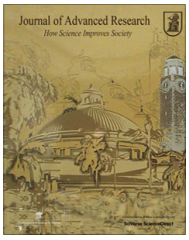
Journal of Advanced Research (2014) 5, 481–489

Cairo University

Journal of Advanced Research



ORIGINAL ARTICLE

Cyber-physical security of Wide-Area Monitoring, Protection and Control in a smart grid environment

Aditya Ashok *, Adam Hahn, Manimaran Govindarasu

Department of Electrical and Computer Engineering, Iowa State University, Ames, IA, USA

ARTICLE INFO

Article history:
Received 21 September 2013
Received in revised form 28 November 2013
Accepted 10 December 2013
Available online 27 December 2013

Keywords:
Cyber-physical security
Cyber security
WAMPAC
Smart grid

ABSTRACT

Smart grid initiatives will produce a grid that is increasingly dependent on its cyber infrastructure in order to support the numerous power applications necessary to provide improved grid monitoring and control capabilities. However, recent findings documented in government reports and other literature, indicate the growing threat of cyber-based attacks in numbers and sophistication targeting the nation's electric grid and other critical infrastructures. Specifically, this paper discusses cyber-physical security of Wide-Area Monitoring, Protection and Control (WAMPAC) from a coordinated cyber attack perspective and introduces a game-theoretic approach to address the issue. Finally, the paper briefly describes how cyber-physical testbeds can be used to evaluate the security research and perform realistic attack-defense studies for smart grid type environments.

Introduction

Smart grid technologies utilize recent cyber advancements to increase control and monitoring functions throughout the electric power grid. The smart grid incorporates various individual technical initiatives such as Advanced Metering Infrastructure (AMI), Demand Response (DR), Wide-Area Monitoring, Protection and Control systems (WAMPAC) based on Phasor Measurement Units (PMU), large scale renewable integration in the form of Wind and Solar generation, and Plug-in Hybrid Electric Vehicles (PHEV). Of these initiatives, AMI and WAMPAC depend heavily on the cyber infrastructure and its data transported through several communication protocols to utility control centers and the consumers. Cyber security concerns within the communication and computation infrastructure may allow attackers to manipulate either the power applications or physical system. Cyber attacks can take many forms depending on their objective. Attackers can perform various intrusions by exploiting software vulnerabilities or misconfigurations. System resources can also be rendered unavailable through denial of service (DoS) attacks by congesting the network or system with unnecessary data. Even secure cyber systems can be attacked due to insider threats, where a trusted individual can leverage system privileges to steal data or impact system operations. Also, weaknesses in communication protocols allow attackers to steal or manipulate data in transit.

AMI is based on the deployment of smart meters at consumer locations to provide two-way communication between

* Corresponding author. Tel.: +1 5155097636.
E-mail address: aashok@iastate.edu (A. Ashok).

Peer review under responsibility of Cairo University.

2090-1232 © 2014 Production and hosting by Elsevier B.V. on behalf of Cairo University.
http://dx.doi.org/10.1016/j.jare.2013.12.005

the meter and the utility. This provides the utility with the ability to push real-time pricing data to consumers, collect information on current usage, and perform more advanced analysis of faults within the distribution system. Since AMI is associated with the distribution system, typically a huge volume of consumer meters needs to be compromised to create a substantial impact in the bulk power system reliability. This is in strong contrast to the impact a coordinated cyber attack on WAMPAC would have on bulk power system reliability. Therefore, the main focus of this paper is to study pertinent issues in cyber-physical security of WAMPAC. However, it is to be noted that important several cyber security and privacy issues do exist with respect to AMI and are beyond the scope of this paper [1].

Wide-Area Monitoring, Protection and Control (WAMPAC)

Wide Area Monitoring, Protection and Control systems (WAMPAC), leverages the Phasor Measurements Units (PMUs) to gain real-time awareness of current grid operations and also provides real-time protection and control functions such as Special Protection Schemes (SPS) and Automatic Generation Control (AGC), besides other emerging applications such as oscillation detection, and transient stability predictions. While communication is the key to a smarter grid, developing and securing the appropriate cyber infrastructures and their communication protocols is crucial. WAMPAC can be subdivided further into its constituent components namely, Wide-Area Monitoring Systems (WAMS), Wide-Area Protection Systems (WAP), and Wide-Area Control (WAC).

PMU's utilize high sampling rates and accurate GPS-based timing to provide very accurate, synchronized grid readings. While PMU's provide increasingly accurate situational awareness capabilities, their full potential will not be realized unless these measurement data can be shared among other utilities and regulators. Additionally, power system applications need to be reexamined to determine the extent to which these enhancements can improve the grid's efficiency and reliability. The development of advanced control applications will depend on WAMS that can effectively distribute information in a secure and reliable manner. An example of WAMS deployment is NASPInet, which is the development of a separate network for PMU data transmission and data sharing including real-time control, Quality of Service and cyber security requirements [2].

Wide-Area Protection (WAP) involves the use of system wide information collected over a wide geographic area to perform fast decision-making and switching actions in order to counteract the propagation of large disturbances [3]. The advent of Phasor Measurement Units (PMU) has transformed protection from a local concept into a system level wide-area concept to handle disturbances. Several protection applications fall under the umbrella of Wide-Area Protection (WAP), but the most common one among them is Special Protection Schemes (SPS). The North American Electric Reliability Council (NERC) defines SPS as an automatic protection system designed to detect abnormal or predetermined system conditions, and takes corrective actions other than and/or in addition to the isolation of faulted components to maintain system reliability [4]. Such action may include changes in demand, generation (MW and MVAR), or system configuration to maintain system stability, acceptable voltage, or power flows. Some of the most common SPS applications are as follows: generator rejection, load rejection, under frequency load shedding, under voltage load shedding, out-of step relaying, VAR compensation, discrete excitation control, HVDC controls.

Until the advent of PMUs, the only major Wide-Area Control mechanism in the power grid was Automatic Generation Control (AGC). The AGC functions with the help of tie line flow measurements, frequency and generation data obtained from Supervisory Control and Data Acquisition (SCADA) infrastructure. The purpose of the AGC in a power system is to correct system generation in accordance with load changes in order to maintain grid frequency at 60 Hz. Currently, the concept of real-time WAC using PMU data is still in its infancy and there are no standardized applications that are widely deployed on a system wide scale, though there are several pilot projects in that area [5]. Some of the potential WAC applications are secondary voltage control using PMU data, Static VAR Compensator (SVC) control using PMUs, and inter-area oscillation damping.

The main contributions of this paper are identification of some of the pertinent issues in cyber-physical security of WAMPAC, introduction of a game theoretic framework that can model both cyber and physical system aspects together, and a brief overview of the capabilities of cyber-physical testbeds in validating and evaluating the proposed research issues. We begin by introducing a generic architecture of WAMPAC that identifies the attack points, followed by a classification of different types of cyber attacks. We then address the various cyber security issues, the potential solutions, and future efforts that are needed in every aspect of WAMPAC namely, Monitoring, Protection and Control. We also propose a game-theoretic framework to model some of the cyber-physical security issues in WAMPAC using strategic games. We conclude the paper by introducing the need for cyber-physical testbeds, and presenting a brief case study to show their potential capabilities in validation of the research.

Cyber attack taxonomy on WAMPAC

Fig. 1 shows a generic Wide-Area Monitoring, Protection and Control (WAMPAC) architecture with the various components involved. The system conditions are measured using measurement devices (mostly PMUs), these measurements are communicated to a logic processor to determine corrective actions for each contingency, and then appropriate actions are initiated, usually through high speed communication links. The inherent wide area nature of these schemes presents several vulnerabilities in terms of possible cyber intrusions to hinder or alter the normal functioning of these schemes. Even though SPS are designed to cause minimal or no impact to the power system under failures, they are not designed to handle failures due to malicious events like cyber attacks. Also, as more and more SPS are added in the power system, it introduces unexpected dependencies in the operation of the various schemes and this increases the risk of increased impacts like system wide collapse, due to a cyber attack. It therefore becomes critical to reexamine the design of the Wide-Area Protection schemes with a specific focus on cyber-physical system

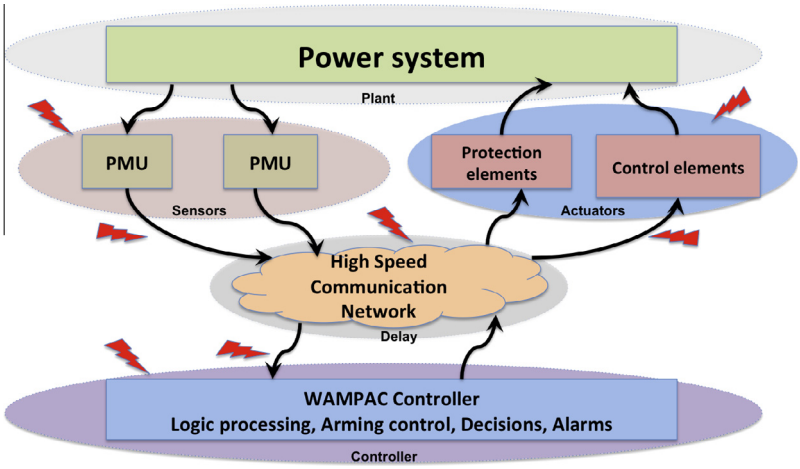


Fig. 1 Generic WAMPAC architecture.

security. This is also supported well by the WECC RAS Guide [6], which recommends that specific cyber security protection methods must be determined by each utility, and applications to protect RAS equipment be made similar to other critical cyber assets in the power system.

Fig. 1 also presents a control systems view of the power system and the wide-area protection scheme. The power system is the plant under control, where the parameters like currents and voltages at different places are measured using sensors (PMUs) and sent through the high-speed communication network to the Wide-Area Protection controller for appropriate decision making. The controller decides based on the system conditions and sends corresponding commands to the actuators which are the protection elements and VAR control elements like SVC and FACTS devices for voltage control related applications. There are different places where a cyber attack can take place in this control system model. The cyber attack could affect the delays experienced in the forward or the feedback path or it could directly affect the data corresponding to sensors, the actuators or the controller. Fig. 1 also indicates the attack points on this control system model through the lightning bolts.

Cyber attack classification

Conceptually, we identify two three classes of attacks on this control system model for WAMPAC. They are timing based attacks, integrity attacks and replay attacks.

Timing attacks: Timing is a crucial component in any dynamic system (here a protection scheme) and in our case the control actions should be executed on the order of 100–150 ms after the disturbance. This system therefore cannot tolerate any type of delay in communications and therefore are vulnerable to timing based attacks. Timing attacks tend to flood the communication network with packets and this slows the network down in several cases and also shuts them down in some cases, both of which are not acceptable. These types of attacks are commonly known as denial of service (DoS) attacks.

Data integrity attacks: Data integrity attacks are attacks where the data is corrupted in the forward or the reverse path in the control flow. This means that there could be an attack which directly corrupts the sensor data, which in this case is the PMU data, or the actuator data, which is the command given to the protection elements or the VAR control elements. This translates to actions like blocking of the trip signals in scenarios where the controller actually sent a trip command to the protection elements or the controller commanded to increase VAR injection while the attack caused the injection to decrease or vice versa.

Replay attacks: Replay attacks are similar to data integrity attacks, where the attacker manipulates the PMU measurements or the control messages by hijacking the packets in transit between the PMU and the Phasor Data Concentrator (PDC) or the control center. In several cases, a replay attack is possible even under encrypted communication as the attack packets are valid packets with the message's data integrity being intact except for the timestamp information.

Coordinated attacks on WAMPAC

Intelligent coordinated attacks can significantly affect a power system's security and adequacy by negating the effect of system redundancy and other existing defense mechanisms. North American Electric Reliability Council (NERC) has instituted the Cyber Attack Task Force (CATF) to gauge system risk from such attacks and develop feasible, and cost-effective mitigation techniques. NERC CATF identifies intelligent coordinated cyber attacks as a category of events that are classified as High Impact Low Frequency (HILF), which cause significant impacts to power system reliability beyond acceptable margins [7].

The failure of any single element in the power system, such as a transformer or a transmission line, is a credible contingency (N-1). The possibility of simultaneous failures of more than one element in the system is also taken into account when they are either electrically or physically linked. However, the definition of a "credible" contingency changes when potential failures from coordinated cyber attacks are considered. Also, an intelligent coordinated attack has two dimensions, where attacks can be coordinated in space and/or time. For example, elements that do not share electrical or physical relationships can be forced to fail simultaneously, or in a staggered manner at appropriate time intervals depending on the system response, which could result in unanticipated consequences.

The traditional approach to determining system reliability with (N-1) contingencies and a restricted set of multiple contingencies is no longer sufficient.

Fig. 2 presents several sample coordinated attack scenarios on several important WAMPAC applications like State Estimation, Automatic Generation Control and Special Protection Schemes (Remedial Action Schemes) respectively and their impacts. A coordinated data integrity attack on a key monitoring application like State Estimation could be achieved by compromising the various meters that measure or transfer the power flow measurements to the control center. This spatial coordinated attack results in a poor situational awareness of the power system and also leads to incorrect system operation leading in line overloads and market impacts in terms of uneconomical generation [8]. Similarly, a coordinated data integrity attack on Automatic Generation Control application would cause an imbalance in system generation and load resulting in frequency imbalance and reliability impacts [9]. Finally, we can consider the case of a coordinated attack on Remedial Action Schemes, which are part of WAP. The attack scenario is a combination of data integrity and denial of service attacks on the protection relays and substation communications happening in different locations, staggered in time. This type of attack results in operational reliability impacts and has the potential to cause cascading outages depending on the power system loading conditions [10].

WAMPAC: cyber security concerns, solutions and future requirements

This section will provide a brief analysis of major concerns followed by current solutions and required future efforts with respect to WAMPAC.

WAMS: concerns, solutions and future efforts

The deployment of a WAMS presents numerous cyber security concerns. The infrastructure must provide both high availability and integrity of the PMU data, while also providing some confidentiality of certain utility data. The infrastructure must simultaneously send PMU readings to many different parties to ensure everyone has a real-time system view. Therefore, the infrastructure must utilize multicast traffic to conserve network bandwidth. The design of adequate access control and authentication is also challenging. Malicious individuals must not be able to spoof or modify PMU messages as this would result in inaccurate utility estimations of the grid's state.

WAMS requires a high-speed networking infrastructure, which limits the time available to perform computationally expensive cryptographic operations, such as digital signatures. Faster symmetric key methods must be implemented; however, this requirement along with the dependency on multicast communication creates difficult key deployment strategies. This also adds additional complexity to key management operations such as redeployments, revocations, and group modifications.

Known solutions: Access control and authentication mechanisms have been proposed to address these requirements. NASPInet has identified a publisher/subscriber access control mechanisms to support the dynamic sharing of PMU data. Additionally, the IEC 61850-90-5 standard has been developed to provide support of IP-based multicast transmission and symmetric key-based authorization methods (as opposed to digital signatures) to help achieve time constraints [11]. Additionally, the need for a trusted Key Distribution Center (KDC) has been addressed to facilitate the dynamic development and distribution of shared group keys.

Future efforts: Research into KDC designs that adequately achieve both system performance and cyber security requirements. Exploring KDC schemes that provide effective key and group management within the allotted system constraints remains important.

Additional issues exist through dependencies on group keys, specifically; a malicious or compromised group member could spoof messages from any system utilizing that key. Authentication mechanisms that support both group and individual paradigms may be necessary to limit the impact of a successful attack.

WAPAC: concerns, solutions and future efforts

Wide-Area Protection and Control schemes are based on protocols such as IEC 61850, which support increased

Attack Type	Attack vectors	Attack Target	Impacted Application	Coordination	Impacts
Data Integrity	Via SCADA network, RTU, IED access	SCADA status and analog measurements	State Estimation (**Wide – Area Monitoring**)	Space, same time	Poor situational awareness, Line overloads, Market Impacts
Data Integrity, DoS, Combination	Via SCADA network RTU access	Frequency, Tie-line power flow measurements	Automatic Generation Control (**Wide – Area Control**)	Space, same time	Frequency Imbalance, Operational reliability, Market Impacts
Data Integrity and DoS Combination	Via Substation LAN remote access	IEC 61850 GOOSE messages	Remedial Action Schemes (**Wide – Area Protection**)	Space, staggered time	Operational reliability, Potential to cascading outages

Fig. 2 Sample coordinated attack scenarios targeting WAMPAC.

communication between both local and remote substation devices. However, substations are geographically dispersed and often maintain limited physical network protections, thereby increasing their exposure to a cyber attack. To enforce strong communication security, messages should be authenticated to ensure that malicious commands or meter readings cannot be injected into the network.

Substation communications must also provide real-time performance. Many substation applications, such as protective relaying, which requires tripping breakers to protect physical equipment during transient spikes in current, must be executed within milliseconds. Compared to WAMS, this information is generally used for local purposes, thereby reducing the need for long-range transmission. However, many messages will require multicast communication to increase network performance.

Known solutions: The IEC 61850 standard has provided the ability for substation devices to communicate securely between themselves and the control center. However, the dependency on legacy devices provides additional concerns, as they many not support the required security functions. Research into bump-in-the-wire (BITW) security devices has explored low-latency methods for adding additional devices to retrofit communication security mechanisms. BITW mechanisms enable unsecured legacy protocols be used more securely and efficiently [12].

Future efforts: Although support for secure communication is natively supported by protocol standards, additional security concerns remain. Both public key and symmetric cryptography provide unique advantages and disadvantages [13]. A public scheme method would assume each device has its own private key and then utilizes either a list of other device's public keys or a certificate authority to enable device authentication. Unfortunately, the low latency requirements may limit public-key authentication in certain situations. Symmetric key approaches will require groups of devices leveraging shared keys. These shared keys could then be used to authenticate messages from other members. While this method is computationally easier than public key methods, it introduces additional key management concerns. Requirements for multicast communication may provide requirements for group keys, which add complexity to the key management functions.

Cyber-physical security of WAMPAC using game-theoretic approaches

The previous section introduced the cyber attack classification on WAMPAC architecture and also presented how coordinated cyber attack scenarios can cause major operational impact on the system reliability. In this section, we introduce game theory and briefly explain how it can be used as a tool to address cyber-physical security for WAMPAC systems. Depending on the formulation of the strategic game, a game-theoretic setting can help identify the most likely attack scenarios and can provide a basis for security investments given a specific attacker characterization. The game-theoretic framework provides a pragmatic method to characterize the impacts of different types of coordinated cyber attacks and also helps to identify mitigation measures, either in terms of security reinforcements or in terms of developing new planning approaches to reduce the attack impacts, based on how the problem is formulated. It allows certain flexibility to adapt the modeling by allowing for different attacker models under different settings. The formulation of the game can incorporate uncertainties from the defender and the attacker in terms of the information sets of the attacker and the defender, i.e., the attack targets, the system operating conditions, the load variations and generation uncertainties. Also, the game-theoretic framework can capture the attack impacts in terms of load loss, line flow violations, voltage violations or even the possibility of cascading outages nicely in terms of a solution cost in order to obtain the best defender strategy. Dynamic game formulations provide a modeling framework where the attacker plays various strategies based on the defender actions and the defender can adapt his defense by learning how the attacker progressively updates his strategy.

Cyber-physical security modeling using strategic games

Fig. 3 provides a basic intuition about how our current work using game theory addresses the various issues in cyber-physical security. While several existing attempts [14–17] applying game theory in network security involves modeling the attacker and the defender costs in the cyber layer (Cost 1 and Cost 2 in Fig. 3), the modeling is incomplete as they do not look at the impacts of the actions on the cyber layer in the physical layer.

Similarly, some of the earlier work studying cyber attacks on the power system considers only costs of attack impacts (Cost 3 in Fig. 3) represented as a physical system metric such as loss of load, and line flow violation. However, our approach using game theory models the interaction between the attacker and the defender in a cyber-physical system scenario capturing all the relevant costs together in a single framework:

- Cost 1: The attacker actions in the cyber layer.
- Cost 2: The attack impacts from the cyber layer to the impacts on the physical system.
- Cost 3: The defender actions in the cyber layer in terms of security reinforcements.
- Cost 4: The defender actions in the physical layer in terms of new operational strategies.

The role of game theory in the proposed research can further be understood by looking at how the proposed research closes the loop on both the cyber and the physical layers, as shown in Fig. 4. The intrusions on the cyber layer of the power system, namely the SCADA cyber environment, are captured by using Stochastic Petri Nets (SPN). Stochastic Petri Nets are used to model the entire cyber network, which can be characterized by various security measures like firewalls, intrusion detection systems and password mechanisms [18]. The modeling provides probabilities of attacks for the components of the cyber network. These probabilities can be translated into the attack costs for an attacker and help to characterize the attacker actions. The attacker actions can be used to evaluate the power system impacts, which also could be translated into costs of attack impacts. Based on these inputs, and an appropriate selection of information sets available for the attacker and the defender, a particular game formulation can be applied. Game theory then provides optimal response strategies for the defender given an attacker strategy and this serves as a feedback mechanism to model new defense measures. As noted in Fig. 4, the defense measures could be modeled either

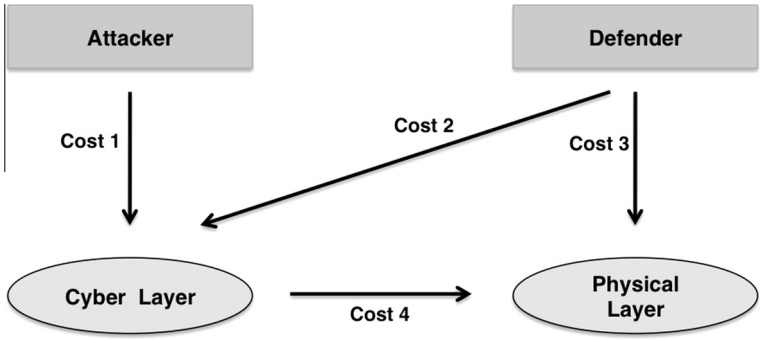


Fig. 3 Cyber physical game theory model.

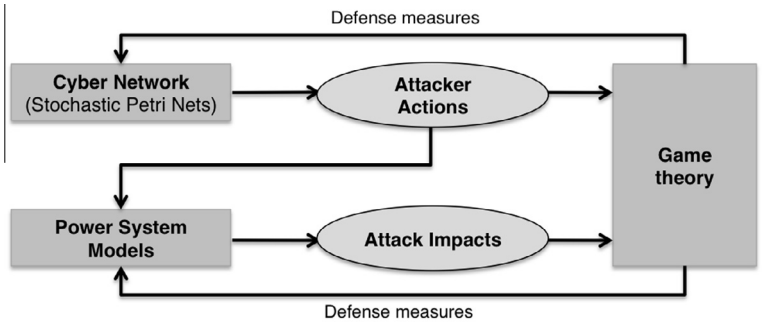


Fig. 4 A game theoretic framework for cyber security.

in the cyber layer or in the physical layer or both depending on how the strategies of the defender are modeled.

Cyber layer risk assessment: Risk assessment at the cyber layer involves defining of the cyber network topology in terms of the existing SCADA security measures such as firewall and password models at various substations. Generalized Stochastic Petri Nets (GSPN) can be used to model the cyber network [19]. The states of the stochastic process are the status of intrusions to a network that are inferred from the abnormal activities. These include malicious packets flowing through pre-defined firewall rules and failed logon passwords on the computer system. The detailed modeling of the cyber net using GSPN models for a standard test system can be found in Ten et al. [18]. By modeling the entire cyber network using the GSPN model, the steady state probabilities of an attacker passing through the various security measures to create a successful attack on selected components can be obtained. The probabilities of a particular cyber component being attacked given the SCADA security measures is used to obtain the costs of the attacker and the defender which is used as an input to the game formulation. The costs of the attacker hence can be defined as

$$\text{Cost}_{\text{attacker}} = \delta * \pi$$

where δ represents a conversion factor to translate the steady state probability π for a particular attack into an equivalent financial cost.

Impact characterization: The physical impact of a cyber intrusion on a SCADA cyber net can be measured by defining the power system topology corresponding to the cyber system and then deciding on appropriate power system metrics to capture the impacts [18] uses loss of load as an impact metric in their risk assessment framework. We note that while loss of load could be a good candidate for assessing impact, not all cyber attacks would result in loss of load. Therefore, we propose to include other common operational metrics such as line flow violations, and voltage violations. Once the appropriate impact metrics are identified based on the particular application to be studied, we can easily define the impact of the attacks in terms of costs. Similar to the previous definition of attacker/defender costs, we can define the attack impact costs as

$$\text{Cost}_{\text{impact}} = \kappa * \Delta x$$

where κ represents the unit cost of an impact metric deviation Δx in terms of dollars. For example, if the impact metric is loss of load, the impact cost would be $\kappa * \Delta L$, where ΔL is the amount of load lost in terms of MW and κ is defined in terms of \$/MW.

Different types of impact metrics could be loss of load indices, flow violations, voltage violations, etc. Each of these impact metrics could be easily modeled as a cost depending on the application. The solution of the game will depend on what costs dominate the attacker and the defender payoffs. Therefore, if the game-theoretic framework is applied for obtaining a power system planning approach, we can ignore the attack and defense costs so that the solution is influenced only by the way the impacts are characterized.

Attack modeling: The nature of the strategic interaction between the attacker and the defender is captured by attack modeling. First, the type of the particular attacks under study and their scope is clearly defined, e.g., risk assessment of coordinated attacks. Then an appropriate attack template is identified, which indicates actual targets of the attack. In

the power system, examples of attack targets are transmission lines, transformers, generators, loads, etc. Based on the attack model and the template the attacker and the defender can be characterized with corresponding action spaces. The action space of the attacker is the set of actions, which the attacker can choose. For example if the attack model is to choose to create a (N-2) contingency, then the action space consists of all possible combinations of any two components in the power system. Similarly, for the defender the action space could be the set of components that the defender chooses to protect. Depending on the application under study, the action spaces can be chosen to vary. Also, the characterization involves clearly identifying the information set available to each player about the other player's preferences, payoffs and strategies.

Game formulation and solution strategies: The formulation of the game model is very important in the entire modeling framework as it determines the nature of the solution strategies. Based on the attack modeling (which provides attacker/defender characterization), risk assessment (which provides attacker/defender costs) and impact characterization (which provides the impact costs), an appropriate game model can be chosen to obtain the best response strategies for the attacker and the defender.

Potential game formulations: We identify several potential game-theoretic formulations, which help to model various cyber attack scenarios based on the attack model, and the information sets available to the attacker and the defender. The strategic game formulations could vary from a simple single stage game to a complex multistage game where the attacker and the defender play repeatedly over infinite possible rounds of the game. Some of the potential types of game formulations are as follows:

1. Zero sum games: In its simplest form, this type of games involve two players having opposing objectives, in our case the attacker and the defender. We can consider the attacker's gain as the loss for the defender and vice versa.
2. Nonzero sum games: In this type of games, the two players do not have exactly opposing objectives. In our case, we can consider scenarios where the attacker's payoffs for a certain action are different from that of the defender's payoffs for a certain defensive action.
3. Bayesian games: In a Bayesian game formulation, the information about characteristics and payoffs of the other players, namely the attacker/defender is incomplete. Players have probabilistic beliefs about the type of each player and they update their beliefs as the game is played, i.e., the belief a player holds about another player's type might change based on the actions they have played.
4. Learning and behavioral games: These types of games assume that players can learn over time about the game and how other players are behaving. Behavioral game-theoretic formulations are based on how humans actually play games and are not based on the assumption that players respond optimally to a rival strategy.

The solution strategies obtained using game theory would be flexible based on the type of the application considered. For example, when performing risk-assessment and mitigation, the solution strategies identify the best responses in terms of security investments to tolerate the attacks modeled through the attacker actions. Similarly, game theory can also provide solution strategies in terms of minimizing the impact on the real-time operation of the power system provided that the defender actions are characterized appropriately to correspond to operational strategies.

Cyber-physical testbed based evaluation

The previous section identified how cyber-physical security can be modeled using game theory as a tool. In this section, we motivate the importance of cyber-physical testbeds to study the impacts of coordinated cyber attacks on the smart grid.

Need for testbeds

As more and more cyber security issues and concerns arise in a smart grid environment, there is a growing need to validate new research studies on real systems. However, it becomes prohibitively expensive to create and run experiments on a large-scale realistic test system. The other traditional alternative to such a scenario would be to depend on pure simulation based methods to validate such studies. However, due to the multiple and sophisticated interactions between the various cyber and physical systems in a smart grid environment, traditional simulation tools fail to capture such interdependencies accurately.

In order to accurately capture the attack effects and their impacts, a testbed needs to capture three key elements and their interdependencies: the cyber infrastructure, the communication infrastructure and the physical infrastructure. Cyber-physical testbeds model realistic cyber environments and provide accurate evaluations of vulnerabilities that exist in the cyber systems and also help to quantify the impact of a cyber intrusion on the operation of the underlying physical system. The overall research scope that can be addressed using a testbed includes [10]:

1. Vulnerability assessment – inspect weaknesses in industry standards, software platforms, network protocols and configurations.
2. Impact analysis – explore the physical system impacts from various cyber attacks to quantify physical impact.
3. Mitigation research – evaluation of mitigation strategies against various attacks and system topologies and configurations.
4. Cyber-physical metrics – development of metrics, which combine cyber-physical properties.
5. Data and model development – provide researchers with the information required to explore innovative security approaches.
6. Security validation – design methods to enable evaluation of the security posture of a system for self-assessment and compliance requirements.
7. Interoperability – evaluate how products and technologies support and connect with real-world environments.
8. Cyber forensics – explore methods for detecting attacks specific to industry protocols and field devices.
9. Operator training – provide operators with the ability to interact with power system controls during simulated cyber attacks.

The testbed design process entails making effective tradeoffs based on the intended purpose. An efficient testbed design typically consists of the integration of physical, emulation and simulation-based components, thereby achieving a balance of cost, simulation fidelity and accuracy. A detailed methodology of testbed design, the various tradeoffs, testbed applications and case studies are presented in Hahn et al. [10]. The following section briefly summarizes key observations from one such case study that was presented in Hahn et al. [10].

Case study: coordinated attacks on Remedial Action Schemes

The Remedial Action Scheme (RAS) considered in the case study was defined to reduce generation at a particular bus when one of the two lines connected to it is tripped and has been adapted from WECC RAS list [20]. The coordinated attack scenario considered is the tripping of one of the two transmission lines in the system through a data integrity attack on the associated protective relay. This action triggers the protection sequence as defined in the RAS. As per the definition of the RAS, the relay, which acts as the RAS controller, sends out a generation drop command to the generation controller so that the other connected line is prevented from overload. However, this communication is interrupted by creating a denial of service attack on either the communication network switch that transports the control message or the RAS controller relay itself as part of the coordinated attack. If the generation is not reduced within a certain time threshold, the other line connected to the generator trips out on overload, isolating the generator from the rest of the power system.

For this coordinated attack scenario with the data integrity and the denial of service attack, experiments were designed and repeated to identify the attack volumes necessary to choke the network switch and the relay, and also to identify the variation in latency for the cases where the RAS control message was able to reach the generator controller. One key observation which was made was that the protective relay was much more vulnerable to DoS attacks as it could be disrupted with significantly lesser bandwidth compared to the network switch. In terms of power system impacts, even though the first relay trip did not cause much damage, the second relay tripping isolated a generator of the network and therefore caused significant damage. If this scenario were considered under heavy system loading conditions, this would have resulted in cascaded tripping of lines causing a system wide blackout event.

Conclusion

In this paper, we articulated the importance of securing the WAMPAC to maintain bulk power system reliability. We presented cyber attack taxonomy on WAMPAC, and also identified the cyber security requirements, concerns and future requirements for the various applications. Then, the paper introduced different types of coordinated cyber attack scenarios in WAMPAC and presented their potential impacts. A game-theoretic framework is proposed to model cyber-physical security for WAMPAC applications. Finally, the paper introduces cyber-physical testbeds as key components to validate the proposed cyber security research and briefly summarizes how coordinated attacks on WAP could be analyzed using such testbeds.

The game theoretic approach opens up new in avenues cyber-physical security modeling as coordinated cyber attacks are modeled as a strategic interaction between the attacker and the defender. This enables game theory to model cyber attack 'threats', which cannot be modeled using traditional risk assessment approaches. By appropriately choosing a game-theoretic formulation we can model dynamic cyber attack scenarios depending on the attacker/defender model, and the information sets available to the attacker and the defender. We plan to begin by introducing a simple zero-sum game formulation to establish a basic understanding of the game model involved. Then we intend to further extend this framework to complicated scenarios such as multi-stage games, Bayesian games and other game theory models based on learning and behavioral games in our future work.

Conflict of interest

The authors have declared no conflict of interest.

Acknowledgment

The authors would like to thank Dr. Saurabh Amin for providing us insights on game theoretic concepts and formulations.

References

[1] Cleveland F. Cyber security issues for advanced metering infrastructure (AMI). In: Proceedings of power and energy society general meeting – conversion and delivery of electrical energy in the 21st century; 2008.
[2] Bobba R, Heine E, Khurana H, Yardley T. Exploring a tiered architecture for naspinet. In: Proceedings of innovative smart grid technologies (ISGT); 2010.
[3] Terzija V, Valverde G, Cai D, Regulski P, Madani V, Fitch J, et al. Wide-area monitoring, protection, and control of future electric power networks. Proc IEEE 2011;99(1):80–93.
[4] Madani V, Novosel D, Horowitz S, Adamiak M, Amantegui J, Karlsson D, et al. IEEE PSRC report on global industry experiences with system integrity protection schemes (SIPS). IEEE Trans Power Deliv 2010.
[5] North American Synchrophasor Initiative (NASPI). Phasor Data Applications Table [Internet]; 2009. Available from: <https://www.naspi.org/File.aspx?fileID=537>.
[6] Western Electricity Coordinating Council. WECC Remedial Action Scheme Design Guide [Internet]; 2006. Available from: <http://www.wecc.biz/committees/StandingCommittees/OC/TOS/RWG/Lists/Calendar/Attachments/13/06a-RAS_Guide_5.02.pdf>.
[7] North American Electric Reliability Corporation. High-impact, low frequency event risk to the North American bulk power system. In: Jointly-commissioned summary, Report, US Department of Energy; 2009.
[8] Liu Y, Ning P, Reiter MK. False data injection attacks against state estimation in electric power grids. In: Proceedings of the 16th ACM conference on computer and communications security, CCS '09, ACM, New York, USA; 2009.
[9] Sridhar S, Manimaran G. Data integrity attacks and their impacts on SCADA control system. In: Proceedings of power and energy society general meeting; 2010.

[10] Hahn A, Ashok A, Sridhar S, Govindarasu M. Cyber-physical security testbeds: architecture, application, and evaluation for smart grid. IEEE Trans Smart Grid 2013.
[11] Martin K. Synchrophasor standards development – IEEE C37.118 & IEC 61850. In: Proceedings of system sciences (HICSS), 2011 44th Hawaii international conference; 2011.
[12] Tsang P, Smith S, Yasir. A low-latency, high-integrity security retrofit for legacy scada systems. In: Jajodia S, Samarati P, Cimato S, editors. Proceedings of the IFIP TC 11 23rd international information security conference, vol. 278. Proceedings of IFIP the international federation for information processing. US: Springer; 2008.
[13] Fuloria S, Anderson R, Alvarez F, McGrath K. Key management for substations: symmetric keys, public keys or no keys?. In: Proceedings of power systems conference and exposition (PSCE), IEEE/PES; 2011.
[14] Alpcan Tansu, Basar Tamer. Network security: a decision and game-theoretic approach. Cambridge University Press; 2010.
[15] Gueye A, Marbukh V. A game-theoretic framework for network security vulnerability assessment and mitigation. In: Grossklags J, Walrand J, editors. Decision and game theory for security, vol. 7638 of lecture notes in computer science. Berlin, Heidelberg: Springer; 2012.
[16] Roy S, Ellis C, Shiva S, Dasgupta D, Shandilya V, Wu Q. A survey of game theory as applied to network security. In: Proceedings of system sciences (HICSS), 2010 43rd Hawaii international conference; 2010.
[17] Holmgren A, Jenelius E, Westin J. Evaluating strategies for defending electric power networks against antagonistic attacks. IEEE Trans Power Syst 2007.
[18] Ten CW, Liu CC, Manimaran G. Vulnerability assessment of cybersecurity for scada systems. IEEE Trans Power Syst 2008.
[19] Bause F, Kritzinger PS. Stochastic petri nets: an introduction to the theory. Sigmetrics Perform Eval Rev 1998;26(2), doi: 10.1145/288197.581194, <http://www.doi.acm.org/10.1145/288197.581194>.
[20] WECC remedial action scheme catalog summary [Internet]; 2008. Available from: <http://www.wecc.biz/committees/StandingCommittees/OC/TOS/RWG/Lists/Calendar/Attachments/4/WECC-RAS-CATALOG%2010-22-2008%20Master.pdf>.