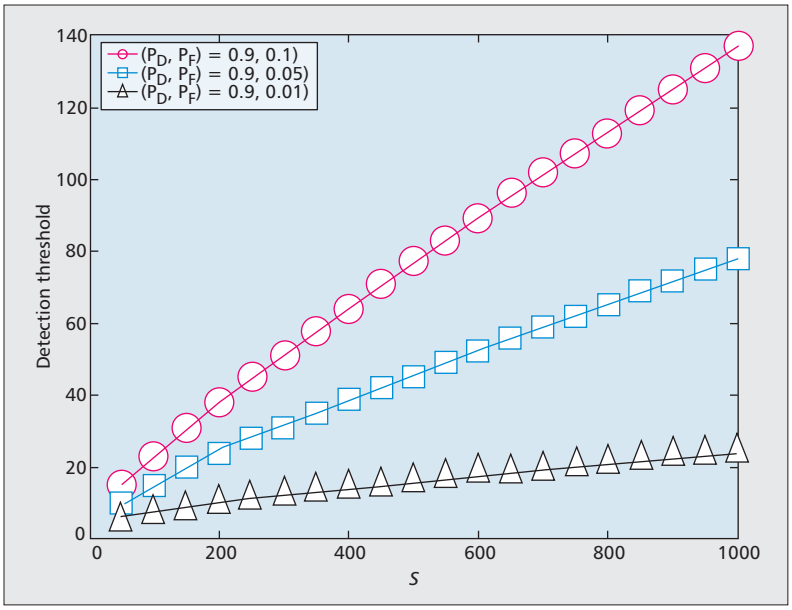

Figure 3. *Detection threshold with respect to the number of nodes under surveillance (*S*). The detection threshold increases with* S*, and the higher false alarm probability contributes to a larger detection threshold for attack inference.*

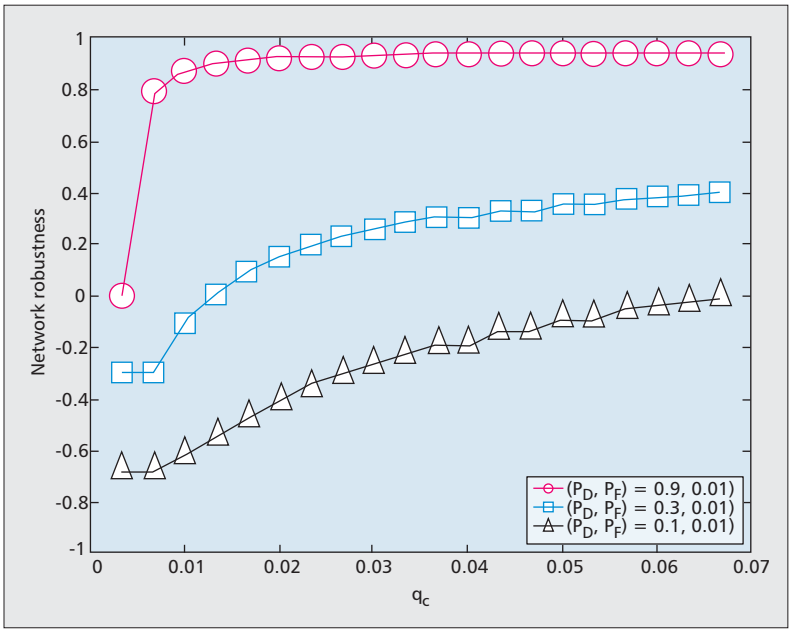

Figure 4. *Network robustness at the attack and defense game equilibrium with respect to critical values for percolation-based connectivity* q_c *and* $N = 300$*. It is shown that fragile network topology (small* q_c*) and poor detection capability (low* P_D*) tend to benefit the adversary as the network robustness tends to be negative.*

With the network robustness defined earlier, the outcome of the attack and defense game equilibrium can be used to evaluate the cyber security in a smart grid communication network. The defender is said to have a better chance to win the game if the network robustness is greater than zero. Since different network configurations result in distinct critical values q_c for the percolation-based connectivity, Fig. 4 displays the network robustness at the game equilibrium with respect to the critical values. Intuitively, fragile network topology (small q_c) and poor detection capability (low P_D) tend to benefit the adversary, whereas the network equipped with robust network structure (large q_c) and effective detection capability (high P_D) is able to prevent the network from disruption under intentional attack.

Empirical Data

To validate the employment of the fusion-based defense mechanism and the proposed game-theoretic analysis, real-world network topology data are used to investigate the cyber security as a performance benchmark to smart grid communication network. With the aid of the proposed analytical tools, the network robustness of different networks can be quantitatively specified and evaluated on the same scale. As the Internet router-level topology and the power grid may be the largest manmade network in the world, and they are very likely to be the foundations of the smart grid due to their maturity, the empirical data of these networks [7, 15] are used to investigate the network robustness. It can be seen in Fig. 5 that the EU power grid is more robust than the Internet when the detection probability is low. The presence of hub nodes in the Internet renders it prone to disintegration if the fusion center fails to detect the attack. In addition, the discrepancy of the network robustness between these two networks decreases, and the network robustness approaches 1 as the detection capability increases, which suggests that the adversary gradually loses its advantage in disrupting the network, and the damage caused by intentional attack can be alleviated by the fusion-based defense mechanism.

Conclusion

This article elucidates the smart attacks and their countermeasures in a smart grid communication network, where the adversary takes advantage of the network topological features and communication protocol vulnerabilities to manipulate or disrupt the entire system. Due to the network resilience, network robustness is quantitatively defined via percolation-based connectivity as a performance metric of cyber security in a smart grid communication network. To

enhance the cyber security, the fusion-based defense mechanism is employed for attack inference based on the collected information from each node. More important, an attack and defense game is formed between the adversary and the defender, and the outcome of the game equilibrium is used to evaluate the network robustness of the entire system. We use the game-theoretic approaches to analyze the network robustness of the synthetic network models and empirical data from the Internet-router level topology and the EU power grid. The results show that the fusion-based defense mechanism is able to effectively enhance the cyber security by acquiring one-bit (minimum) information from each node, and different network topologies indeed have remarkable impacts on the network robustness. This article therefore offers a new theoretic framework on network robustness and novel insights on cyber security in smart grid communication networks.

ACKNOWLEDGMENT

This research is sponsored by the National Science Council and INTEL Corp. under the contract of NSC 100-2911-I-002-001, and by the NSC under the contract of NSC 98-2221-E-002-065-MY3 .

REFERENCES

[1] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-Physical System Security for the Electric Power Grid," *Proc. IEEE*, vol. 100, no. 1, Jan. 2012, pp. 210–24.
[2] A System View of the Modern Grid, NETL, U.S. DOE, 2007.
[3] M. He and J. Zhang, "A Dependency Graph Approach for Fault Detection and Localization Towards Secure Smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 2, June 2011, pp. 342–51.
[4] Y. Liu, P. Ning, and M. K. Reiter, "False Data Injection Attacks Against State Estimation in Electric Power Grids," *Proc. ACM Conf. Comp. Commun. Security*, Nov. 2009, pp. 21–32.
[5] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious Data Attacks on the Smart Grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, Dec. 2011, pp. 645–58.
[6] T. T. Kim and H. V. Poor, "Strategic Protection Against Data Injection Attacks on Power Grids," *IEEE Trans. Smart Grid*, vol. 2, no. 2, June 2011, pp. 326–33.
[7] R. Albert, H. Jeong, and A.-L. Barabási, "Error and Attack Tolerance of Complex Networks," *Nature*, vol. 406, no. 6794, July 2000, pp. 378–82.
[8] R. Cohen *et al.*, "Breakdown of the Internet Under Intentional Attack," *Phys. Rev. Lett.*, vol. 86, no. 16, Apr. 2001, pp. 3682–85.
[9] S. Xiao, G. Xiao, and T. H. Cheng, "Tolerance of Intentional Attacks in Complex Communication Networks," *IEEE Commun. Mag.*, vol. 45, no. 1, Feb. 2008, pp. 146–52.
[10] P.-Y. Chen and K.-C. Chen, "Intentional Attack and Fusion-based Defense Strategy in Complex Networks," *Proc. IEEE GLOBECOM 2011*, Dec. 2011.
[11] P. Smith *et al.*, "Network Resilience: A Systematic Approach," *IEEE Commun. Mag.*, vol. 49, no. 7, July 2011, pp. 88–97.
[12] D. S. Callaway et al., "Network Robustness and Fragility: Percolation on Random Graphs," *Phys. Rev. Lett.*, vol. 85, no. 25, Dec. 2000, pp. 5468–71.
[13] P. K. Varshney, *Distributed Detection and Data Fusion*, Springer-Verlag, 1996.
[14] S. Boyd and L. Vandenberghe, *Convex Optimization*, Cambridge Univ. Press, 2004.
[15] R. V. Solé *et al.*, "Robustness of the European Power Grids Under Intentional Attack," *Phys. Rev. E*, vol. 77, Feb. 2008, p. 026102.

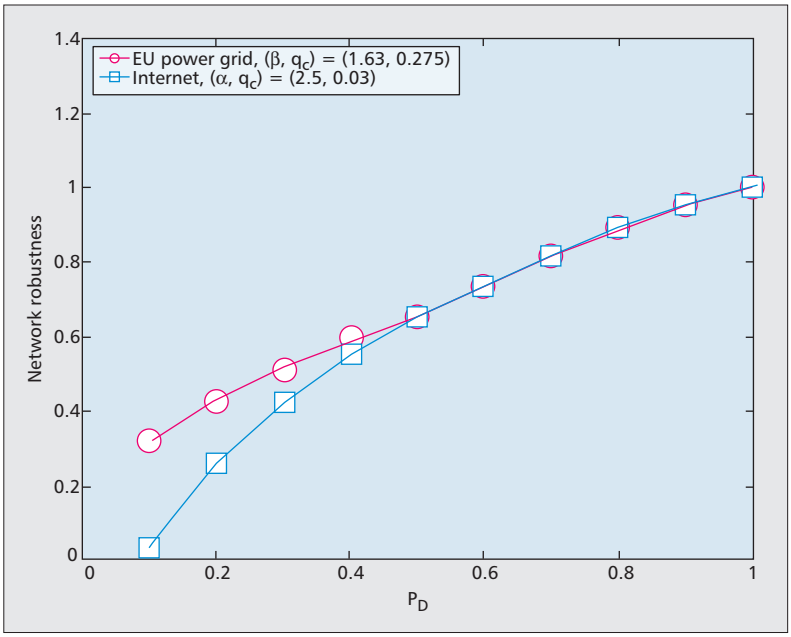

Figure 5. *Network robustness of the Internet router-level topology and the EU power grid. The empirical data are the network parameters collected in [7, 15]. The topological map of the Internet contains 6209 nodes and 12,200 links, and the EU power grid contains 2783 nodes and 3762 links. The discrepancy of the network robustness between these two networks decreases, and the network robustness approaches 1 as the detection capability increases.*

BIOGRAPHIES

PIN-YU CHEN (pinyu@umich.edu) received his B.S. degree in electrical engineering and computer science from the Undergraduate Honors Program of National Chiao Tung University, Taiwan, in 2009, and his M.S. degree in communication engineering from National Taiwan University in 2011. He is currently working toward his Ph.D. degree in the Electrical Engineering and Computer Science Department, University of Michigan, Ann Arbor. He received the IEEE GLOBECOM 2010 GOLD Best Paper Award, and his research interests include network science, interdisciplinary network analysis, and their applications to communication systems.

SHIN-MING CHENG (smcheng@cc.ee.ntu.edu.tw) received B.S. and Ph.D. degrees in computer science and information engineering from National Taiwan University in 2000 and 2007, respectively. He joined the Graduate Institute of Communication Engineering, National Taiwan University as a postdoctoral research fellow in 2007. His research interests include information security, cognitive radio networks, and network science.

KWANG-CHENG CHEN (chenkc@cc.ee.ntu.edu.tw) received his B.S. degree from National Taiwan University in 1983, and M.S. and Ph.D. degrees from the University of Maryland, College Park, in 1987 and 1989, all in electrical engineering. From 1987 to 1998 he was with SSE, COMSAT, the IBM Thomas J. Watson Research Center, and National Tsing Hua University, Hsinchu, Taiwan, working on mobile communications and networks. He is a Distinguished Professor and the director of the Graduate Institute of Communication Engineering and the Communication Research Center, National Taiwan University. He has received a number of awards and honors, including a 2011 IEEE ComSoc WTC Recognition Award, and co-authored three IEEE papers receive the 2001 ISI Classic Citation Award, the IEEE ICC 2010 Best Paper Award, and IEEE GLOBECOM 2010 GOLD Best Paper. His research interests include wireless communications and network science.