6-2016

Smart Grid Security: Threats, Challenges, and Solutions

Anibal Sanjab

Walid Saad

Ismail Guvenc

Arif I. Sarwat

Saroj Biswas

Smart Grid Security: Threats, Challenges, and Solutions

Anibal Sanjab[1], Walid Saad[1], Ismail Guvenc[2], Arif Sarwat[2], and Saroj Biswas[3]
[1] Wireless@VT, Bradley Department of Electrical and Computer Engineering, Virginia Tech, Blacksburg, VA USA,
Emails: {anibals,walids}@vt.edu
[2] Department of Electrical and Computer Engineering, Florida International University, Miami, FL, USA, Email: {iguvenc,asarwat}@fiu.edu
[3] Department of Electrical and Computer Engineering, Temple University, Philadelphia, PA, USA, Email: saroj.biswas@temple.edu

***Abstract*—The cyber-physical nature of the smart grid has rendered it vulnerable to a multitude of attacks that can occur at its communication, networking, and physical entry points. Such cyber-physical attacks can have detrimental effects on the operation of the grid as exemplified by the recent attack which caused a blackout of the Ukranian power grid. Thus, to properly secure the smart grid, it is of utmost importance to: a) understand its underlying vulnerabilities and associated threats, b) quantify their effects, and c) devise appropriate security solutions. In this paper, the key threats targeting the smart grid are first exposed while assessing their effects on the operation and stability of the grid. Then, the challenges involved in understanding these attacks and devising defense strategies against them are identified. Potential solution approaches that can help mitigate these threats are then discussed. Last, a number of mathematical tools that can help in analyzing and implementing security solutions are introduced. As such, this paper will provide the first comprehensive overview on smart grid security.**

I. Introduction

Realizing the vision of a smart electric grid is contingent upon the effective integration of new information and communication technologies into the traditional generation-transmission-distribution physical systems. This, in turn, will give rise to a cyber-physical power system known as the *smart grid (SG)* in which a cyber layer that handles computations, communication, and data exchange, is tightly coupled with the physical system which handles the generation, transmission, and distribution of electric power as shown in Fig. 1.

Despite the significant advantages introduced by this cyber-physical coupling, the resulting dense interconnectivity between various SG elements and the increased reliance on its cyber system makes the grid more vulnerable to a multitude of cyber-physical attacks (CPAs) that aim at compromising its functionalities. This increased SG vulnerability is corroborated by the recent discovery of the control system malware, known as Stuxnet [1], which targets programmable logic controllers (PLCs) of industrial systems giving the adversary the ability to have control over the physical system. The fear of such threats has peaked after the first CPA-induced Ukranian blackout which has recently affected 225,000 customers spanning several Ukranian cities [2]. Clearly the security of the smart grid as one of the most critical technical challenges facing its deployment [3].

With such culminating risks, identifying and understanding potential threats which can target the SG is essential to achieve a more secure grid. This identification enables devising new security measures and strategies to thwart such attacks and make the grid more robust and resilient. However, due to the complex and large-scale nature of the SG, various challenges accompany these diagnostic and corrective efforts.

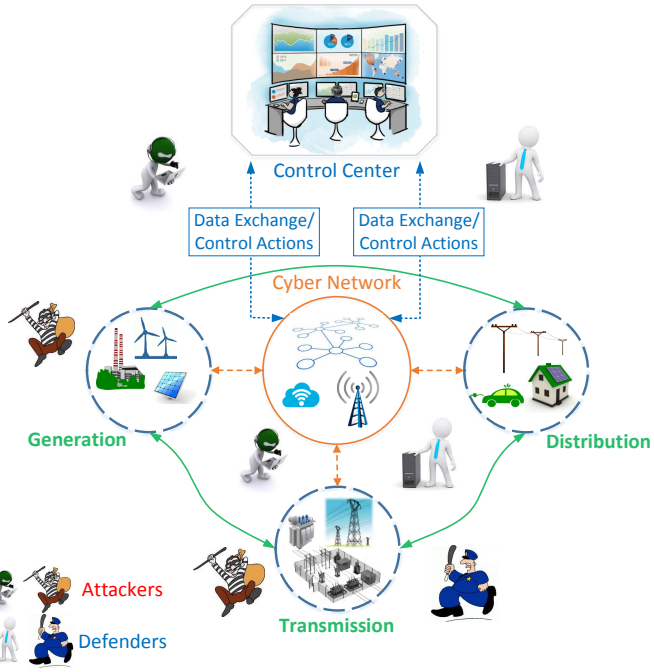

Fig. 1. Illustration of a smart grid architecture highlighting the underlying cyber layer and security threats.

The main contribution of this article is to provide the first comprehensive overview on the security threats facing the SG. In particular, the goal of this paper is threefold:

1) identify and explore the CPA threats which can target the smart grid,
2) discuss the unique challenges of analyzing SG security problems, and,
3) propose solution approaches and analytical frameworks which can help in analyzing the security of the SG and devising proper defense strategies.

In a nutshell, due to its necessity for all facets of daily life activities, interrupting the supply for electricity emerged as a lucrative target for adversarial activities. Insuring the sustainability and availability of electricity supply via SG functions is imperative but challenging as it requires a comprehensive knowledge of the various aspects of SG security. To this end, this paper aims at providing an inclusive investigation of the various security threats, challenges, and solutions pertaining to SG security.

II. Smart Grid Security Threats

Given its cyber-physical nature, the SG will inherit physical and dynamic system threats as well as well-known communication and network threats such as those targeting its integrity and availability[1]. However, the goals of such attacks will significantly differ from those sought by adversaries targeting classical cyber systems, such as communication networks. For instance, an attack on the SG primarily aims to disturb the operation of the physical generation, transmission, and distribution systems by exploiting their reliance on their underlying cyber layer. This is in contrast to conventional network attacks which typically seek to solely cause some sort of damage to or interruption of the cyber layer's functionality. The key SG security threats are discussed next.

A. Integrity

Integrity refers to the credibility of the data collected and transferred over the grid. Attacks that target this integrity can cause false estimation of the real-time state of operation of the system as well as lead to the unobservability or even instability of the system. Next, we present two key types of integrity attacks.

1) Data injection attacks (DIAs): DIAs consist of an adversary manipulating exchanged data such as sensor readings, feedback control signals, and electricity price signals. Such attacks can be done by compromising the hardware components (as in the case of Stuxnet), or intercepting the communication links. The most studied type of DIAs is the one that targets the grid's state estimator. The states of a power system consist of the voltage magnitudes and phase angles at every bus. Estimation of these states enables complete monitoring of the power and current flows throughout the grid.

To estimate these states, a number of measurements are collected from around the grid which include real and reactive power flows over transmission lines or injected/withdrawn at buses, voltage magnitudes, and, due to the placement of phasor measurement units (PMUs), synchronized voltage and current phase angles. The collected measurements are then fed to a state estimator which, using a maximum likelihood estimator, generates real-time estimates of the states which are used for operational and pricing purposes.

Therefore, manipulating the collected measurements results in a false estimate of the state of operation of the system. In turn, such false states can lead to incorrect operational actions whose effects can range from inducing incorrect pricing to destabilizing the power system. In practice, a bad data detection (BDD) mechanism is deployed to detect outliers. However, the authors in [4] showed the existence of a *stealthy data injection attack model* that can manipulate the state estimation outcome without being detected by common BDD mechanisms. The effects of such attacks vary widely depending on the goal of the attacker.

- *System damage:* Some DIAs are primarily concerned with damaging the system and have a purely destructive nature, such as in terrorist attacks. For example, an attacker can manipulate system measurements so that a congested transmission line falsely seems to not have reached its thermal transmission limit. Thus, based on these false estimates, the system operator would route more power over the line which leads it to over-heat and sag. This sagging reduces the distance in between the line and ground (or other objects in between) which can trigger a line to ground fault. Under stress conditions, such a fault can induce large fluctuations in system dynamics that can lead to tripping additional lines, disconnecting generators, load shedding, or even a system blackout.
- *Financial benefit:* Real-time pricing in electricity markets is based on the state estimator's real-time estimate of the state of operation of the system. Thus, corrupting the state estimates using DIAs leads to manipulation of the electricity prices in a way that is lucrative to the attacker [5].
  This is illustrated in Fig. 2 which corresponds to a DIA targeting measurements of three line flow measurements over the IEEE 30-bus test system. Clearly, without any attack, the prices are equal throughout the system. However, the attack successfully manipulated the prices causing, for example, a 27% increase in the price at bus 7. Thus, suppose that the attacker is a market participant who sells power at bus 7 and buys the same amount of power at bus 20. As seen in Fig. 2, without any attack, this transaction generates no profit. However, in the presence of an attack, the participant reaps a 30% profit from this transaction.

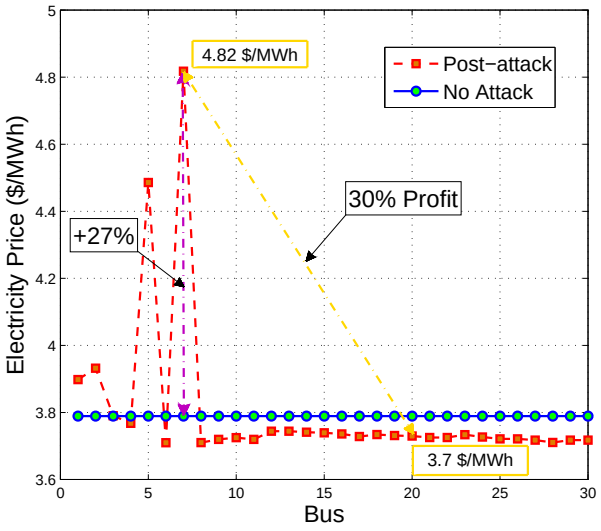

Fig. 2. Electricity price manipulation using data injection attacks.

Beyond targeting the state estimator, data injection attacks can target wide area protection, monitoring, and control (WAPMC) schemes which rely on global data collected from around the system to detect the occurrence of a disturbance

[1]Privacy is yet an important facet of smart grid security that is out of scope of this article due to space limitations.

and take corrective actions to stop its propagation. In this regard, manipulating the exchanged data can lead to a false characterization of a disturbance leading to false disconnection of lines, generators, or loads [6].

2) Time synchronization attacks: To better monitor the grid, there has been an increased use of PMUs – high-speed measurement units (typically 30-60 samples/second) capable of measuring the voltage and current phasors as well as local frequencies. Given that the measurement devices are spread around the system, sending their collected measurements to data concentrators or control centers is subject to transmission delays. Therefore, in order to properly align and analyze the measurements, all the collected PMU data are synchronized based on a time reference provided by a global positioning system (GPS) signal. This time referencing provides a time stamp to each collected measurement. The high speed sampling capabilities and, most importantly, the synchronization between the collected measurements enable accurate real-time wide area monitoring, protection, and control of the SG.

Here, an adversary can manipulate the time reference of the time stamped measured phasors to create a false visualization of the actual system conditions thus yielding inaccurate control and protection actions. Attacks that target PMU time synchronization are known as *time synchronisation attacks (TSAs)* [7]. Using TSAs, the GPS signal is spoofed and counterfeited by the attacker so that PMU sampling is done at the wrong time hence generating measurements with wrong time stamps. Recent results in [7] have shown that TSAs can produce significant fault location errors which can go up to 180 km for a line of length 400 km and even trigger a false alarm regarding the presence of a fault. This false alarm can result in a disconnection of a transmission line which can then trigger a cascading chain of failures across the grid. Such a false disconnection was one of the main culprits that led to the North American Northeast blackout in 1965 [6].

B. Availability

Availability pertains to the accessibility to every grid component as well as to the information transmitted and collected, whenever needed. Attacks compromising this availability are known as *denial of service (DoS)* attacks that can block key signals to compromise the stability of the grid and observability of its states.

In this regard, maintaining generation-load balance is essential for the SG operation. Indeed, the angular frequency of a synchronous generator is based on the difference between the electric power it serves and the input mechanical power of its turbine provided by, for example, burning fuel or coal. For the generator to retain constant angular frequency, its mechanical power should always match its connected electric load. Thus, if the mechanical input is kept constant, an increase in the electric load leads to a drop in angular frequency while a decrease in load leads to a rise in frequency. Consequently, generators are equipped with local and global control systems that typically follow a three-layer design as shown in Fig. 3 to maintain a constant frequency.

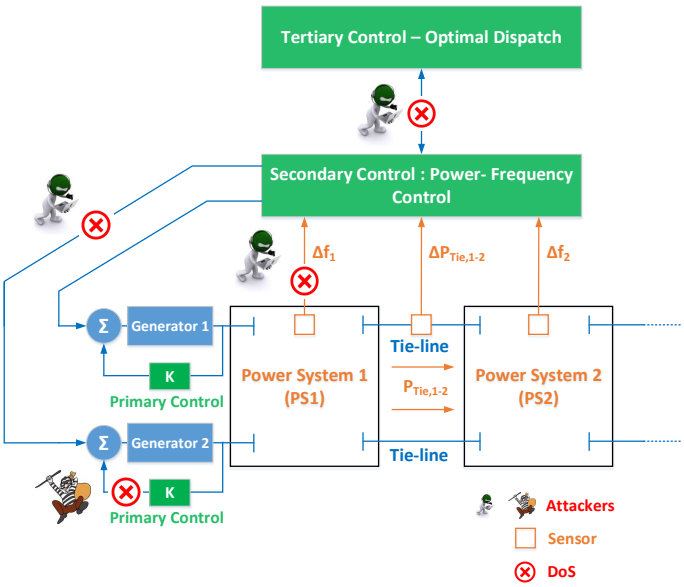

Fig. 3. Illustration of the three-layered control architecture of a smart grid: Δf_i is the deviation in frequency within PS_i from the nominal frequency (60 Hz in most of North and South America, 50 Hz in most other areas of the world), and $\Delta P_{\text{tie,1-2}}$ is the deviation in power flowing over the tie-lines from the scheduled value. Generators 1 and 2 are part of PS_1.

The *first layer* consists of a local primary proportional controller which aims at adjusting the mechanical power of the generation to match the changes in electric load. This proportional control reduces the frequency deviation but maintains a steady state error. To eliminate this steady state error, a central integral control is used in which various generators participate. This integral control represents the *secondary control layer*. The *tertiary control*, corresponds to a supervisory control responsible for allocating enough spinning reserve and for optimally dispatching the units participating in the secondary control. Moreover, the SG consists of an interconnection of many power systems which are connected using tie-lines. Thus, a deviation in frequency at one system triggers deviations in the power flowing over the tie-lines. Consequently, a control scheme known as *power-frequency control* regulates the tie-line power flow based on the sensed frequency deviations.

Therefore, the dynamic stability of the grid is crucially dependent on the availability of the sensor measurements and control signals provided by the three layers of control. In fact, using DoS to block the primary control signal and prevent it from decreasing the mechanical input power following a drop in the load leads to the acceleration of the generator and its shut down by an over-frequency relay. Moreover, a DoS blocking secondary control from eliminating steady state frequency errors can lead to the loss of synchronism between generators. Analogously, blocking tertiary control can have similar effects and can lead to suboptimal operation incurring large monetary losses.

This hence also sheds light on the difference between threats

on the SG as a CPS and threats pertaining to conventional cyber systems. In fact, compromising availably can destabilize the SG. In contrast, a DoS may not, in most cases, stop the operation of a cyber system, but it will typically incur delays.

C. Additional Dynamic System Attacks

As a dynamic control system, various dynamic system attacks (DSAs) can be launched at the SG. One well investigated such type of attacks is known as *replay attacks (RAs)* which can have serious effects on system stability [8]. In RAs, the adversary injects input data in the system without causing changes to the measurable outputs. To launch this attack, an adversary compromises sensors, monitors their outputs, learns from them, and repeats them while injecting its attack signal. Another type of DSAs is known as *dynamic data injection attacks (D-DIA)* which uses knowledge of the grid's dynamic model to inject data that causes unobservability of unstable poles [9]. As a result, a successful D-DIA prevents the grid's operator from detecting instability which, in turn, can lead to a system collapse. A *covert attack* is one other type of DSAs that is basically a closed loop version of an RA [9].

D. Physical Threats

Given the wide footprint over which the power system is physically spread, the danger of physical attacks in which an adversary physically attacks a physical component such as a generator, substation, or transmission line is prominent. For example, components can be physically attacked remotely using a rifle as was the case in a sniper attack which targeted a substation in California in 2013 [10]. Another type of physical attacks consists of physical manipulation of smart meters for energy theft purposes.

E. Coordinated Attacks

The power system typically incorporates robustness measures that helps it survive potential failures. Under typical system conditions, an attack leading to the failure of one or few components might not always have significant effects on the grid's operation. For example, the power system follows the so-called "$N-1$" security criterion which instills redundancies in the system design allowing the preservation of the system's state of normal operation even after the loss of one of its N components.

However, *coordinated attacks (CAs)* can still be launched by resourceful adversaries that exploit the dense interconnections between grid components to launch simultaneous attacks of different types targeting various components. For example, the recent CPA-caused blackout of the Ukranian grid is a CA which concurrently targeted three power distribution companies. The adversary compromised a number of their computers to gain control of the SCADA system to simultaneously disconnect around 27 substations [2].

CAs are the most challenging types of attacks since they can surpass traditional reliability and robustness design solutions and require a multi-layered security solution approach.

Table I summarizes the discussed threats, their associated security types, and their main potential SG targets.

III. Challenges

The aforementioned threats naturally give rise to a number of key challenges, as detailed next.

A. Limitation of Traditional Cyber Security Solutions

Existing cyber security solutions that have been devised for cyber systems are invaluable for improving SG security. For example, existing intrusion detection and cryptographic solutions will certainly contribute towards better grid security. However, some of these solutions might not be directly applicable to the SG due to a number of reasons:

1) *Presence of a physical system:* existing cyber security solutions do not consider the presence of a physical system. However, as discussed in Section II, one of the main goals of attacks on the SG is to damage to the physical system. Thus, SG attacks are designed based on the physical effects that they can cause. Therefore, any security solution that does not directly account for the physical system is simply not adequate for defending the smart grid.
2) *Risk management and diffusion:* the analysis of the propagation of attacks in a physical system is different from that corresponding to cyber systems. For instance, the study of how computer malware propagates in a cyber system is different from how failures cascade and propagate throughout a dynamic CPS such as the SG.

B. Limitations of Existing Reliability Evaluation Solutions

There exists several studies for improving the power system's reliability and availability via various means such as improving redundancies and maintenance processes. Such existing reliability designs are primarily concerned with studying failure events which are likely to occur up to a certain level. However, a CA can cause various coordinated failures, as discussed in Section II-E, that have very low probability of naturally happening and, as such, they are not typically accounted for in reliability analyses. In fact, the cyber layer has provided an increased reachability for the adversaries using which various components that are located at separated geographic locations can be concurrently targeted.

C. Limitations of Conventional Control-Theoretic Solutions

Conventional control-theoretic security analyses are primarily concerned with designing robust controls which can preserve operational requirements in face of exogenous disturbances. However, such analyses do not explicitly account for the cyber layer and all the underlying cyber threats that it can introduce to a CPS such as the SG.

D. Tradeoff Between Security and Performance

SG security solutions must be inherently cognizant of the performance of the system. In particular, these solutions must seamlessly integrate with the grid with minimal disruption to its operation and performance. This tradeoff between security and performance is much more pronounced in the SG, compared to communication networks, due to the CPS

TABLE I
SG SECURITY THREATS

Threat Label	Security Breach Type	Main SG Target
Data injection attacks (DIA)	Integrity	State estimator, WAPMC
Time synchronization attacks	Integrity	PMUs, WAPMC
Denial of service attacks	Availability	Primary, secondary, and tertiary controls, WAPMC
Dynamic system attacks (Dynamic DIA, Replay, Covert)	Dynamic integrity	Primary, secondary, and tertiary controls
Physical destruction	Physical	Physical system components
Meter manipulation	Physical	Smart meters
Coordinated attacks	All of the above	All of the above

nature of the grid. For example, the best security strategy to thwart cyber attacks from penetrating the grid is to completely eliminate wireless and Internet connectivity. Even though this will improve the security of the grid, it will deprive it from all the economic and operational advantages that the cyber layer introduces. Thus, finding the best security strategy while meeting stringent performance requirements is a key challenge.

E. Aging Components

One of the reasons that renders SG security even more challenging is that most of the components of the system were designed and implemented decades ago. Hence, at the time of their design, cyber layer integration had not been proposed yet; and thus, the security threats that it introduces had not been anticipated. Therefore, patching mechanisms to accommodate for the newly introduced threats are of high importance and, undeniably, pose serious challenges.

IV. SOLUTION APPROACHES

Given the culminating threats facing the SG, security solutions must be developed to thwart potential attacks and maintain the operation of the grid. In particular, due to the high complexity involved, a systematic approach for securing the system is needed. To this end, a proposed systematic approach is illustrated in Fig. 4 and is detailed next.

A. Prevention Phase

The prevention phase involves reinforcing the security of the system to prevent any attack from successfully intruding and intervening in its operation. Here, various types of analyses can be performed:

1) *Vulnerability assessment and risk management:* vulnerability assessment consists of determining which grid components are vulnerable to which types of threats. Using past data, the SG operator can identify which components have historically been subject to which attacks. For example, since spoofing attacks targeting GPS signals are common, PMUs are expected to be vulnerable to spoofing and TSAs [7]. Moreover, the vulnerability of some components can be also analyzed analytically and experimentally. For example, a non-encrypted sensor data is vulnerable to RAs given that the attacker can easily learn a sequence of previously generated data and repeat it. Similarly, a meter unprotected with firewall that is connected to the Internet will be vulnerable to data injection attacks.
   Risk management uses vulnerability assessment results and combines them with an estimation of the effect that a vulnerability can have on the SG. Risk management in SG includes two key tasks:
   a) *Contingency analysis:* assessing the effect that the loss of a component such as a transmission line, generator, transformer, or sensor, can have on the dynamic stability and operating state of the grid.
   b) *Cascading failures analysis:* analyzing the propagation of failures over the grid.

   The later requires understanding the interdependencies between the various grid elements to anticipate the cascading chain of events that may occur when some components are lost. For example, the loss of a transmission line in heavy loaded conditions might lead to cascading failures resulting in a blackout while the loss of another line might have unnoticeable effects.
   Vulnerability assessment and risk management are continuously evolving processes using which the operator continuously learns about potential threats and vulnerabilities so as to improve its protection of the system.
2) *Security reinforcement:* once threats and their associated effects are characterized, policies for reinforcing the grid security must be derived. However, such reinforcement procedures are typically subject to budgetary and investment constraints. Thus, the results obtained from vulnerability and risk management can be used to create a ranking of the most critical components to protect first. Security reinforcement can include encrypting a number of sensor readings, replacing some meters with more sophisticated and capable models [5], replacing wireless with wired communication, or implementing robust control designs. Security reinforcement is a robustness measure which aims at securing the grid against a range of potential threats.

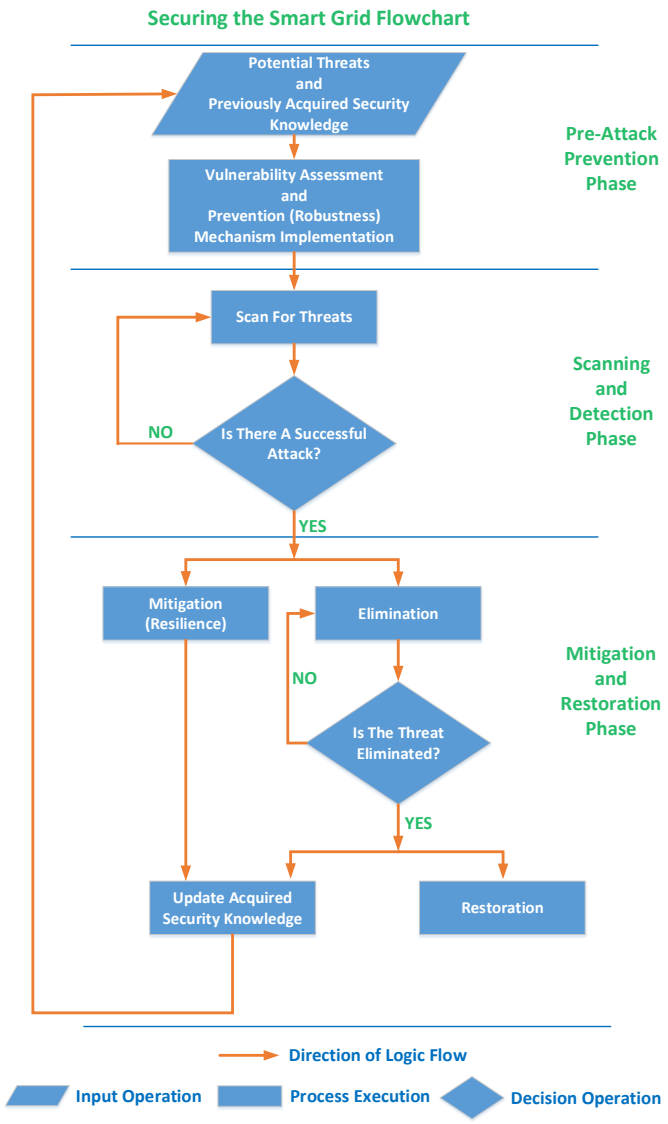

Fig. 4. Flowchart illustrating a systematic approach for the defense of the grid against CPAs.

B. Scanning and Detection

Vulnerability assessment, risk management, and security reinforcement constitute a preventive measure to thwart potential attacks which can target the grid. However, they cannot completely secure the grid against all types of attacks for two main reasons:

1) *Undiscovered threats:* there are many emerging vulnerabilities and attack strategies of which the operator might not be aware.
2) *Budget constraints:* budgetary constraints can limit the volume of possible security reinforcement implementations.

Therefore, the operator must continuously scan the system to detect new threats which have passed the attack prevention defense lines. This is crucial for stealthy and advanced persistent threats which penetrate the system and run long-term stealthy attacks that cannot be obviously identified.

Various detection mechanisms have been studied in literature with each focusing on detecting a type of SG attacks. For example, the work in [11] provides a methodology for detecting stealthy data injection attacks targeting the state estimator while the authors in [12] propose a detection mechanism against TSAs targeting PMUs. Moreover, the authors in [8] propose a detection mechanism against replay attacks.

C. Mitigation, Elimination, and Restoration

Once an attack is detected using detection mechanisms or by witnessing an apparent damage to the grid, mitigating the effect of the attack and eliminating it become essential for restoring the normal operating state.

1) *Mitigation:* during the occurrence of an attack, mitigation measures can be deployed to reduce its effect on the system. Mitigation techniques may include: a) power system protection techniques which can be used for stopping the propagation of disturbances, b) spinning reserves or distributed generation which can be leveraged to meet the loss of generation, c) load shedding which disconnects a part of the total load in order to prevent a complete collapse of the system, and d) islanding which splits the grid into small disjoint systems to stop the propagation of failures and dynamic disturbances. Mitigation techniques are forms of resilience measures in which the system sacrifices some operational quality to decrease the risk of a complete collapse.
2) *Elimination and Restoration:* to restore the normal operating state of the system once an attack is detected, taking prompt actions to eliminate it becomes critical. Elimination can be done by various means such as replacing compromised components or updating their software. After threat elimination, SG elements that had been disconnected such as transmission lines, generators, and loads can be reconnected to restore normal operation.

After an attack, the operator's knowledge about this attack and the vulnerabilities of the system as well as the ways of detecting and mitigating this attack evolves. Therefore, this allows for the operator to update its defense policies to improve the security of the grid.

Table II summarizes the discussed threats, challenges, and solutions while providing relevant comments. To successfully analyze SG security and deploy the aforementioned solutions, a number of analytical frameworks can be leveraged, as discussed next.

V. Analytical Frameworks for Smart Grid Security Analysis

Implementing effective SG security solutions requires analytical frameworks which enable modeling of the grid's cyber and physical systems and their tight coupling, the interdependency between various grid components, and the decision making processes of the operator and attackers.

TABLE II
SUMMARY OF SG SECURITY THREATS, CHALLENGES, AND SOLUTIONS.

Threats	Integrity attacks	Data injection attacks.
		Time synchronisation attacks.
	Availability attacks	Denial of service attacks.
	Dynamic system attacks	Replay attacks.
		Dynamic data injection attacks.
		Covert attacks.
	Physical attacks	Physical damage.
		Meter manipulation.
	Coordinated attacks	Multiple concurrent types and targets.
Challenges	Limitation of cyber security solutions	Presence of physical system.
		Different risk propagation mechanisms.
	Limitation of reliability evaluation solutions	Presence of unlikely coordinated failures.
	Limitation of conventional control-theoretic solutions	Presence of cyber layer.
	Tradedoff: security vs. performance	Security must preserve operational requirements.
	Aging components	Old equipments: need security patching.
Solutions	Prevention	Vulnerability assessment and risk analysis.
		Security reinforcement.
	Detection	Focus: stealthy and persistent threats.
		Constraints: budget.
	Mitigation, elimination, and restoration	Mitigation: block propagation, leverage reserves.
		Elimination: Update compromised components.
		Restoration: reconnect disconnected components.

In addition to using solutions from information security, power system protection, control theory, and reliability evaluation, additional analytical tools are very useful in modeling and studying SG security problems as discussed next.

A. Modeling Using Networked Control Systems

Networked control systems (NCSs) [13] combine communication and information technologies with control system designs to model CPSs such as the SG. Indeed, in NCSs, a shared communication network is responsible for the communication between the various sensors, actuators, and controllers in the CPS. As a result, NCSs can be used to model the cyber-physical nature of the smart grid which is extremely important for studying potential threats and deriving appropriate security solutions for the SG.

B. Graph-Theoretic Techniques

Given that the SG is a networked cyber-physical system (NCPS), *graph-theoretic* techniques can be useful to model the network interconnectivity between the grid components. In fact, a graph is represented by a set of vertices and a set of edges connecting these verticies. For SG security applications, the verticies can represent components such as generators, transformers, loads, or meters. while edges can model the interconnectivity between these components. The modeling of this interconnectivity can consider real, physical connectivity between the components [14] or functional, logical connectivity modeling the interdependencies between those components [6].

Hence, graph-theoretic methods are very useful for understanding the networked nature of the SG and analyzing the interconnectivity between its elements to shed light on the threats facing the grid and their propagation.

C. Game-Theoretic Techniques

Game theory is a set of mathematical tools used to analyze strategic interaction and decision making between entities, referred to as players, with interconnected, conflicting or aligned, interests. In a typical SG security setting, an attacker aims to choose an attack strategy to maximize the damage caused to the grid while the operator (defender) aims at choosing a defense strategy to minimize the damage to the system. Thus, due to the conflicting objectives of the attackers and defenders, game-theoretic techniques [15] provide invaluable tools to model their optimal decision making and hence finding the best defense strategy given the potential strategies of the attackers.

Various works have applied game-theoretic techniques to the analysis of smart grid security problems. For example, our recent work in [5] used game theory to characterize the best set of meters to defend in order to thwart data injection attacks which can be carried out by multiple adversaries.

VI. FUTURE OUTLOOK

In this paper, a comprehensive analysis of the various SG security threats, incurred challenges, and potential solutions have been investigated. This analysis paves the way for more in-depth investigations of each of the discussed threats and their correlations in order to quantize their combined effects on the SG. This will enable devising appropriate solutions against coordinated attacks which threaten the sustainability of current and future smart grids.

REFERENCES

[1] D. Kushner, "The real story of stuxnet," *IEEE Spectrum*, vol. 50, no. 3, pp. 48–53, March 2013.

[2] T. C. Robert M. Lee, Michael J. Assante, "Analysis of the cyber attack on the Ukranian power grid. defense use case." *SANS ICS*, March 2016. [Online]. Available: http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf

[3] J. G. Kassakian, R. Schmalensee, G. Desgroseilliers, T. D. Heidel, K. Afridi, A. Farid, J. Grochow, W. Hogan, H. Jacoby, J. Kirtley *et al.*, "The future of the electric grid," *Massachusetts Institute of Technology, Tech. Rep*, pp. 197–234, 2011.

[4] Y. Liu, P. Ning, and M. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, pp. 1–33, May 2011.

[5] A. Sanjab and W. Saad, "Data injection attacks on smart grids with multiple adversaries: A game-theoretic perspective," *IEEE Transactions on Smart Grid*, vol. to appear, 2016.

[6] A. Sanjab and W. Saad, "On bounded rationality in cyber-physical systems security: Game-theoretic analysis and application to smart grid protection," in *IEEE/ACM CPS Week, Workshop on Cyber-Physical Security and Resilience in Smart Grids*, April 2016.

[7] Z. Zhang, S. Gong, A. Dimitrovski, and H. Li, "Time synchronization attack in smart grid: Impact and analysis," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 87–98, March 2013.

[8] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *47th Annual Allerton Conference on Communication, Control, and Computing*, Sept. 2009, pp. 911–918.

[9] F. Pasqualetti, F. Dorfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 58, no. 11, pp. 2715–2729, Nov 2013.

[10] J. Pagliery, "Sniper attack on california power grid may have been an insider, dhs says," *CNN. com*.

[11] W. Niemira, R. Bobba, P. Sauer, and W. Sanders, "Malicious data detection in state estimation leveraging system losses and estimation of perturbed parameters," in *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Oct. 2013, pp. 402–407.

[12] Z. Zhang, M. Trinkle, A. D. Dimitrovski, and H. Li, "Combating time synchronization attack: A cross layer defense mechanism," in *ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS)*, April 2013, pp. 141–149.

[13] J. P. Hespanha, P. Naghshtabrizi, and Y. Xu, "A survey of recent results in networked control systems," *Proceedings of the IEEE*, vol. 95, no. 1, pp. 138–162, Jan. 2007.

[14] S. Bi and Y. J. Zhang, "Graphical methods for defense against false-data injection attacks on power system state estimation," *IEEE Transactions on Smart Grid*, vol. 5, no. 3, pp. 1216–1227, May 2014.

[15] T. Alpcan and T. Başar, *Network security: a decision and game-theoretic approach*. New York: Cambridge University Press, 2011.