INVITED PAPER

Cyber–Physical Attack-Resilient Wide-Area Monitoring, Protection, and Control for the Power Grid

By Aditya Ashok, *Member IEEE*, Manimaran Govindarasu, *Fellow IEEE*, and Jianhui Wang, *Senior Member IEEE*

ABSTRACT | Cybersecurity and resiliency of wide-area monitoring, protection, and control (WAMPAC) applications is critically important to ensure secure, reliable, and economical operation of the bulk power system. WAMPAC relies heavily on the security of measurements and control commands transmitted over wide-area communication networks for real-time operational, protection, and control functions. The current "N–1" security criterion for grid operation is inadequate to address malicious cyber events; therefore, it is important to fundamentally redesign WAMPAC and to enhance energy management system applications to make them attack resilient. In this paper, we present three key contributions to enhance the cybersecurity and resiliency of WAMPAC. First, we describe an end-to-end attack-resilient cyber–physical security framework for WAMPAC applications encompassing the entire security life cycle including risk assessment, attack prevention, attack detection, attack mitigation, and attack resilience. Second, we describe a defense-in-depth architecture that incorporates attack resilience at both the infrastructure layer and the application layer by leveraging domain-specific security approaches at the WAMPAC application layer in addition to traditional cybersecurity measures at the information technology infrastructure layer. Third, we discuss several attack-resilient algorithms for WAMPAC that leverage measurement design and cyber–physical system model-based anomaly detection and mitigation along with illustrative case studies. We believe that the research issues and solutions identified in this paper will open up several avenues for research in this area. In particular, the proposed framework, architectural concepts, and attack-resilient algorithms would serve as essential building blocks to transform the "fault-resilient" grid of today into an "attack-resilient" grid of the future.

KEYWORDS | Attack resilience; attack-resilient framework; cyber–physical security; wide-area monitoring protection and control

I. INTRODUCTION

The traditional electric power grid is undergoing a massive transformation across its entire spectrum—generation, transmission, and distribution—through the various smart grid initiatives driven by the U.S. Department of Energy [1]. Under the smart grid vision, the electric power grid is envisaged to leverage advances in several areas such as renewable integration, distributed generation, microgrids, demand response, plug-in hybrid electric vehicles, advanced metering infrastructure, increased deployment of advanced measurement devices such as phasor measurement units (PMUs) for synchrophasor measurements, and high-speed communication networks to support synchrophasor applications. Wide-area monitoring, protection, and control (WAMPAC) essentially consists of a mix

Manuscript received September 2, 2016; revised February 10, 2017; accepted March 6, 2017. The work of A. Ashok was supported by the Pacific Northwest National Laboratory (PNNL), which is a multiprogram national laboratory operated by Battelle for the U.S. Department of Energy under Contract DE-AC05-76RL01830. The work of J. Wang was supported by Argonne National Laboratory (ANL), which is a U.S. Department of Energy laboratory managed by UChicago Argonne, LLC under Contract DE-AC02-06CH11357; and by the Office of Electricity Delivery and Energy Reliability, U.S. Department of Energy (DOE) under Contract DE-OE0000839.
(Corresponding author: Aditya Ashok.)
A. Ashok is with Pacific Northwest National Laboratory (PNNL), Richland, WA, USA.
M. Govindarasu is with the Department of Electrical and Computer Engineering, Iowa State University (ISU), Ames, IA, USA.
J. Wang is with the Energy Systems Division at Argonne National Laboratory, Argonne, IL, USA (e-mail: jianhui.wang@ieee.org).

Digital Object Identifier: 10.1109/JPROC.2017.2686394

of modern and legacy measurement and actuation devices interconnected by a diverse variety of communication and networking technologies. WAMPAC applications provide control room operators with adequate situational awareness to securely and reliably operate the grid during system disturbances and natural events. Therefore, WAMPAC applications serve as an essential backbone for bulk power grid security, reliability, and resiliency.

Inherently, the secure and reliable operation of WAMPAC relies heavily on the security of wide-area measurements and control commands transmitted over the supervisory control and data acquisition (SCADA) communication networks for real-time operational, protection, and control functions. However, recent findings documented in government reports and other literature indicate the threat of cyber-based attacks is growing in numbers and in sophistication targeting the energy sector and in particular the electric grid [2]–[6]. A major cyber incident in the bulk power system, such as the recent one in Ukraine [5], could have potentially serious consequences in the grid operation in terms of socioeconomic impacts, market impacts, equipment damage, and/or large-scale blackouts. Several efforts at the national level such as the U.S. Department of Energy cybersecurity roadmap for energy delivery systems [7], North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) [8], NISTIR 7628 [9], and a National Electric Sector Cybersecurity Organization Resource (NESCOR) report [10] have been initiated, and are being undertaken to ensure that appropriate best practices, standards, and safeguards are put in place to enhance the security and resiliency capabilities of the electric power grid against sophisticated cyber threats.

The main focus of this paper is to introduce architectural concepts and algorithms pertaining to the cyber–physical security of WAMPAC applications, covering mostly the bulk power system. To that end, the key contributions of this paper include: 1) an end-to-end attack-resilient WAMPAC security framework that encompasses risk assessment, attack prevention, attack detection, attack mitigation, and attack resilience; 2) defense-in-depth architecture for attack-resilient WAMPAC that encompasses infrastructure and application-layer resilience; and 3) attack-resilient WAMPAC algorithms for key WAMPAC applications that leverage measurement design, cyber–physical system (CPS) model-based anomaly detection and mitigation. In addition, the paper also provides pointers to current and relevant literature that describes specific solution approaches in detail, wherever applicable.

The remainder of this paper is organized as follows. Section II provides a general introduction to WAMPAC through a high-level conceptual architecture and a quick overview of different types of cyber attacks in the context of WAMPAC. Section III presents an elaborate discussion on the end-to-end cyber–physical attack-resilient framework for WAMPAC. Section IV introduces the defense-in-depth architecture for achieving attack-resilient WAMPAC. Section V describes in detail the pertinent research issues for each aspect of WAMPAC separately, and briefly describes several attack-resilient WAMPAC algorithms to address those issues with illustrative case studies. Section VI summarizes the contributions of the paper and provides some general conclusions.

II. WAMPAC—ARCHITECTURE AND CYBER ATTACK MODELS

WAMPAC applications leverage SCADA systems to monitor, control, and protect the power grid. These SCADA systems collect various types of measurements from remote substations that are spread all across the grid into the energy management system (EMS) software at the control centers where operators can observe the data and issue appropriate control commands to ensure the system is operated safely, reliably, and economically. Some of the fundamental WAMPAC applications at the EMS are state estimation (SE), which includes topology estimation, automatic generation control (AGC), real-time contingency analysis, remedial action schemes (RASs), security constrained optimal power flow (SCOPF), economic dispatch (ED), and unit commitment. The availability of widespread global positioning system (GPS) time-synchronized PMU data has enabled several new and emerging WAMPAC applications such as phase angle monitoring (PAM), power oscillation monitoring (POM), power damping monitoring (PDM), voltage stability monitoring (VSM), and dynamic line rating [11].

A. Wide-Area Monitoring

SE is one of the basic wide-area monitoring applications that provide situational awareness about the system operating states to the operators. The state estimator relies on SCADA to obtain the status and analog measurements from the various remote terminal units (RTUs) at the substations. Based on the status measurements from the various breakers and switches at the substations, it builds a network topology, which is used by the rest of the EMS applications. This network topology is then used along with various analog measurements such as power flows, voltages, currents, tap settings, etc., to perform the SE process and obtain a snapshot of the system states, i.e., the voltage magnitudes and phase angles. This output of state estimator is used by several applications in the operations and planning of the power grid, such as contingency analysis, SCOPF, and various market applications. Typically, the state estimator is run once every 1 to 5 min at the utility control centers. Recent research efforts are looking at how high-fidelity synchrophasor measurements from the PMUs can be integrated into the state estimator to improve its performance. Also, as

mentioned above, there are several WAM applications that rely exclusively on PMU data such as PAM, POM, and PDM.

B. Wide-Area Protection

Typically, power system protection has been a localized concept, where protective relays work in isolation to detect faults on transmission lines, bus bars, and equipment such as generators, transformers, or loads and act quickly to protect the equipment by opening the circuit breakers. Examples of such local protection schemes are overcurrent, distance protection, and bus-bar protection. Typically, these types of protection schemes rely on offline configuration of the relay settings by the protection engineers. However, with the advent of high-speed communication networks, protocols, and synchronized PMU data, several protection schemes that rely on wide-area communication and relay coordination have been deployed and are being widely used. Some of the examples are pilot protection schemes and RAS. By definition, RAS can detect abnormal or predetermined system events and conditions, and respond with quick, automatic corrective actions to prevent, counteract, and mitigate the propagation of a small disturbance into a large-scale event. Such actions typically include load or generation shedding (MW and MVAR), changes in system configurations such as tripping lines, etc., and are often designed as safety measures to ensure the wide-area interconnected system does not cascade under stressed operating conditions. RAS are extremely sensitive to time delays and have strict timing requirements, typically, in the order of 50–150 ms.

C. Wide-Area Control

AGC is one of the major wide-area control (WAC) mechanisms in the power grid and has been around for several decades [12]. The main function of the AGC is to ensure a tight system operating frequency band around the nominal frequency (e.g., 60 Hz in North America). The AGC algorithm uses tie-line power flow measurements, frequency measurements, and generation data obtained from SCADA in order to maintain frequency within acceptable limits, and also to ensure tie-line flows match their expected schedules for economical grid operations. Typically, the AGC algorithm runs once every 2–4 s and constantly adjusts system generation to follow the load in an automated manner without operator intervention. Similarly, regional (secondary) voltage control is another wide-area control application, although not widely deployed in the United States, that attempts to regulate system voltages through the use of voltage control devices such as shunt capacitors, synchronous condensers, and flexible alternating current transmission system (FACTS) devices [13], [14]. There are several other emerging WAC applications as well that rely on the output of WAM applications such as PDM, POM, and VSM.

D. Cyber Attacks on WAMPAC

This section provides a brief overview of the different types of potential cyber attacks with respect to the generic WAMPAC architecture. It also provides a brief description of the mapping of cyber layer attacks onto physical system impacts through the associated WAMPAC applications with example scenarios.

Fig. 1 shows a high-level schematic of a generic WAMPAC architecture with the various components as part of the cyber and physical layers at the control center and the substations. At the control center we have the EMS that runs various WAMPAC applications. At the substation, we have the protection elements such as the relays, PMUs, and the actuator elements that control the real and reactive power outputs of generators, transformers and other voltage control elements such as capacitor banks. Fig. 1 also highlights the attack points on this architecture with lightning bolt symbols. As shown in Fig. 1, all the elements that are part of the cyber layer at both the control center and the substations are vulnerable to multiple types of cyber attacks.

1) Attacker Model: The overall landscape of potential attackers is quite broad, ranging from unsophisticated script kiddies and disgruntled employees all the way up to terrorist groups, trusted insiders, and sophisticated actors backed by nation states, as identified in NERC's Cyber Attack Task Force (CATF) report [6]. As mentioned in the CATF report, though the likelihood of a coordinated and stealthy cyber attack from the sophisticated actors is small, the potential consequences to the reliability of the grid could be catastrophic. Therefore, the threat model we consider for the various cyber attacks on key WAMPAC applications involves sophisticated attackers who could perform coordinated attack actions both spatially and temporally, and also attempt to evade detection through stealthy attack vectors that impact the reliability of the bulk power system. Some of these stealthy attack vectors leverage prior knowledge about the measurement configurations, system topology, and operational parameters to perform consistent data manipulations that deceive existing bad-data detection mechanisms in the control center EMS.

2) Types of Cyber Attacks: There are several types of sophisticated cyber threats such as intrusions, denial of service (DoS), malware, insider threats, and other forms of targeted attacks, which establish some sort of backdoor into the system for exploitation at a later point in time. The underlying implementation mechanisms of cyber attacks are constantly evolving, and therefore the list of cyber attack mechanisms mentioned above may not be exhaustive. However, irrespective of the specific implementation mechanism of a cyber attack, its impact eventually is reflected in one or more of the key cybersecurity properties such as confidentiality (C), integrity (I) and availability (A), also commonly

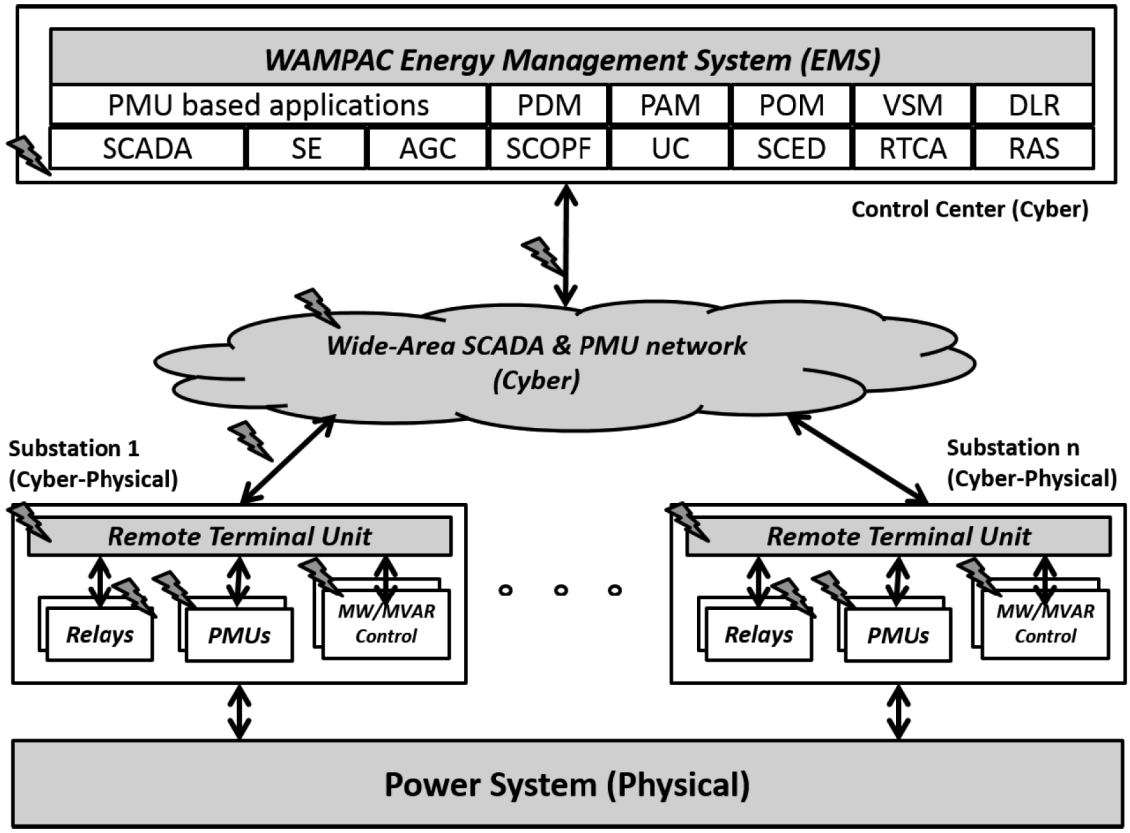

Fig. 1. ***High-level schematic of WAMPAC.***

known as the CIA properties. Specifically, for the purpose of this paper, we focus on the types of attacks that impact the integrity and availability of measurement and control data because they are considered to have a direct impact on the reliability and security of the bulk power system. Therefore, we classify the different types of cyber attacks for WAMPAC cybersecurity into one of the following categories: data integrity attacks, DoS attacks, time-based attacks, replay attacks, and coordinated attacks [14], [15].

- Data integrity attacks: Attacks that target either the measurements or the control signals, e.g., man-in-the-middle (MITM) attacks.
- DoS attacks: Attacks that flood a communication network or a specific host to delay or stop network traffic, causing an interruption of SCADA data availability.
- Timing-based attacks: Attacks that introduce arbitrary time delays in SCADA communication by varying latencies to cause unintended failures in SCADA availability or reliability.
- Replay attacks: Attacks that replay previous sequences of valid communication packets to deceive the SCADA applications. Typically, such attacks are hard to execute due to common replay protection features in some SCADA communication protocols.
- Coordinated attacks: According to the NERC High Impact Low Frequency (HILF) report, coordinated cyber attacks present a major threat to the reliability and security of the power grid capable of causing cascading blackouts on large portions of the system [16]. Coordinated cyber attacks represent a class of attacks where the adversary coordinates the attacks from multiple points in either space (spatial attacks), or in time (temporal attacks), or a combination of both. The coordinated attack vectors could take into account the system responses to initial disturbances and could cause secondary and tertiary events, which could steer the system into instability, eventually leading to a cascading failure scenario.

Fig. 2 shows the mapping of the different types of cyber attacks onto the various cyber resources such as the SCADA servers, human–machine interfaces (HMIs), historians, field devices, network infrastructure elements such as routers and switches, and network protocols. Fig. 2 further maps how these in turn impact the WAMPAC applications such as SE, AGC, RAS, etc., eventually leading to operational impacts, such as overloads, load loss, and economic impacts like locational marginal price (LMP) fluctuations.

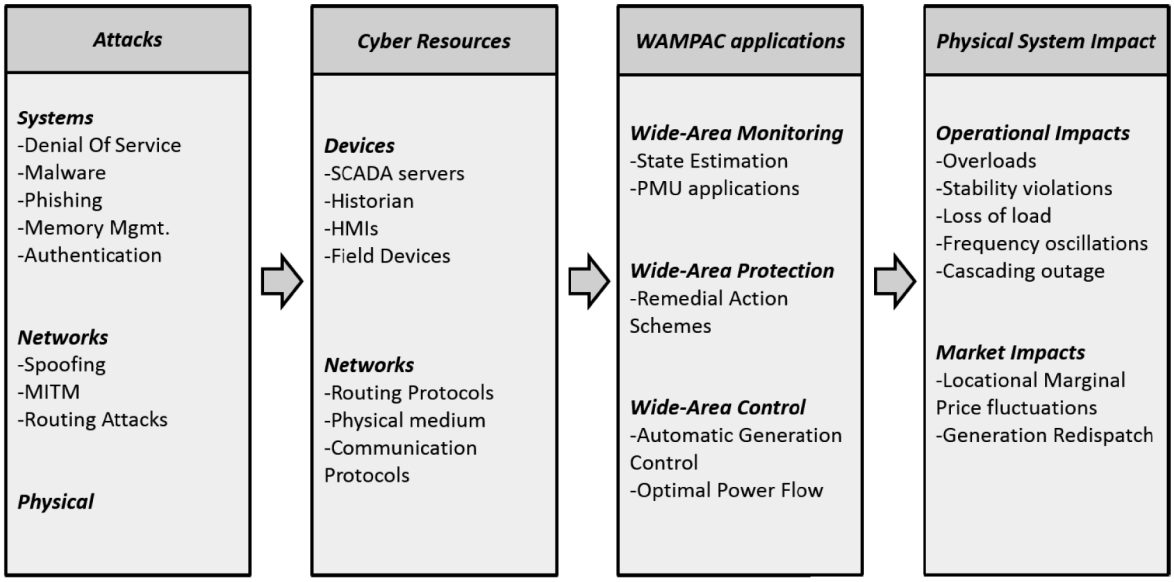

Fig. 2. ***Mapping from attacks to impacts on WAMPAC applications.***

III. END-TO-END ATTACK-RESILIENT CYBER–PHYSICAL SECURITY FRAMEWORK FOR WAMPAC

In this section, we describe an end-to-end cyber–physical attack-resilient framework for WAMPAC that extends across the spectrum of the various solution domains ranging from risk assessment to attack prevention, detection, mitigation, and resilience. Specifically, this section will provide a quick overview of an end-to-end security life cycle for cyber–physical attack resilience in the power grid and then explain in detail how the attack-resilient framework could be applied to address specific research issues on securing the WAMPAC applications in the grid.

Fig. 3 shows an end-to-end security life cycle for attack-resilient WAMPAC applications in the power grid through a hub-and-spokes model encompassing attack deterrence, attack prevention, attack detection, attack mitigation, attack resilience, and attack forensics. Attack deterrence is the ability of the defender to positively influence the potential adversary not to carry out attacks through laws, policies, treaties, or via the possession of offensive capabilities. Obviously, not every potential adversary can be deterred; in such cases, attacks from them must be prevented. Attack prevention is the ability of the defender to prevent attacks on the system via risk assessment, risk mitigation, security processes, technologies, and practices. NERC CIP compliance covers several aspects of attack prevention [8]. Not every attack is preventable (e.g., zero-day exploits); in such cases, those attacks must be detected online and suitable mitigations must be applied to maintain or gain operational status of the system without any degradation or violation in performance, stability, or operational security of the grid. It is important to note that not every attack can be detected and mitigated; in such cases, the system must have adequate resiliency to maintain or regain operational status, perhaps at a degraded level of performance, stability, or reliability. In the worst case scenario, some attacks may penetrate this end-to-end security chain (not deterred, not detected and mitigated, no resilience against) and cause damage to the system; in such cases it is useful to do forensic analysis to determine the source and originator of the attack. Such an analysis would help to deter future attacks. Traditionally, the problem of attack attribution has been very difficult to solve, because adversaries are always a step ahead of the defenders. Additionally, there are inherent challenges in performing live attack forensics on SCADA systems with diverse, and often legacy, hardware and embedded software, while attack deterrence typically ties to policies, laws, and offensive capabilities. Therefore, we will only elaborate on aspects from attack prevention through attack resilience as part of the framework for the rest of this paper.

Essentially, each spoke of the hub-and-spoke model highlights some of the innovative cyber–physical security approaches that leverage sound mathematical and scientific tools and enabling technologies to prevent the succession of attacks along the security life cycle. Fig. 4 shows the attack-resilient research framework for WAMPAC applications in the power grid. In particular, it shows how the various potential solutions at the different spokes in the security life cycle, namely, attack prevention, attack detection, attack mitigation, and attack resilience, fit into the WAMPAC conceptual architecture. The framework also includes the traditional SCADA measurements that are fed as inputs to the WAMPAC applications at the control center. Under the context of coordinated cyber attacks, these SCADA and

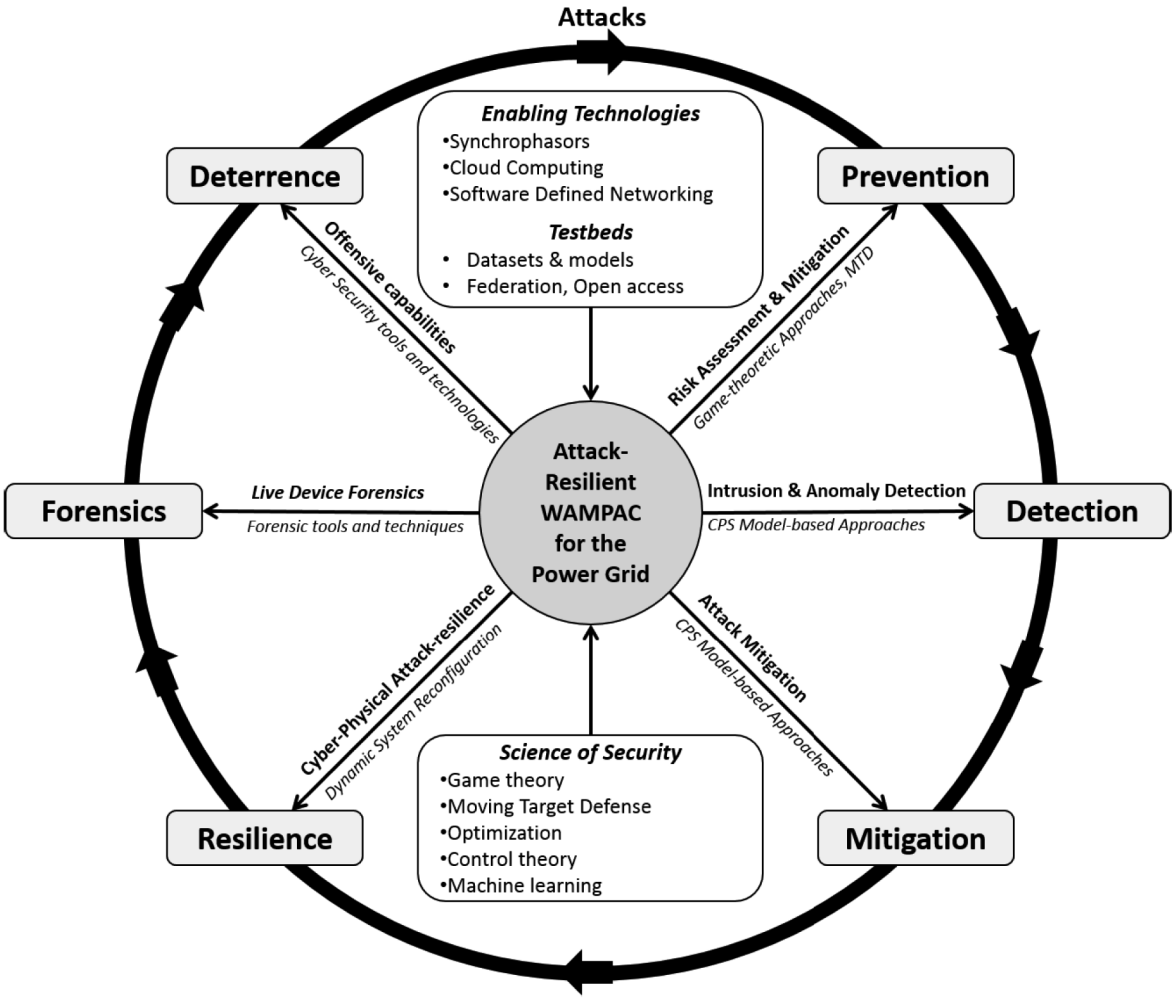

Fig. 3. ***End-to-end security life cycle for attack-resilient WAMPAC.***

PMU measurements (analog/status) could be subject to different types of cyber attacks such as data integrity, DoS, MITM, and replay attacks that adversely influence the outputs of the WAMPAC applications.

A. Attack Prevention

In the proposed framework, attack prevention would be achieved through a combination of multiple approaches: quantitative risk assessment, attack-resilient measurement design, and moving-target inspired algorithms.

Quantitative risk assessment involves modeling all the components of risk, namely, threats, vulnerabilities, and impacts, using approaches such as probabilistic or game-theoretic modeling. The use of game-theoretic tools allows some flexibility to adapt the modeling by allowing for different attacker models and behaviors in different settings, and provides a pragmatic method to characterize the impacts of different types of cyber attacks; it also helps to identify mitigation measures, either in terms of cyber layer security reinforcements or in terms of developing new operational planning approaches to reduce attack impacts, depending on problem formulation.

Attack-resilient measurement design involves algorithms that identify and recommend redundant measurement deployments that could be fed additionally into the WAMPAC applications, thereby increasing the difficulty of creating successful attacks. The optimal selection of redundant measurements is achieved by formulating a design problem that optimizes the placement of new sensors (e.g., PMUs) such that the accuracy, bad-data detection capability, and observability of the system improve while satisfying cost constraints.

Moving-target inspired algorithms leverage a redundant measurement design and randomize the associated design parameters at the WAMPAC algorithm level while still ensuring that the functionality of the algorithm is maintained.

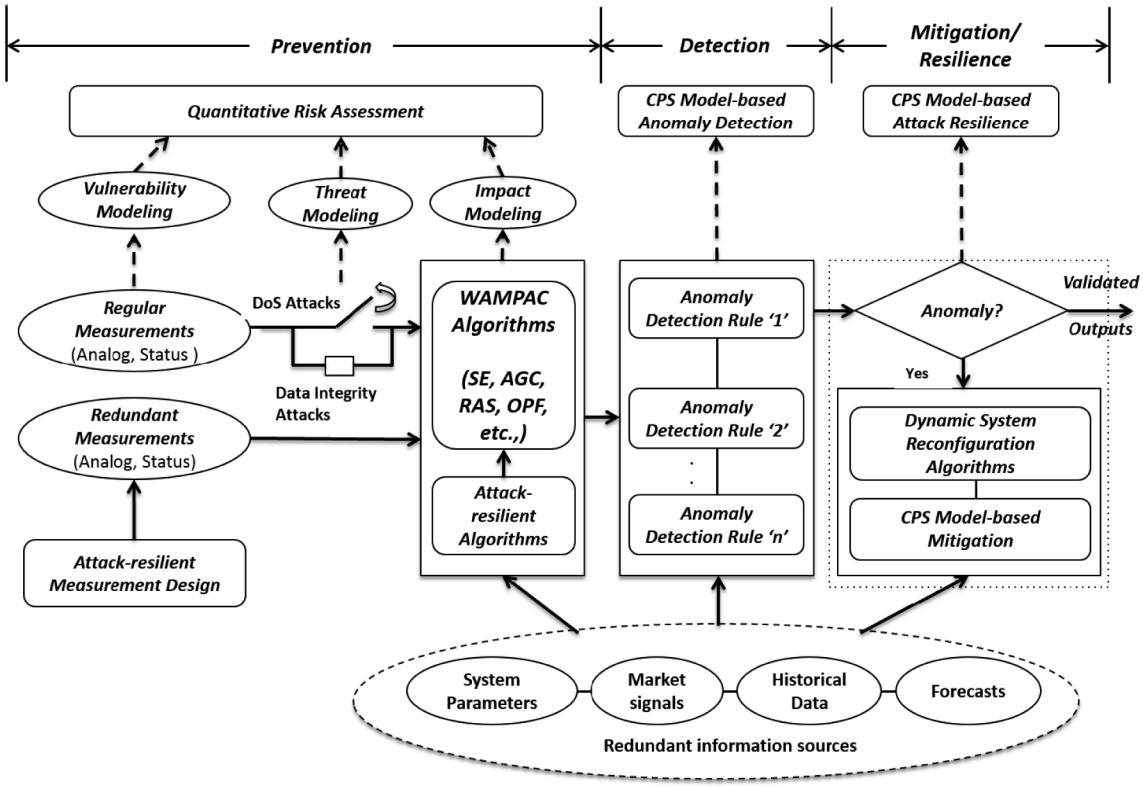

Fig. 4. ***End-to-end attack-resilient cyber–physical security framework for WAMPAC.***

B. Attack Detection

In the proposed framework, CPS model-based anomaly detection approaches that leverage sound mathematical tools from machine learning and related domains are critical for the detection of cyber attacks beyond traditional information technology (IT) intrusion detection techniques. Additionally, specification-based anomaly detection approaches serve a complementary role to CPS model-based approaches and enable the reduction of false positive rate by capturing the normal behavior and existing security policies as part of a formal specification or language.

1) CPS Model-Based Anomaly Detection: These approaches would essentially leverage information from independent and redundant information sources such as forecasts, historical data, weather, and market data. The output of traditional WAMPAC algorithms such as SE or AGC can be validated through several application-specific anomaly detection rules that capture the correlation between the actual and predicted data based on probabilistic or statistical characterization. This characterization defines the boundaries of when data is classified as an anomaly and typically involves tradeoffs between false positives and false negatives to achieve optimal performance.

2) Specification-Based Anomaly Detection: These approaches would rely on defining the existing communication behavior of the various system components at the protocol level through the form of a formalism such as an abstract specification language/grammar, regular expressions, finite state machines, Petri nets, etc. Existing specification-based anomaly detection approaches are able to capture, track, and validate the current state of the communications between system components as a result of a well-defined specification of the underlying communication protocol behaviors and sequences [17]–[20].

C. Attack Mitigation/Resilience

In the proposed framework, attack mitigation/resilience would be achieved using CPS model-based mitigation, and dynamic system reconfiguration and resiliency algorithms appropriately. These approaches would rely on sound tools from control theory to identify optimal system responses.

1) CPS Model-Based Mitigation: One of the aspects of attack mitigation/resilience in the proposed framework is the ability of the attack-resilient WAMPAC algorithm to recover from faults, either partially or completely. Based on the output of the anomaly detection module, if the data are considered "anomalous," a CPS model-based mitigation method would be triggered. This module typically would use a similar subset of redundant information (described earlier) to mask or recover from the measurement anomalies. For example, if the SCADA measurement data used by the AGC application are found to be untrustworthy, then

the control signal would be calculated based on a statistical model that uses short-term load forecast information along with system generation parameters to predict its most likely value for a particular balancing authority area until a redundant, trusted source of SCADA telemetry is restored.

2) Dynamic System Reconfiguration and Resiliency Algorithms: Another aspect of attack mitigation/resilience in the proposed framework is the ability to dynamically alter the configuration of the power system to minimize the effects of the attack on the grid. This type of countermeasures is critical for attack-resilient protection, where the failure of protection schemes like RAS could potentially cause cascading outages in a very short time frame. Examples of such dynamic reconfiguration and resiliency are intelligent islanding of the system and generation redispatch to relieve overloads. As part of the proposed research framework, software defined networking (SDN)-based cyber–physical approaches that involve a correlation of cyber and physical state information for WAMPAC and market applications would be explored. Also, various dynamic routing and network reconfiguration strategies would be analyzed by quantifying the latency and service interruption caused by them versus the security benefits offered by them in terms of reducing the attack surface on the fly [21].

IV. DEFENSE-IN-DEPTH ARCHITECTURE FOR ATTACK-RESILIENT WAMPAC

Transforming the "fault-resilient" power grid of today into an "attack-resilient" power grid of the future, capable of surviving sophisticated cyber attacks, requires an end-to-end comprehensive technical approach that incorporates both offline and online security measures across cyber, control, and physical layers of the system, leveraging CPS security properties at multiple levels for different attack classes. The electric grid's cyber–physical properties, legacy attributes of control systems, and physical redundancies must be incorporated in the development of smart grids tailored by a CPS security and resiliency approach. This section presents an overview of the proposed defense-in-depth research architecture that includes both infrastructure and application layer security measures at multiple levels for different attack classes.

Admittedly, there is no single unique solution or "magic bullet" to achieve resiliency for the future power grid against sophisticated attacks. Typically, a defense-in-depth approach focuses on multiple levels of security to defend against a class of attacks, whereas a defense-in-breadth approach addresses a combination of techniques and tools across technological, human, and supply chain domains to defend against multiple attack classes. The term defense-in-depth has been interpreted quite differently across the various domains it has been applied to since its original inception in the military [22]. However, the use of multiple layers of defense measures is a common aspect in all these interpretations. Another aspect of defense-in-depth is the ability to increase the cost of attacks for the adversary. While techniques such as moving target defense (MTD) could achieve this, they often utilize redundancy and diversity of solution tools and technologies, which could complement a "defense-in-breadth" approach. Therefore, these approaches are complementary and synergistic, and they need to be applied according to the problem addressed.

A comprehensive approach for securing the WAMPAC should involve this synergy of defense-in-depth and defense-in-breath approaches appropriately at different levels such as control center, substations, and the field devices such as the intelligent electronic devices (IEDs) to protect from and be resilient against a wide class of advanced cyber threats. Also, the suitability of defense-in-depth versus defense-in-breadth approaches is often influenced by the various tradeoffs such as security versus usability, security versus performance, and security versus cost. For example, if multiple layers of security such as encryption are added, authorization on a highly time-critical wide-area protection application would strengthen the security, but it could lead to violation of real-time constraints. For the purposes of this paper, the term "defense-in-depth approach" refers to a combination of multiple layers of defense measures at multiple levels (control center, substations, IEDs) using a combination of traditional IT infrastructure layer and application layer security measures appropriately. This definition captures some of the essential aspects of both the approaches mentioned previously.

Fig. 5 presents an overarching defense-in-depth architecture for attack-resilient WAMPAC. This architecture takes into account both the cyber and physical characteristics of the power grid by combining efforts to prevent, detect, mitigate, and be resilient to cyber attacks at both the infrastructure and applications layers. Fig. 5 shows how the measurements from the SCADA and PMU networks are screened at the infrastructure layer by traditional cybersecurity mechanisms such as intrusion detection systems, firewalls, etc. As a next layer of defense at the application layer, the framework consists of cyber–physical attack resilience that is incorporated into some of the fundamental applications in WAMPAC, namely, SE, AGC, and RAS.

A. Infrastructure Layer Attack Resilience

Fig. 6 presents the pertinent research issues and potential solutions for achieving attack resilience at the infrastructure layer for WAMPAC. The various issues are listed across the various solution domains, namely, offline risk assessment, attack prevention, and online attack detection, mitigation, and resilience. In order to have resilience at multiple layers in alignment with the defense-in-depth architecture, it is essential to leverage existing and emerging

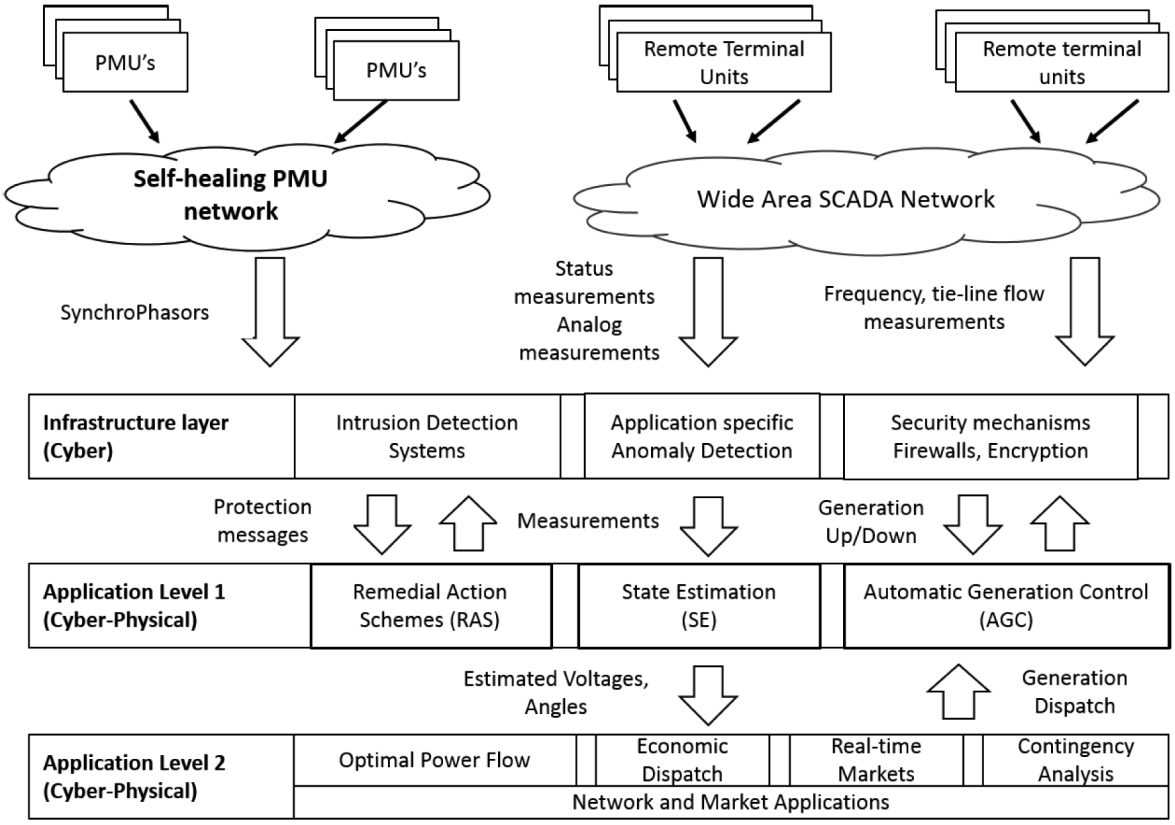

Fig. 5. ***Defense-in-depth architecture for attack-resilient WAMPAC.***

infrastructure-layer security measures to complement application-layer security approaches. We have listed some of the most pertinent research issues and potential solution approaches in infrastructure layer attack resilience here for the sake of completeness, but the primary focus of this paper is to elaborate on application-layer cyber–physical attack resilience.

1) Risk Assessment: Conceptually, there are two main approaches to assessing risk, namely, qualitative and quantitative approaches. Qualitative risk assessment typically involves categorizing the known risks into discrete ranges according to the probability of each event and its consequence in order to create a risk matrix [23]. Based on the risk matrix, a risk rating can be obtained for each risk as a low-, medium-, or high-risk event. This serves to prioritize the identified risks and undertake appropriate risk mitigation measures to reduce residual risk. Qualitative risk assessment is easier to perform because it is based on operational experience and does not rely on obtaining accurate probability values for the various risks, which are often considered hard to quantify and standardize.

Quantitative risk assessment, on the other hand, attempts to model the behavior and interaction of the system using mathematical models in order to evaluate the risk and provide relative risk prioritization [24]–[26].

Risk can be defined as the product of the threat of a particular attack, the probability that a particular vulnerability is exploited to execute that attack, and the impact it has on the system [27]

$$\text{risk} = \text{threats} * \text{vulnerabilities} * \text{consequences}. \quad (1)$$

Threats originate from the various threat actors who could potentially attack the system. Threats essentially represent the probability that a particular threat actor would perform an attack. The various threat actors include script kiddies, hacktivist groups, disgruntled employees, malicious insiders, terrorist organizations, and rival nation states. Vulnerabilities represent the weaknesses in the cyber system devices, communication protocols, and software that could be exploited by the threat actors to perform a certain type of cyber attack. The exploited vulnerabilities could cause various types of consequences on the physical power system such as line overloads, voltage violations, unstable operating conditions, physical equipment damage, and even large-scale cascading blackouts.

Threats could be explicitly modeled using game-theoretic tools, because they capture human behavior and preferences better than other probabilistic approaches. Depending on how the game-theoretic model is formulated, the outcome of the game varies, and this translates

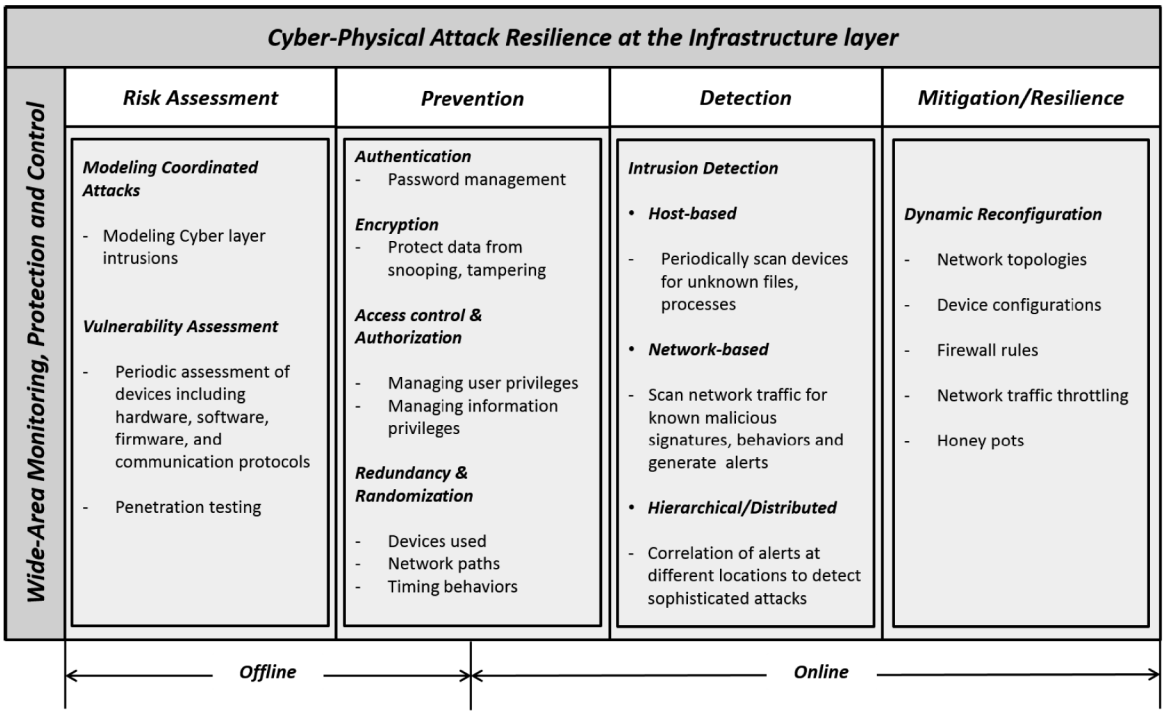

Fig. 6. ***Infrastructure layer attack resilience.***

into identifying the threats of various possible attack actions for specified attacker behavior and preferences [28]. From a practical perspective, threat modeling using game-theoretic tools is reliant on input data (probabilities) about sophisticated attacker behaviors [29], [30], which is extremely difficult. Obtaining realistic and meaningful input data for threat modeling remains an unsolved and open issue for most of the mathematical approaches. Therefore, most of the game formulations often rely on simplifying assumptions to leverage available empirical data [31].

Vulnerabilities could be quantified as steady-state probabilities of certain types of events that affect grid reliability. Therefore, vulnerabilities are modeled by representing cyber system models and security mechanisms, such as password protection, firewalls, intrusion detection systems, etc., along with the specific application layer interactions, using mathematical modeling tools such as petri nets [25]. The probability values for vulnerabilities in the cyber network are typically obtained through empirical and/or simulation studies.

Impacts are modeled and quantified through power system simulations to obtain metrics that can be converted into cost. Examples of impact metrics that could be converted to cost are load lost, which could be converted into cost by multiplying it by the LMPs. Similarly, the other impact metrics could be quantified depending on the specific use case being considered.

Most of the existing quantitative approaches often neglect "threats" as part of the modeling because they are dependent on human behaviors that are hard to quantify. Therefore, risk is often modeled as just a product of vulnerability and impacts. Because the steady-state probability information that represents vulnerabilities is based on empirical data, there is no single range of risk values that could be considered acceptable. However, quantitative risk assessment approaches provide a relative ranking of risks that could be used to set acceptable thresholds. This would help guide optimal investments to secure the system and minimize the residual risk.

2) Attack Prevention: Attack prevention typically involves a combination of authentication measures, access control, and authorization that manages user and information privileges for the various SCADA systems, and data encryption measures, wherever permissible, to protect from snooping and tampering. In addition, attack prevention could be achieved by exploiting redundant infrastructure elements (e.g., devices, network paths) to randomize the communication patterns and timing behaviors based on MTD-inspired approaches to prohibitively increase the cost of the attacks for the adversary [32], [33].

3) Attack Detection: Attack detection at the infrastructure layer typically involves the deployment of intrusion/anomaly detection systems (IDSs) that are host based, network based, or a hierarchical/distributed implementation where the individual alerts from different IDSs could be correlated in a security information and event management

(SIEM) software to identify coordinated attacks based on a combination of cyber layer information along with the physical system state information [34]–[38].

4) Attack Mitigation and Resilience: Attack mitigation and resilience involves dynamically changing the configuration of infrastructure elements like device configurations, network topologies, firewalls, traffic filtering, and honey pots. Also, in certain cases, several IDSs consists of features that provide some sort of active defense capabilities like dynamically modifying firewall rules, etc., that would classify them as intrusion prevention systems [34], [35], [39], [40]. Some of the existing efforts in this area have looked at the concept of SDN to implement one or more of these features [41], [42].

B. Application Layer Attack Resilience

Fig. 7 presents the pertinent research issues and potential techniques that could be applied to achieve attack resilience at the application layer for WAMPAC. Similar to the infrastructure layer, the various research issues are listed across the solution domains from risk assessment to attack mitigation/resilience.

1) Risk Assessment: Risk assessment is performed offline and typically involves modeling the different types of coordinated attacks such as data integrity attacks, DoS attacks, MITM attacks, and replay attacks on the different types of measurements and control commands. One of the key requirements for application layer risk assessment is integrated modeling of the different aspects of risk, namely, threats, vulnerabilities, and impacts, considering the cyber and physical system interactions together. The potential techniques for offline quantitative risk assessment include probabilistic models [26], stochastic petri-net-based models [25], and game-theoretic models [24].

In order to get some intuition about quantitative risk assessment and how each of the three components in the risk equation [see (1)] can be modeled, let us consider a simple example: the risk assessment for tripping of transmission lines by an attacker. For the sake of simplicity, let us consider only lines at two different substations. Let us also assume that an attack on substation 1 is more impactful than one on substation 2, because attack on substation 2 creates only a temporary failure. However, we also assume it is stealthier than the first attack due to the nature of the cyber components involved.

The steady-state probabilities for compromising the relays in substations 1 and 2 are obtained by modeling the cyber layer explicitly, and this involves the substation firewalls, the network switches, and the relays. Based on the specific device characteristics, each substation has probabilities for the attack scenario, which is the tripping of the relay in that substation.

In terms of impact, depending on the way the generation was dispatched, the two attack scenarios would have varying impacts. We could simply utilize the magnitude of load loss as an impact metric. A simple power flow solution or

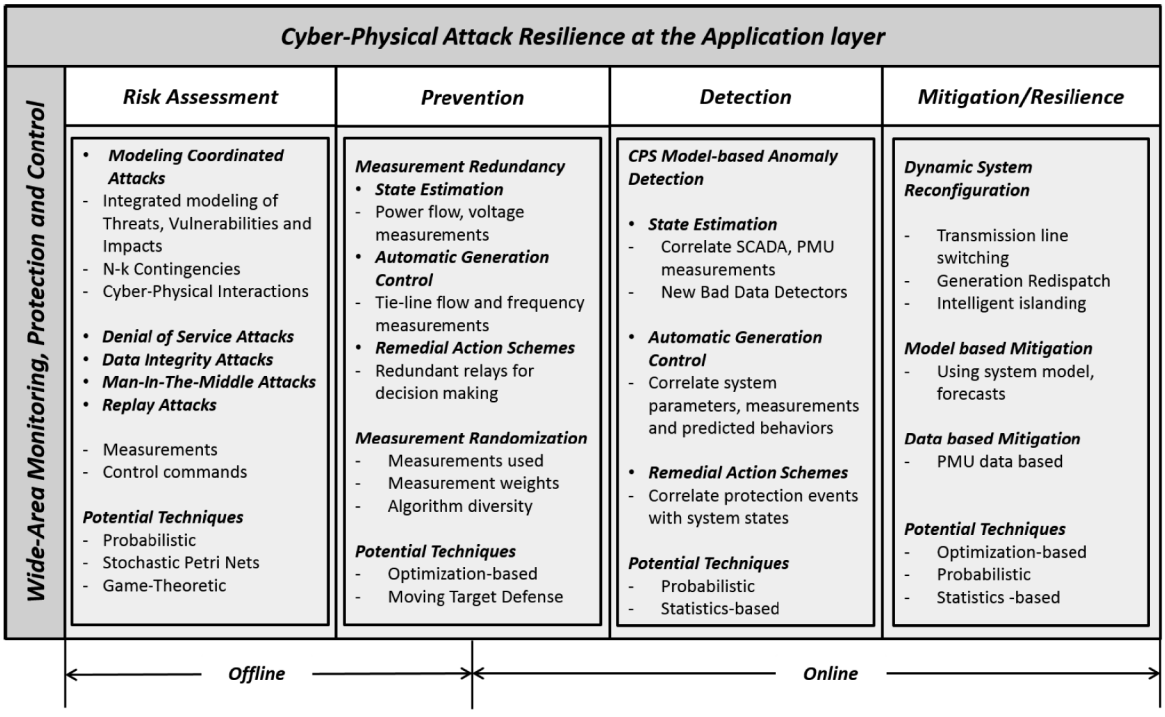

Fig. 7. ***Application layer attack resilience.***

time-domain simulation for the two attack scenarios would provide the values for the impact metric.

In order to model threats, we need to capture the preferences of the attacker in the modeling. This could be accomplished in a strategic game with cost functions that indicate relative preference. In our case, we can assume two specific attacker types: 1) the attacker prefers maximum impact; and 2) the attacker prefers stealthier attack. Effectively, this translates into two different cost functions for the attacker, and depending on the equilibrium solution of the strategic game, the attacker would choose one attack action over the other (tripping of relays either in substation 1 or substation 2). The equilibrium solution provides the values for the threat component of risk. Once we have these three individual components, we can obtain risk values that are specific to an attacker type and behavior for each of the two attack scenarios. A similar intuitive example is explained in more detail in [28].

2) Attack Prevention: Attack prevention at the application layer could be translated into having enough redundancy and diversity in the measurements that the attacker needs to compromise more devices in order to create a sophisticated, stealthy, and impactful cyber attack. The redundancy/diversity in measurements varies for different WAMPAC applications. For example, in SE it corresponds to increasing the status and analog measurements to detect and validate the existing measurements. Similarly, in the case of AGC algorithms, it corresponds to having more tie-line and frequency measurements. In the case of RAS, it corresponds to having multiple relays for decision making. If the system is designed with adequate redundancy, then measurements that are used as part of the specific WAMPAC algorithm or even some variations of the algorithm could be randomized such that the normal functioning is not affected. This would partially eliminate certain attack vectors by making it difficult for the attacker to create an impactful attack. The potential techniques for attack-resilient measurement design would be based on optimization theory and MTD for measurement randomization [43], [44].

3) Attack Detection: Attack detection at the application layer involves the development of CPS model-based anomaly detection algorithms that leverage certain redundant information sources such as system parameters, historical data, forecasts, market signals, etc., to develop WAMPAC application-specific anomaly detection rules that are complementary to traditional infrastructure-based anomaly/intrusion detection algorithms. Using the anomaly detection rules, existing SCADA and PMU measurements could be correlated to detect malicious measurement anomalies. The potential techniques for attack detection would be based on system specifications or probabilistic and statistical characterizations to detect anomalies [45], [46].

4) Attack Mitigation and Resilience: Attack mitigation and resilience at the application layer involves protection of the system reliability during extreme attacks where existing prevention and detection measures are inadequate. This involves approaches that dynamically change the system configuration in order to manage or prevent the attack impacts from causing major cascading outages. This could be achieved, for example, by dynamically changing the system topology, dispatching generation to relieve overloads, or intelligently islanding certain parts of the system. Another aspect of attack mitigation/resilience involves the use of CPS model-based and PMU data-based mitigation approaches as a backup for performing critical functions of WAMPAC applications. The potential techniques for attack mitigation/resilience would be based on optimization theory and probabilistic and statistics-based methods [46].

V. ATTACK-RESILIENT WAMPAC ALGORITHMS

This section will present a detailed discussion on specific research issues that are relevant to key WAMPAC applications, and also on how such an attack-resilient framework could be applied to develop solution approaches along various stages of the security life cycle for each of the individual aspects of WAMPAC, namely, wide-area monitoring, wide-area protection, and wide-area control separately.

As a general note, we would like to mention that many of the emerging WAMPAC applications rely heavily on the availability and integrity of widespread PMU data. Existing research counts on PMU data being part of solutions to cyber–physical security problems in the power grid. However, to the best of our knowledge, not enough work has been done to identify potential vulnerabilities, impacts, and solutions when PMU data are compromised. This remains one of the critical aspects in cyber–physical security of WAMPAC that warrants increased attention from the research community in the next decade. Therefore, we chose to focus the rest of the discussion on research issues and solutions that address existing and common WAMPAC applications, although some of the research issues and potential solutions apply equally to the new PMU-based WAMPAC applications as well.

A. Wide-Area Monitoring

1) Research Issues: State estimators and several other WAM applications generally rely on accurate and timely analog and status measurements from remote substations for proper operation. Given that several of the traditional EMS applications rely heavily on the output of state estimators, securing them against cyber attacks is extremely critical. Much current and recent work has looked at what the stealthy attack vectors are in SE that go beyond existing detection methods [47]–[53]. These stealthy attack vectors target not only the analog measurements [47], but also the status measurements, leading to incorrect system topology being used for SE [54], potentially causing incorrect control decisions. Existing research also identifies various attack

impacts on SE [47], operational metrics like system operating limits [54], and market impacts such as LMP fluctuations [53]. Some of the recent literature in this area also addresses the attack-prevention [48]–[50], [55], and attack-detection aspects [45], [52], [56] to incorporate cyber–physical attack resilience for the state estimator.

2) Potential Solutions:

Attack-resilient measurement design: One of the attack prevention measures for SE could involve attack-resilient measurement design, i.e., the optimal placement of new measurements, e.g., PMUs, in the system such that the system observability, bad-data detection capabilities, and detection accuracy are improved with the smallest number of new measurements added and at the lowest possible cost [43], [57]–[60].

Fig. 8 presents a simple example using the IEEE 9-bus system to illustrate how this would work. The solid squares indicate existing power flow measurements and the arrows indicate injection measurements. All these measurements together form the existing measurement set. Under normal conditions, these measurements should provide observability and bad-data detection. However, during attacks these may not be adequate. Therefore, the attack-resilient measurement design (ARMD) process would take into account the existing measurement set along with the operating conditions and attack scenarios to identify the locations of the new measurements to increase redundancy of the existing measurement set at the lowest possible cost for several possible scenarios including loss of one or more substation RTUs due to cyber attacks [43]. As part of our detailed analysis in [43], we performed a case study with the IEEE 14-bus system and obtained measurement placement for all possible scenarios that included loss of all measurements from an RTU or from two RTUs simultaneously. For a baseline measurement set that included 21 measurements, the ARMD methodology provided a minimal-cost solution with 12 additional measurements for ensuring observability during attacks that involve loss of up to two RTUs. The new measurement set not only provides redundancy, it also improves bad-data detection capabilities to detect false-data injection attacks. As shown in the end-to-end attack-resilient framework diagram (Fig. 4), the ARMD process increases the attack resilience of WAMPAC algorithms by increasing the redundancy of the measurement set, thereby also increasing the difficulty of executing a stealthy attack.

Attack-resilient algorithms: Another attack prevention measure for SE is using the concept of MTD, where the measurement redundancy is exploited to create a dynamic measurement configuration every time the algorithm is run. This involves the potential randomization of measurements that are used in the estimation process while maintaining the system observability in order to increase the difficulty of executing a stealthy attack [44].

CPS model-based anomaly detection: Attack detection in the case of WAM applications like SE would involve using information that is independent of traditional SCADA measurements to correlate and validate them. This would complement the existing bad-data detection methods and would help in the detection of stealthy attacks that could otherwise go undetected. For example, information from existing PMUs could be leveraged in conjunction with other information like historical and forecast data to characterize the variation of conventional state estimates and this information could be used to detect malicious measurement modifications [45].

Fig. 9 uses the same IEEE 9-bus system to provide a basic intuition about how model-based anomaly detection could be applied to detect stealthy attacks on state estimators. The existing measurements (solid squares and arrows) are sent to the control center EMS through a wide-area

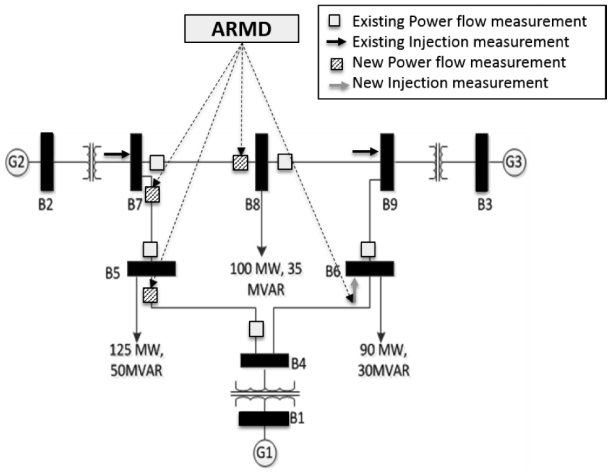

Fig. 8. ***Attack-resilient measurement design–illustrative example.***

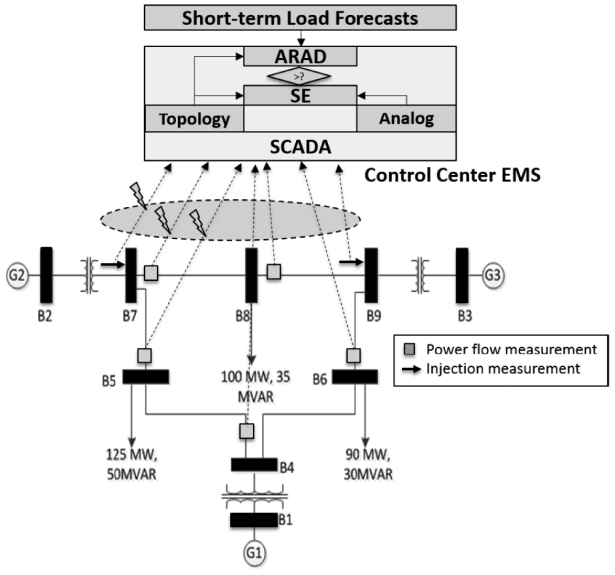

Fig. 9. ***CPS model-based anomaly detection–illustrative example.***

communication network and could be subject to stealthy false-data injection attacks. Typically, these data are used by the state estimator to produce estimates, and this is done by building network topology from status measurements and then feeding it along with the analog measurements into the state estimator. As part of attack-resilient anomaly detection (ARAD) methodology, information from load forecasts would be used in conjunction with the system model and the network topology to predict the system states for comparison with state estimates. Anomalies in state estimates could be identified by performing a statistical characterization of the difference between the predicted and actual state estimates using available historical data. As part of the ARAD approach, an empirical methodology to select the design parameters of the algorithm while ensuring very low false positives and false negatives is also described [45]. The ARAD approach relates to the idea of leveraging independent sources of information to potentially detect anomalies and increase attack resilience as identified in the end-to-end attack-resilient WAMPAC framework diagram (Fig. 4).

Fig. 10 shows how the proposed ARAD methodology is able to identify stealthy attacks on the system state variables by leveraging the statistical characterization. The top and bottom subplots show the difference between the predicted states and actual state estimates for one specific state variable for an entire day (288 samples), where each sample corresponds to a 5-min interval when SE is executed. In this experiment, we have performed the attack during only a part of the day and the attack period can be easily identified using the dotted lines between sample numbers 50 and 200. The solid, dotted, and dotted–dashed lines indicate the mean, standard deviation (SD), and 1.25 * SD of the differences between predicted state estimates and actual state estimator outputs, respectively. This is obtained by using historical load forecast and SCADA data. As we can see in the top subplot, without the attack, the differences between predicted estimates from ARAD and the state estimator outputs fall within the thresholds identified by statistical characterization. In the bottom subplot, we can see that the differences between predicted and actual state estimates fall outside the thresholds identified, enabling the detection of the stealthy attacks. More detailed experimental results are presented in [45].

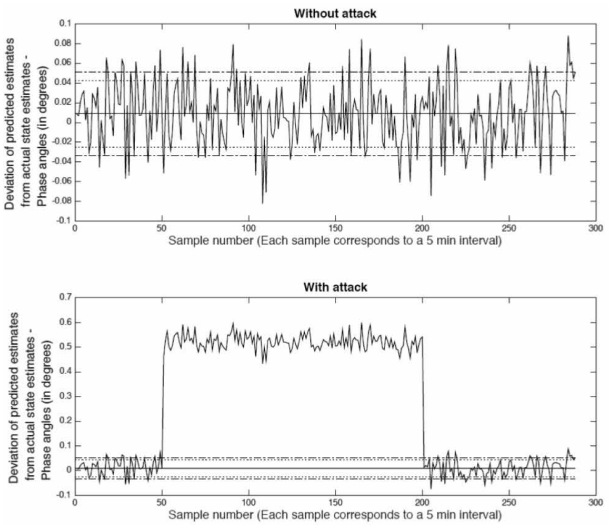

Fig. 10. ***Detection of stealthy attacks using ARAD.***

CPS model-based mitigation: In the case of SE, attack mitigation/resilience could be achieved by exploiting the measurement redundancy and ignoring measurements that were detected as anomalous by the anomaly detection algorithms. In certain cases, the removal of faulty measurements in the measurement set could cause a loss of observability and this would be typically handled with the addition of pseudomeasurements. These measurements are typically estimated from historical values and load forecasts. As the pseudomeasurements are generally less accurate than regular measurements, such an approach could also involve the optimal adjustment of measurement weights in order to minimize the impact on the state estimates.

B. Wide-Area Protection

1) Research Issues: The inherent reliance on wide-area communication and relay coordination of wide-area protection schemes [61] presents several vulnerabilities in terms of possible cyber intrusions to hinder or alter the normal functioning of these schemes. Therefore, it is critical to analyze how different types of cyber attacks impact the operation of the RAS and develop suitable countermeasures to mitigate the attacks. The existing literature has shown the vulnerability of RAS and other protection schemes to various types of cyber attacks and their impacts [62]–[66]. Considering the sensitivity of protection schemes to strict timing requirements, potential attack vectors could involve a combination of data-integrity and DoS attacks, as described in [62], leading to the possibility of cascading outages on the grid. Also, addition of more and more wide-area protection (WAP) schemes to the power system introduces unexpected dependencies in the operation of the various schemes, and this increases the risk to the system from cyber attacks. It therefore becomes critical to reexamine the design of the WAP schemes with a specific focus on cyber–physical security.

2) Potential Solutions:

Attack-resilient measurement design: Attack prevention in particular will be achieved through redundant relay deployments for monitoring and mitigation in the RAS, associated communication channels, and coordination functions with suitable validations so as to ensure there is no single point of failure in the protection scheme.

Attack-resilient algorithms: Another aspect of attack prevention would involve randomization of relay coordination functions (e.g., randomly selecting a subset of relay communications from the redundant set for decision making, randomizing the timing of the device interactions within the latency constraints) so as to prevent the adversary from easily inferring the actual RAS operation accurately.

Fig. 11 shows the IEEE 9-bus system to provide some insights on attack-resilient protection algorithms. In this figure, we have a redundant set of protection relays (indicated by the shaded and solid white squares) and RAS controllers (RAS C) at the control center EMS for a wide-area protection scheme. These components along with the generation controller (GC) are part of a generation reduction RAS that reduces generation when one of the two relays connected to substation at bus 7 trips out. As part of normal operation, only one set of relays, either the shaded or the solid white ones, is used as primary devices. The same is the case with the RAS controllers. The attacker could potentially leverage the static communication patterns and device configurations to trigger the RAS and block device communications during the RAS to cause further impacts to grid stability. But if the active set of devices that serves as primary for the RAS could be randomly chosen based on MTD approaches, the difficulty of executing an attack would be increased. This type of solution approach would increase attack resilience through dynamic system reconfigurations that do not impede critical operational functions as identified in the attack-resilient WAMPAC framework (Fig. 4).

CPS model-based anomaly detection: Attack detection would incorporate spatial and temporal characteristics of substation automations (e.g., relay reclosure timings, relay fault zone coverage) and communications (e.g., relay coordination) together with physical system properties to identify potential cyber attacks. This would be implemented through a two-level hierarchical anomaly detection system: substation-level (level 1) detection of communication and physical anomalies pertaining to relay protection functions, and system-level (level 2) correlation of substation alerts and wide-area communication pertaining to system protection functions to detect system-level anomalies, including coordinated malicious cyber events.

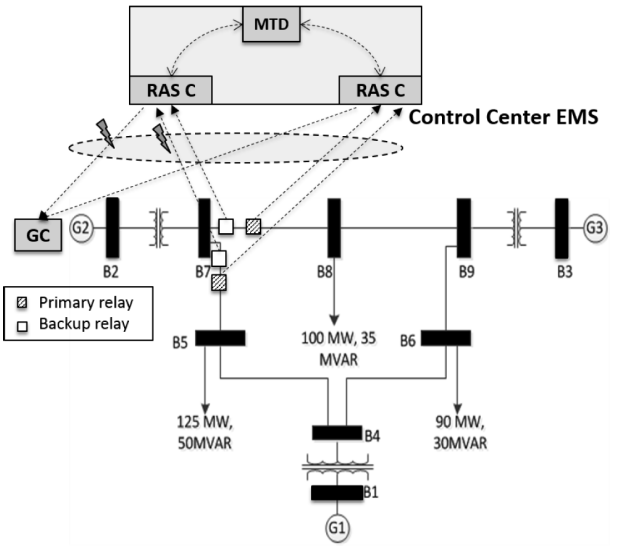

Fig. 11. ***Attack-resilient protection–illustrative example.***

Dynamic system reconfiguration: For a WAP application such as RAS, attack mitigation/resilience would involve a quick dynamic reconfiguration of the power system to prevent the propagation of the attack impacts. This could potentially include isolating the faulted portion of the system in the form of intelligent islanding schemes, transmission line switching to relieve overloads and eliminate stability violations, and/or generation redispatch, whichever seems acceptable and applicable to the utility operations considering the specific attack scenario.

C. Wide-Area Control

1) Research Issues: Similar to the WAM applications, the AGC algorithm leverages the wide-area communications infrastructure of SCADA to obtain tie-line and frequency measurements at the control center, and issues control commands based on the area control error (ACE) values to the generating units [12]. Quite often, these measurements are obtained from sensors in remote, unmanned substations. This makes the sensors susceptible to compromise. Several efforts have studied the impact of data integrity attacks on AGC [46], [67]–[69]. Similarly, the impact of data integrity attacks on voltage control application has been analyzed in [70].

2) Potential Solutions:

Measurement/algorithm randomization: Randomization of tie-line or frequency measurements for AGC or of voltage measurements for secondary voltage control could ensure that even if certain devices are compromised, the measurements originating from them may not necessarily be used to calculate the control signals. Similarly, developing alternative algorithms and randomly selecting one during operation could render an attack strategy ineffective.

CPS model-based anomaly detection: The inputs feeding into the WAC algorithm are dependent on several factors such as time of day, weather, time of year, etc. Hence, the algorithm should be able to dynamically adjust bad-data detection rules according to the system conditions. The need is to develop algorithms for characterization of inputs based on existing system conditions. Attack detection should also include methodologies to distinguish measurements corrupted by cyber attacks from measurements observed during normal disturbances. This is critical because incorrect mitigation dispatched during normal system disturbances could further degrade performance.

CPS model-based mitigation: The mitigation algorithms should take advantage of physical system information in order to identify the best strategy to restore the system. For example, the ramp rates of generators could be useful in attack scenarios where the system generation has deviated from optimal. The mitigation algorithm could dispatch fast-acting units in order to quickly reestablish generation–demand balance. Research efforts should focus on improving forecast techniques and exploiting forecasts to operate mitigation strategies. The mitigation should include methods to identify compromised sensors and eliminate them from the computation of control signals. By using a combination of forecast-aided measurements for compromised sensors and actual system measurements from a set of trustworthy sensors, the error introduced by inaccurate load forecasts could be significantly reduced.

Fig. 12 shows the IEEE 9-bus system with measurements and control areas to illustrate how the attack-resilient control (ARC) algorithm detects and mitigates stealthy attacks on AGC. The solid white and gray squares indicate frequency and tie-line flow measurements, respectively, for control area 1. The AGC algorithm running on the control center EMS for area 1 typically computes its real-time ACE (ACE_{RT}) using the tie-line and frequency measurements identified. A smart attacker could manipulate the tie-line and frequency measurements consistently to remain undetected in the basic bad-data detection checks in the EMS. Therefore, in order to detect such anomalies, ARC uses short-term load forecasts to predict possible ACE ranges (ACE_{LF}) for the current operating period and uses that for validating ACE_{RT}.

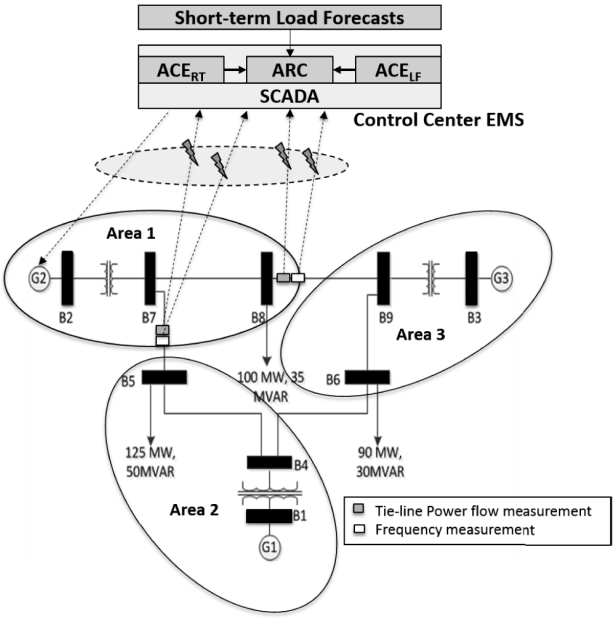

Fig. 12. ***CPS model-based anomaly detection and mitigation–illustrative example.***

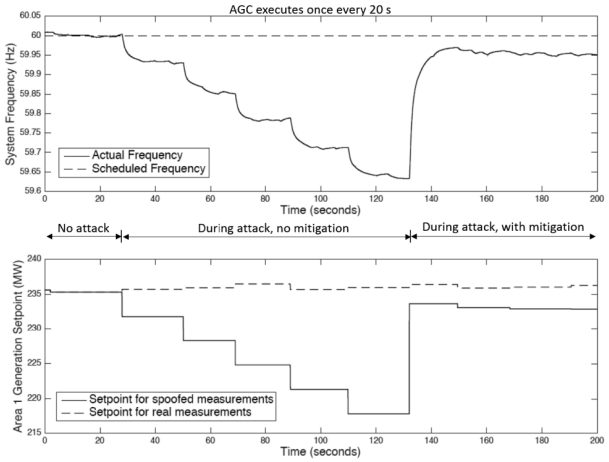

Fig. 13. ***Stealthy attack detection and mitigation by ARC.***

If anomalies are detected, then the ARC algorithm uses forecast-based ACE, ACE_{LF}, as mitigation [46].

Fig. 13 shows results from an experimental case study on the IEEE 9-bus system, where the AGC measurements for area 1 are subject to a stealthy attack that tries to push the system frequency away from 60 Hz to cause load shedding. As a part of this case study, AGC is executed once every 20 s. As indicated in the figure, the results actually show three phases, namely, before attack, during attack without any mitigation, and during attack with ARC mitigation. In order to show the impact of the attack, we have plotted system frequency (top subplot), and area 1 generation set points (bottom subplot). Before the attack, we can see that the frequency is close to 60 Hz, and correspondingly the total generation in area 1 matches the load plus net tie-line power flow export. However, during the attack, the actual frequency drops due to incorrect generation signals sent to area 1. In order to clearly show how the spoofed tie-line power flow measurements and frequency measurements bias the AGC to continually issue generation ramp down commands, we have plotted the set points due to both spoofed and actual measurements in the bottom subplot. During the attack, we can clearly observe that the attacker is able to deceive the AGC algorithm into believing that there is excess generation. Therefore, during the attack phase without the mitigation, we can see that the AGC reduces area 1 generation from its ideal set points, leading to a decline in frequency. In order to show the effectiveness of the ARC algorithm, we activate the mitigation around 130 s, after which we can see that the Area 1 generation is restored based on load forecasts, and consequently the system frequency is restored to values much closer to 60 Hz. More detailed experimental results can be found in [71]. Through this case study, we can see how such a solution approach leverages CPS model-based

anomaly detection and mitigation as described in the attack-resilient WAMPAC framework (Fig. 4).

VI. CONCLUSION

In this paper, we have made three key contributions to enhance the cybersecurity and resiliency of WAMPAC. First, we outline an end-to-end attack-resilient cyber–physical security framework for WAMPAC applications in the power grid. Specifically, the attack-resilient framework addresses the entire security life cycle including risk assessment, attack prevention, attack detection, attack mitigation, and attack resilience. Second, we describe a defense-in-depth architecture that incorporates attack resilience at both the infrastructure and the application layers. This layered defense architecture for WAMPAC leverages domain-specific security approaches at the WAMPAC application layer in addition to traditional cybersecurity measures at the IT infrastructure layer. Third, we identify pertinent cyber–physical security research issues for key WAMPAC applications and describe several attack-resilient algorithms leveraging measurement design and CPS model-based anomaly detection and mitigation to address the research issues identified. We also provide illustrative case studies to provide fundamental insights into various attack-resilient prevention, detection, and mitigation algorithms. The research issues and potential solutions identified in this paper open up several avenues for future research in this area. The proposed framework, architectural concepts, and attack-resilient algorithms would serve as essential building blocks to transform the "fault-resilient" grid of today into an "attack-resilient" grid of the future. ■

Acknowledgement

The authors would like to thank the U.S. Department of Energy Office of Electricity Delivery and Energy Reliability's Cybersecurity for Energy Delivery Systems (CEDS) Program for providing funding to develop some of the core technical content in this paper. Also, they would like to acknowledge the valuable inputs and comments from S. Sridhar (PNNL), D. McKinnon (PNNL), S. Shamsuddin (ANL), P. Wang (ISU), and several industry experts for helping shape the overall technical approach described in the paper.

REFERENCES

[1] (2016). *The Smart Grid: An Introduction US Department of Energy* [Online]. Available: http://energy.gov/oe/downloads/smart-grid-introduction-0

[2] S. Baker, S. Waterman, and G. Ivanov, "In the crossfire: Critical infrastructure in the age of Cyber War," McAfee, Santa Clara, CA, USA, Tech. Rep., 2009.

[3] U.S. Government Accountability Office. (Jan. 2014). *Critical Infrastructure Protection: More Comprehensive Planning Would Enhance the Cybersecurity of Public Safety Entities' Emerging Technology* [Online]. Available: http://www.gao.gov/assets/670/660404.pdf

[4] Industrial Control Systems Cyber Emergency Response Team (ICSCERT). (Aug. 2016.). *ICS-CERT Monitor Newsletters* [Online]. Available: https://ics-cert.us-cert.gov/monitors

[5] SANS Institute and Electricity Information Sharing and Analysis Center (E-ISAC). (Mar. 2016). *Analysis of the Cyber Attack on the Ukrainian Power Grid—Defense Use Case* [Online]. Available: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

[6] NERC Critical Infrastructure Protection Committee (CIPC) Cyber Attack Task Force (CATF)—Final Report, North Amer. Electr. Rel. Corp. (NERC), May 2012.

[7] Roadmap to Achieve Energy Delivery Systems Cybersecurity, U.S. Dept. Energy, MD, USA, 2011.

[8] North American Electricity Reliability Council (NERC). (2016). *Critical Infrastructure Protection (CIP) Standards* [Online]. Available: http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

[9] "NISTIR 7628 Revision 1: Guidelines for smart grid cyber security—Smart grid Cyber security strategy, architecture, and high-level requirements," Nat. Inst. Standards Technol. (NIST), Tech. Rep., Sep. 2014.

[10] National Electric Sector Cybersecurity Organization Resource. (Oct. 2012). *(NESCOR) Wide-Area Monitoring, Protection and Control systems (WAMPAC)—Standards for Cyber Security Requirements* [Online]. Available: http://smartgrid.epri.com/doc/ESRFSD.pdf

[11] G. Antonova, *M. L. S. F. Luis Fabiano dos Santos*.

[12] North American Electric Reliability Council (NERC). (Jan. 2011). *Balancing and Frequency Control*. [Online]. Available: http://www.nerc.com/docs/oc/rs/NERCn%20Balancingn%20andn%20Frequencyn%20Controln%20040520111.pdf

[13] K. Tomsovic, D. E. Bakken, V. Venkatasubramanian, and A. Bose, "Designing the next generation of real-time control, communication, and computations for large power systems," *Proc. IEEE*, vol. 93, no. 5, pp. 965–979, May 2005.

[14] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber physical system security for the electric power grid," *Proc. IEEE*, vol. 100, no. 1, pp. 210–224, Jan. 2012.

[15] National Electric Sector Cybersecurity Organization Resource (NESCOR). (Dec. 2015). *Electric Sector Failure Scenarios and Impact Analyses-Version 3.0* [Online]. Available: http://smartgrid.epri.com/doc/NESCORn%20Failuren%20Scenariosn%20v3n%2012-11-15.pdf

[16] "High-impact, low-frequency event risk to the north American bulk power system jointly-commissioned summary report," North Amer. Electr. Rel. Corp. U.S. Dept. Energy, MD, USA, Tech. Rep., Nov. 2009.

[17] R. Sekar *et al.*, "Specification-based anomaly detection: A new approach for detecting network intrusions," in *Proc. 9th ACM Conf. Comput. Commun. Secur. (CCS)*, New York, NY, USA, 2002, pp. 265–274. [Online]. Available: http://doi.acm.org/10.1145/586110.586146

[18] H. Lin, A. Slagell, C. Di Martino, Z. Kalbarczyk, and R. K. Iyer, "Adapting bro into scada: Building a specification-based intrusion detection system for the DNP3 protocol," in *Proc. 8th Annu. Cyber Secur. Inf. Intell. Res. Workshop (CSIIRW)*, New York, NY, USA, 2013, pp. 5-1–5-4. [Online]. Available: http://doi.acm.org/10.1145/2459976.2459982

[19] R. Berthier and W. H. Sanders, "Specification-based intrusion detection for advanced metering infrastructures," in *Proc. IEEE 17th Pacific Rim Int. Symp. Depend. Comput.*, Dec. 2011, pp. 184–193.

[20] A. Hahn and M. Govindarasu, "Model-based intrustion detection for the smart grid (MINDS)," in *Proc. 8th Annu. Cyber Secur. Inf. Intell. Res. Workshop (CSIIRW)*, New York, NY, USA, 2013, pp. 27-1–27-4. [Online]. Available: http://doi.acm.org/10.1145/2459976.2460007

[21] H. Lin *et al.*, "Self-healing attack-resilient pmu network for power system operation," *IEEE Trans. Smart Grid*, to be published.

[22] U.S. Department Of Homeland Security Control Systems Security Program. (Oct. 2009). *Recommended Practice: Improving Industrial Control Systems Cybersecurity With Defense-In-Depth Strategies* [Online]. Available: https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/%Defense_in_Depth_Oct09.pdf

[23] "Integrating electricity subsector failure scenarios into a risk assessment methodology," U.S. Dept. Energy Electr. Power Res. Inst. (EPRI), MD, USA, Tech. Rep., Dec. 2013.

[24] E. Bompard, C. Gao, R. Napoli, A. Russo, M. Masera, and A. Stefanini, "Risk assessment of malicious attacks against power systems," *IEEE Trans. Syst., Man, Cybern. A, Syst., Humans*, vol. 39, no. 5, pp. 1074–1085, Sep. 2009.

[25] C. W. Ten, C. C. Liu, and G. Manimaran, "Vulnerability assessment of cybersecurity for SCADA systems," *IEEE Trans. Power Syst.*, vol. 23, no. 4, pp. 1836–1846, Nov. 2008.

[26] Y. Jiaxi, M. Anjia, and G. Zhizhong, "Vulnerability assessment of cyber security in power industry," in *Proc. IEEE PES Power Syst. Conf. Exposit.*, Oct. 2006, pp. 2200–2205.

[27] J. T. Mackin, R. Darken, and G. T. Lewis, "Managing Risk in Critical Infrastructures Using Network Modeling," part of an edited monograph titled, "Critical Infrastructure Protection: Elements of Risk," edited by George Mason University, School of Law, Dec. 2007, pp. 65–78. [Online]. Available: http://cip.gmu.edu/wp-content/uploads/2016/06/ElementsofRiskMonograph.pdf

[28] A. Ashok and M. Govindarasu, "Cyber-physical risk modeling and mitigation for the smart grid using a game-theoretic approach," in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. (ISGT)*, Feb. 2015, pp. 1–5.

[29] J. Pita, M. Jain, M. Tambe, F. Ordóñez, and S. Kraus, "Robust solutions to Stackelberg games: Addressing bounded rationality and limited observations in human cognition," *Artif. Intell.*, vol. 174, no. 15, pp. 1142–1171, 2010. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0004370210000986

[30] R. Yang, C. Kiekintveld, F. Ordóñez, M. Tambe, and R. John, "Improving resource allocation strategies against human adversaries in security games: An extended study," *Artif. Intell.*, vol. 195, pp. 440–469, Feb. 2013. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S000437021200152X

[31] V. Verendel, "Quantified security is a weak hypothesis: A critical survey of results and assumptions," in *Proc. Workshop Secur. Paradigms Workshop (NSPW)*, 2009, pp. 37–50. [Online]. Available: http://doi.acm.org/10.1145/1719030.1719036

[32] A. Clark, K. Sun, and R. Poovendran, "Effectiveness of IP address randomization in decoy-based moving target defense," in *Proc. IEEE 52nd Annu. Conf. Decision Control (CDC)*, Dec. 2013, pp. 678–685.

[33] A. R. Chavez, W. M. S. Stout, and S. Peisert, "Techniques for the dynamic randomization of network attributes," in *Proc. Int. Carnahan Conf. Secur. Technol. (ICCST)*, Sep. 2015, pp. 1–6.

[34] CISCO. *Snort-Intrusion Detection System* [Online]. Available: https://www.snort.org/

[35] Suricata. *Suricata-Open Source ids/ips/nsm Engine* [Online]. Available: https://suricata-ids.org/

[36] Splunk. *Splunk-Operational Intelligence, Log Management* [Online]. Available: https://www.splunk.com/

[37] IBM. *Qradar-Security Intelligence Platform* [Online]. Available: http://www-03.ibm.com/software/products/en/qradar

[38] Champion Technol. Corp. *Darklight-Cybersecurity Analytics and Automation Platform* [Online]. Available: https://www.darklightcyber.com/

[39] CISCO. *Ngips-Next-Generation Intrusion Prevention System* [Online]. Available: http://www.cisco.com/c/en/us/products/security/ngips/index.html

[40] Fire Eye. *Fire Eye-Network Security Essentials* [Online]. Available: https://www.fireeye.com/products/nx-network-security-products/nx-essent%ials.html

[41] W. Wang, W. He, and J. Su, "Network intrusion detection and prevention middlebox management in SDN," in *Proc. IEEE 34th Int. Perform. Comput. Commun. Conf. (IPCCC)*, Dec. 2015, pp. 1–8.

[42] T. Xing, Z. Xiong, D. Huang, and D. Medhi, "SDNIPS: Enabling software-defined networking based intrusion prevention system in clouds," in *Proc. 10th Int. Conf. Netw. Service Manage. (CNSM)*, Nov. 2014, pp. 308–311.

[43] A. Ashok, M. Govindarasu, and V. Ajjarapu, "Attack-resilient measurement design methodology for state estimation to increase robustness against cyber attacks," in *Proc. IEEE Power Energy Soc. General Meeting (PESGM)*, Jul. 2016, pp. 1–5.

[44] M. A. Rahman, E. Al-Shaer, and R. B. Bobba, "Moving target defense for hardening the security of the power system state estimation," in *Proc. 1st ACM Workshop Moving Target Defense (MTD)*, 2014, pp. 59–68. [Online]. Available: http://doi.acm.org/10.1145/2663474.2663482

[45] A. Ashok, M. Govindarasu, and V. Ajjarapu, "Online detection of stealthy false data injection attacks in power system state estimation," *IEEE Trans. Smart Grid*, to be published.

[46] S. Sridhar and M. Govindarasu, "Model-based attack detection and mitigation for automatic generation control," *IEEE Trans. Smart Grid*, vol. 5, no. 2, pp. 580–591, Mar. 2014.

[47] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proc. 16th ACM Conf. Comput. Commun. Secur. (CCS)*, 2009, pp. 21–32. [Online]. Available: http://doi.acm.org/10.1145/1653662.1653666

[48] R. Bobba, K. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. Overbye, "Detecting false data injection attacks on dc state estimation," in *Proc. Preprints 1st Workshop Secure Control Syst. (CPSWEEK)*, 2010.

[49] G. Dan and H. Sandberg, "Stealth attacks and protection schemes for state estimators in power systems," in *Proc. 1st IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, Oct. 2010, pp. 214–219.

[50] A. Giani, E. Bitar, M. García, M. McQueen, P. Khargonekar, and K. Poolla, "Smart grid data integrity attacks," *IEEE Trans. Smart Grid*, vol. 4, no. 3, pp. 1244–1253, Sep. 2013.

[51] G. Hug and J. A. Giampapa, "Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1362–1370, Sep. 2012.

[52] 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, pp. 645–658, Dec. 2011.

[53] L. Xie, Y. Mo, and B. Sinopoli, "False data injection attacks in electricity markets," in *Proc. IEEE 1st Int. Conf. Smart Grid Commun. (SmartGridComm)*, Oct. 2010, pp. 226–231.

[54] A. Ashok and M. Govindarasu, "Cyber attacks on power system state estimation through topology errors," in *Proc. IEEE Power Energy Soc. General Meeting*, Jul. 2012, pp. 1–8.

[55] T. T. Kim and H. V. Poor, "Strategic protection against data injection attacks on power grids," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 326–333, Jun. 2011.

[56] A. F. Taha, J. Qi, J. Wang, and J. H. Panchal, "Risk mitigation for dynamic state estimation against cyber attacks and unknown inputs," *IEEE Trans. Smart Grid*, to be published.

[57] B. Gou, "Generalized integer linear programming formulation for optimal PMU placement," *IEEE Trans. Power Syst.*, vol. 23, no. 3, pp. 1099–1104, Aug. 2008.

[58] S. Chakrabarti and E. Kyriakides, "Optimal placement of phasor measurement units for power system observability," *IEEE Trans. Power Syst.*, vol. 23, no. 3, pp. 1433–1440, Aug. 2008.

[59] N. H. Abbasy and H. M. Ismail, "A unified approach for the optimal PMU location for power system state estimation," *IEEE Trans. Power Syst.*, vol. 24, no. 2, pp. 806–813, May 2009.

[60] R. Emami and A. Abur, "Robust measurement design by placing synchronized Phasor measurements on network branches," *IEEE Trans. Power Syst.*, vol. 25, no. 1, pp. 38–43, Feb. 2010.

[61] V. Terzija *et al.*, "Wide-area monitoring, protection, and control of future electric power networks," *Proc. IEEE*, vol. 99, no. 1, pp. 80–93, Jan. 2011.

[62] A. Hahn, A. Ashok, S. Sridhar, and M. Govindarasu, "Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid," *IEEE Trans. Smart Grid*, vol. 4, no. 2, pp. 847–855, Jun. 2013.

[63] X. Liu, M. Shahidehpour, Z. Li, X. Liu, Y. Cao, and Z. Li, "Power system risk assessment in cyber attacks considering the role of protection systems," *IEEE Trans. Smart Grid*, to be published.

[64] C. Konstantinou and M. Maniatakos, "Impact of firmware modification attacks on power systems field devices," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, Nov. 2015, pp. 283–288.

[65] P. Wang, A. Ashok, and M. Govindarasu, "Cyber-physical risk assessment for smart grid system protection scheme," in *Proc. IEEE Power Energy Soc. General Meeting*, Jul. 2015, pp. 1–5.

[66] J. Hoyos, M. Dehus, and T. X. Brown, "Exploiting the GOOSE protocol: A practical attack on cyber-infrastructure," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2012, pp. 1508–1513.

[67] S. Sridhar and M. Govindarasu, "Data integrity attacks and their impacts on SCADA control system," in *Proc. IEEE Power Energy Soc. General Meeting*, Jul. 2010, pp. 1–6.

[68] G. Andersson *et al.*, "Cyber-security of scada systems," in *Proc. IEEE Innov. Smart Grid Technol. (ISGT)*, Jan. 2012, pp. 1–2.

[69] P. Esfahani, M. Vrakopoulou, K. Margellos, J. Lygeros, and G. Andersson, "A robust policy for automatic generation control cyber attack in two area power network," in *Proc. 49th IEEE Conf. Decision Control (CDC)*, Dec. 2010, pp. 5973–5978.

[70] S. Sridhar and M. Govindarasu, "Data integrity attack and its impacts on voltage control loop in power grid," in *Proc. IEEE Power Energy Soc. General Meeting*, Jul. 2011, pp. 1–6.

[71] A. Ashok, S. Sridhar, A. D. McKinnon, P. Wang, and M. Govindarasu, "Testbed-based performance evaluation of attack resilient control for AGC," in *Proc. Resilience Week (RWS)*, Aug. 2016, pp. 125–129.

ABOUT THE AUTHORS

Aditya Ashok (Member, IEEE) received the B.E. degree in electrical and electronics engineering from the College of Engineering, Guindy, Anna University, India, in 2008 and the Ph.D. degree in electrical engineering from Iowa State University (ISU), Ames, IA, USA, in 2017.

Currently, he is a Research Engineer in the Electricity Infrastructure Group under the Energy and Environment Directorate at Pacific Northwest National Laboratory (PNNL), Richland, WA, USA. His research interests include cybersecurity, cyber–physical security solutions for power grid wide-area monitoring, protection, and control applications, and cyber–physical system security testbeds.

Manimaran Govindarasu (Fellow, IEEE) received the Ph.D. degree in computer science and engineering from the Indian Institute of Technology (IIT), Chennai

Currently, he is the Mehl Professor of Computer Engineering in the Department of Electrical and Computer Engineering, Iowa State University, Ames, IA, USA., India, where he has been on the faculty since 1999. His research experiences are in the areas of cyber–physical system (CPS) security for the smart grid, cybersecurity, real-time systems and networks, and Internet of Things (IoT). He has coauthored over 150 peer-reviewed research publications, and has given several invited talks and tutorials at reputed IEEE conferences and delivered more than dozen industry training sessions on the subject of cybersecurity for the power grid (e.g., NERC GridSecCon 2015, 2016). He is a coauthor of the text *Resource Management in Real-time Systems and Networks* (Cambridge, MA, USA: MIT Press, 2001). His research is funded by the National Science Foundation (NSF), the U.S. Department of Homeland Security (DHS), and the U.S. Department of Energy (DOE), and the Power System Engineering Research Center (PSERC).

Dr. Govindarasu served as a guest coeditor for flagship IEEE publications (IEEE Network in 2003 and 2013, IEEE Power & Energy in 2012, and IEEE Transactions on Dependable and Secure Computing in 2017), and has been serving as an Editor for the IEEE Transactions on Smart Grid since 2013. He is the founding chair of the Cyber Security Task Force within the IEEE Power & Energy Society AMPS Committee.

Jianhui Wang (Senior Member, IEEE) received the Ph.D. degree in electrical engineering from Illinois Institute of Technology, Chicago, IL, USA, in 2007.

Currently, he is an Associate Professor with the Department of Electrical Engineering, Southern Methodist University, Dallas, TX, USA. He also holds a joint appointment as Section Lead for Advanced Power Grid Modeling at the Energy Systems Division, Argonne National Laboratory, Argonne, IL, USA.

Dr. Wang is the secretary of the IEEE Power & Energy Society (PES) Power System Operations, Planning & Economics Committee. He is an Associate Editor of the *Journal of Energy Engineering* and an Editorial Board member of *Applied Energy*. He has held visiting positions in Europe, Australia, and Hong Kong, including a VELUX Visiting Professorship at the Technical University of Denmark (DTU). He is the Editor-in-Chief of the IEEE Transactions on Smart Grid and an IEEE PES Distinguished Lecturer. He is also the recipient of the IEEE PES Power System Operation Committee Prize Paper Award in 2015.