Cyber Security for Power System State Estimation

Yacine Chakhchoukh and Hideaki Ishii

Abstract State estimation is a critical application that provides situational awareness and permits efficient operation of the smart grid. The secure, accurate, and fast computation of the state estimates is crucial to execute the complex decisions and diverse control actions needed in real time to provide reliable, economic, and safe power systems that integrate distributed and intermittent renewable generation. This chapter discusses research directions to evaluate the cyber security and develop novel algorithms for securing today and tomorrow's power state estimation and grid operation.

1 Introduction

Power systems are essential in the functioning and development of our modern society. Unfortunately, the modern power systems are vulnerable to cyber attacks that could degrade their performance and cause blackouts [1, 2]. Indeed, the power grid is becoming increasingly complex and the need for implementing sophisticated cyber systems for its automatic operation raises serious concerns regarding its safety. Recently, the US administration warned power companies against cyber attacks such as the ones that targeted Ukraine's power grid in December 2015 [3].

The power systems are evolving toward the so-called smart grid, which enables increased integration of intermittent generation from renewable energy sources such as solar and wind with classical sources such as coal, nuclear, natural gas, and hydroelectric [2]. For example, renewable generation is forecasted to englobe more than two-thirds of all installed generation capacity between now and 2030 [4].

Y. Chakhchoukh
Department of Electrical and Computer Engineering, University of Idaho,
875 Perimeter Drive, MS 1023, Moscow, ID 83844-1023, USA
e-mail: yacinec@uidaho.edu

H. Ishii (✉)
Department of Computer Science, Tokyo Institute of Technology,
4259-J2-54, Nagatsuta-cho, Midori-ku, Yokohama 226-8502, Japan
e-mail: ishii@c.titech.ac.jp

© Springer Nature Switzerland AG 2019

J. Stoustrup et al. (eds.), *Smart Grid Control*, Power Electronics
and Power Systems, https://doi.org/10.1007/978-3-319-98310-3_15

The rapid development of energy storage, sensing, communication, computing technologies, and distributed automatic control will aid this transition. The resulting power grid can be viewed as a large interconnected cyber-physical system [2]. The cyber part will contain all the communication, data analysis, computation, and control needed by the power systems. Developing the cyber part and its applications helps improve the operation of the future power systems but increases vulnerabilities to cyber attacks introduced by malicious agents and hackers. Cyber attackers can be individuals, groups, organizations, or even nations and could be motivated by inducing financial gains or creating nuisance by targeting the power grid. Such attacks can be possible due to the development of complex communication networks, the Internet, and different viruses and malwares. Modern power system control networks are interconnected at certain points with traditional Information Technology (IT) enterprise networks and the Internet. Intruders will have the possibility to access the power systems and modify the normal operation of the system. Actually, manipulations or attacks committed by malicious intruders can result in tremendous adverse effects in both the cyber and the physical worlds.

The vulnerabilities of the smart grid toward cyber attacks are not fully understood and cyber attack impacts could range from a modified electricity market and degraded operation to a threatened integrity of the grid causing material loss and destruction, and even cascading blackouts. The power grid is considered to be an important critical infrastructure and today's economy and society depends on its stable, efficient, and secure operation [5]. The amount of cyber security threats and the success rate of cyber attacks on current Information Technology and Operational Technology systems pose a currently immeasurable amount of risk to this critical infrastructure on which our society and economy depend. Since the reliability and costs can be affected by attacks, it is vital to insure the security and safety of the cyber system against malicious intruders [6, 7]. Research and development of techniques and algorithms for securing critical control systems in the power grid is imperative.

The focus of this chapter is on the cyber security issues that arise in the context of state estimation (SE) in power systems. Real-time operation of the power systems uses the SE results, which consists of the evaluation of voltage magnitudes and phase angles at chosen buses or substations [8, 9]. Several grid operation tools and power market tasks such as contingency analysis, unit commitment, economic dispatch, and locational marginal prices (LMPs) computation rely on an available and accurate state estimation. The SE is also needed by the operator in order to picture the power system condition clearly, which permits situational awareness in order to take the optimal corrective control actions. The results from SE are useful to run a Security Analysis (SA), or the so-called Operational Reliability Analysis (ORA). In the ORA, a contingency analysis is executed to check if the system is (N-1) secure. The term (N-1) secure means that the power system is still stable and in an acceptable state region after any single major contingency. A contingency could be, for example, a loss of a major generator, a transmission line or a large load change. The results from the contingency analysis will determine the need of the operator to intervene in the operation. If the system is safe, then the optimized electricity markets will determine the grid operation and the different power flows in the grid. Otherwise, the operator

will take the appropriate actions such as generation rescheduling to insure the safety of the system which is fundamental.

In order to implement the future smart grid technology, it is necessary to identify the cyber-threats and the cyber-vulnerabilities of the real-time operation of realistic power systems and propose novel theoretical and practical solutions. This is a multidisciplinary area which requires complementary research expertise from systems control, signal processing, and power systems. The process is in general composed of three stages: (1) To assess the cyber-vulnerabilities and their consequences on the power grid. The emphasis here consists in providing a study of attacks targeting the power state and topology of the grid and their impacts on the real-time operation, control and power markets. (2) To propose novel procedures to detect and isolate cyber attacks. The techniques studied consist of adapting new robust signal processing methods for the linear and nonlinear regression and time series contexts, filtering and forecasting in the presence of cyber attacks and non-stationarity. (3) To counter or mitigate the impact resulting from cyber attacks and take the convenient correcting operation actions to ensure a resilient, reliable, efficient, and economical operation of the whole power system.

The organization of this chapter is as follows: In Sect. 2, we first provide an overview of the static state estimation problem and the bad data detection schemes. In Sect. 3, we discuss cyber attack models, configuration, and consequences on the power systems. Section 4 provides interesting and necessary future research directions. Finally, Sect. 5 concludes the chapter.

2 Static Power State Estimation

The static state estimation is run after collecting measurements from the supervisory control and data acquisition units (SCADAs) at remote terminal units (RTUs), and the results are communicated to the control center every 2–5 s. One important objective of the state estimation is to detect accidental bad data, i.e., bad measurements, topology errors, and line parameter inaccuracies and to correct this erroneous sensed data using the power model and available redundant measurements. To fulfill this objective, SE modules from different energy management systems (EMS) vendors are equipped with bad data detectors (BDD).

The objective consists in estimating the vector $x \in \mathbb{R}^n$ obeying a linear regression (DC) or nonlinear regression model (AC). The vector $z \in \mathbb{R}^m$ contains communicated readings from SCADAs. The number n of states is estimated from a larger number of measurements m. The AC model considers reactive power measurements and permits to estimate voltage magnitudes as well as phase angles at different buses or substations. The DC model assumes the voltages to be equal to 1 per unit (p.u.) at all buses and estimates only the phase angles. Obtaining the phase angles gives a clear picture about the power flow paths in the grid. The obtained models are linear regression for DC and nonlinear regression for AC.

In the AC formulation, the state x follows the equation:

$$z = h(x) + e. \tag{1}$$

The vector x provides the power states, i.e., voltage magnitudes and phase angles at the buses of interest. The error vector e is random and assumed Gaussian with zero mean and covariance matrix R. The nonlinear vector function $h(\cdot)$ is known as the measurement function and reflects the grid topology and transmission line parameters. The grid topology is estimated in the topology processor module and is updated continuously by collecting readings of the circuit breakers' binary states (i.e., 0 or 1 that can be obtained from node breaker models). The binary states provide the information about whether the different transmission lines are open or closed [8]. The different line parameters are available in the operators' database and are exploited to reconstruct the nonlinear function $h(\cdot)$. The line parameters are also estimated or updated when needed [8, 9].

In practice, the SE is solved by running an iterative algorithm based on the weighted least squares (WLS) [8], i.e., at the $k+1$ iteration, the state estimate $\hat{\boldsymbol{x}}^{k+1}$ is related to the gain matrix $G(\hat{x}^k) = \left(H^{(k)}(\hat{x}^k)\right)^T R^{-1} H^{(k)}(\hat{x}^k)$ as

$$\hat{x}^{k+1} = \hat{x}^k + \Delta x^k, \tag{2}$$

$$G\left(\hat{x}^k\right)\Delta x^k = \left(H^{(k)}\right)^T\left(\hat{x}^k\right)R^{-1}\left(z - h\left(\hat{x}^k\right)\right). \tag{3}$$

The matrix $H^{(k)}$ is the Jacobian of $h(\cdot)$ with respect to x at step k. The gain matrix $G(\hat{x}^k)$ is factorized following the LQ decomposition. The inverse matrix of $G\left(\hat{x}^k\right)$ can also be computed to evaluate Δx^k.

After the convergence of the algorithm [9], the obtained residuals, i.e., $r = z - h(\hat{x}^k)$ are analyzed in BDD modules to flag possible outliers or bad data. The bad data could be due to natural failures such as sensor, communication channels misbehavior or intrusions and cyber attacks. The most practical outlier detection rules are known as the chi-square (χ_2) test and the "3σ" rejection rule [9]. In the power systems literature, the largest normalized residual rejection (LNR) has been proposed as well. Basically, the largest normalized residual or element in r is rejected if it does not obey the Gaussian assumption (i.e., measurement is rejected if its normalized residual absolute value is larger than 3). The estimation is rerun after removing the detected measurement until no residual is flagged as outlying [9].

3 Cyber Attack Models in the State Estimation and Their Consequences

In this section, we introduce several classes of cyber attack models in the static SE problem. We provide an overview of the current state of research and discuss important future directions to enhance the security for the SE and critical systems affected by inaccuracies in SE.

In general, the security of SCADA systems is a real widespread practical concern since their use is pervasive [5]. In fact, SCADA systems require adapted security studies and newly developed tools that go beyond solutions available in Information Technology (IT). For example, SCADA systems installed in power systems are generally inexpensive, vulnerable, and have long life cycles. The life cycles of SCADA sensors are of a few decades, which means that their defense should be adaptable with possible continuous updates.

The existing bad data detectors implemented at control centers are useful for accidental or random sensor and communication channel errors, but are not adapted to counter sophisticated cyber attacks [10–14]. Cyber attacks targeting SE can be classified into different types such as denial-of-service (DoS) where data is not available or missing which can result in certain states to be unobservable; eavesdroppers which analyze the communication traffic to gain private information [7, 15] and raise privacy concerns; and integrity attacks where the data communicated is modified by a "man-in-the-middle" access where attackers are intermediate nodes in the communication. This latter type of attacks is also known as false data injection (FDI) cyber attacks. They can result in intentionally modified measurements communicated to the control center that could change the state in a stealthy fashion where the attacks could, under certain conditions, escape bad data detectors (BDDs) integrated into existing SE modules at energy management systems (EMS). FDI attacks are invisible and hence raise a lot of concern about the operation of the power grid. We will concentrate on this last type of attacks in the following sections.

3.1 False Data Injection Attacks on Measurements

Analyzing (2), we notice that at each step, a linear regression problem is solved where the state increment Δx^k is evaluated from the residual $r = z - h(x^k)$ regressed on $H^{(k)}$. This means that the estimation is run iteratively after linearizing the regression in each step. With slight abuse of notation, the problem can be reformulated as

$$z = Hx + e. \tag{4}$$

The above linear equation or regression represents also the DC formulation problem where the WLS solution is given by $\hat{x} = (H^T H)^{-1} H^T z$. The covariance of the error vector e is assumed to be equal to the identity matrix for simplicity. Notice that the WLS algorithm corresponds to the maximum likelihood estimator under the assumption that the errors are Gaussian [16].

In this context and as proposed in [10, 11], a man-in-the-middle attack could be generated, for example, in the communication between RTUs and the control center. This attack could create a contamination in the measurements by adding the vector equal to a as $z_a = z + a$. In particular, if the attacker has knowledge of the system topology (i.e., the Jacobian matrix), he can generate an attack with $a = Hc$ [11], that is,

$$z_a = z + a = z + Hc. \tag{5}$$

In this case, the attacker is able to change the state estimate to $\hat{x}_a = \hat{x} + c$ where he controls the state vector bias $c \in \mathbb{R}^n$. The residuals are unchanged, i.e., $r_a = z_a - H\hat{x}_a = z - H\hat{x} = r$, which means that the attack is stealthy to the classical bad data detectors (BDD) based on analyzing the residuals. In other words, a bad data detector that analyzes the vector r_a will not detect any change due to the stealthy attack. Stealthy attacks could be generated on both the DC and AC formulations of state estimation as shown in [11, 13]. Due to the sparsity of the power systems and the matrix H, the attacker does not need to target all sensors or have a global knowledge of the topology when targeting a few buses by a stealthy attack. The intrusion would mislead the operator at the control center because he obtains a modified result that does not reflect the actual state of the grid. All consequent actions at the EMS are contaminated by false data injection (FDI) cyber attacks. The impact of bad data and attacks on SE impacting power markets is discussed in [14, 17].

3.2 FDI Attacks Targetting the Topology of the Grid

False data injection (FDI) type attacks could also target the topology of the grid [18–20]. The topology represents the connectivity of the power system and is updated constantly over time in the topology processor. The binary readings from the circuit breakers representing the transmission line states (i.e., open or closed) are communicated to the control center. An intruder can modify these readings as well as the SCADA analog measurements reflecting, for example, power flows on neighboring lines in a coordinated fashion confirming the false state of the line. Such an attack allows a malicious update of the topology undetected by BDD. This type of FDI attacks clearly requires more knowledge and skills of the system by the intruder. The attacker needs the knowledge of the topology and the measurements or the actual grid state. He needs access to the circuit breaker states and the SCADA analog measurements communicated to the control center [18]. The consequences can be more dangerous and complex for the operation than those caused by attacks only on the measurements as considered in the previous subsection. In [18, 20], stealthy cyber attack strategies on both the power state and the topology of the grid are discussed.

Figure 1 illustrates the 14 bus system where bus 5 is targeted by a cyber attack. The system could be decomposed in subsystems as proposed in [22]. For example, subsystem 1 includes buses 1, 2, and 5 and their connecting lines. The other subsystems are cyclic {2, 4, 5}, {2, 3, 4}, {4, 7, 9}, {6, 9, 10, 11, 13, 14}, {6, 12, 13}, {4, 5, 6, 9, 10, 11}, and radial {7, 8} [20, 22]. The decomposition maximizes the number of bad measurements detected while insuring the observability of the whole system [23].

Figure 2a, b illustrate the vulnerability of several estimators [21, 24] toward stealthy attacks targeting the topology and the state through simulations for the IEEE 30 bus system. In both figures, the final state errors and estimate $\hat{x}$ are shown after

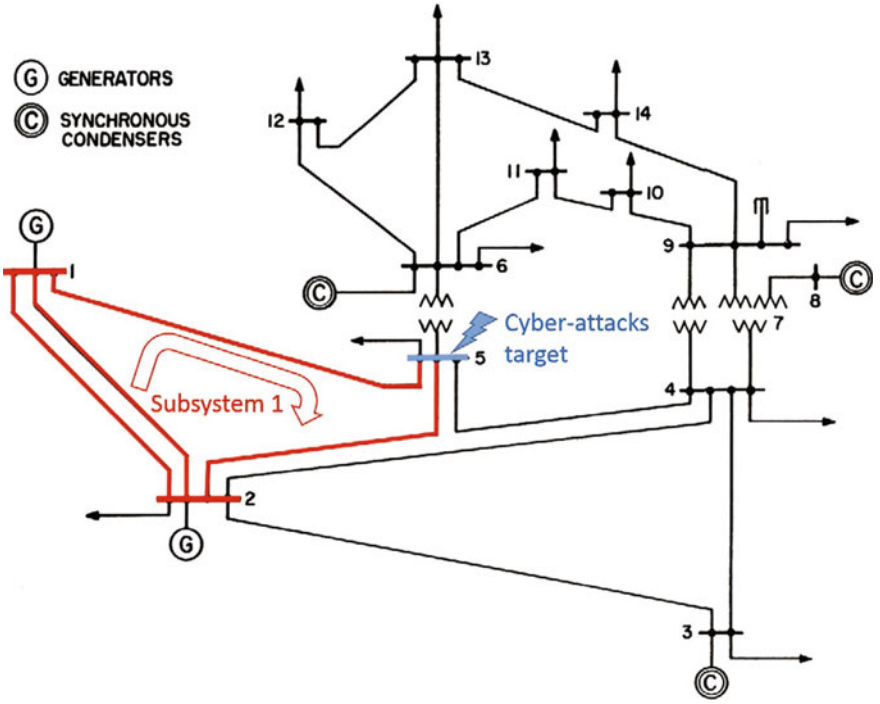
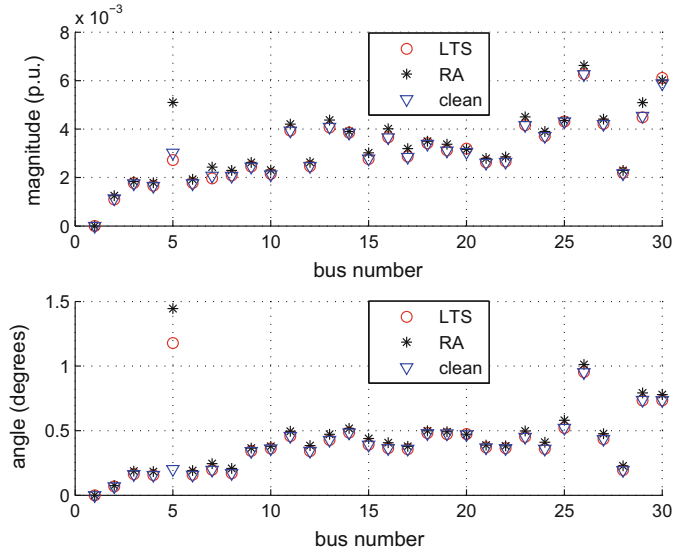
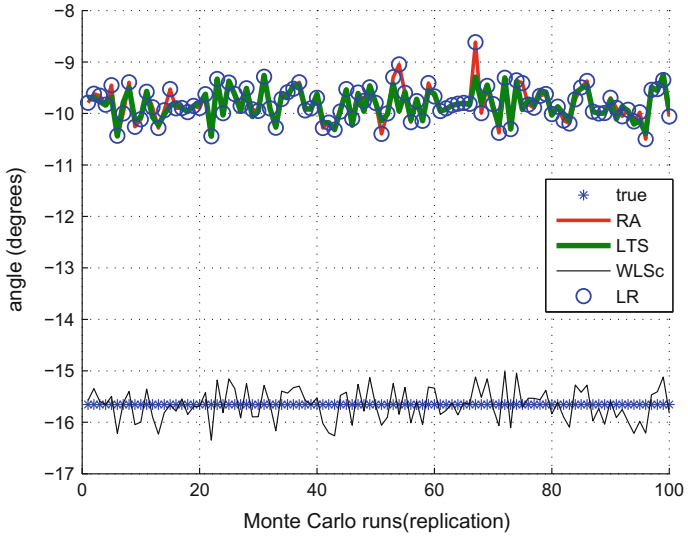


Fig. 1 IEEE 14 bus system (© 2016 IEEE. Reprinted with permission from [39])

cyber-intrusions escaped detection. In this simulation, the true state is obtained from solving a power flow. In practice, the real state is not known by the operator. The figures illustrate the errors in the absence (clean) and presence of stealthy attacks (RA and LTS) assuming the ideal case where the true state is known. In Fig. 2a, the phase angle of a single state at one bus in the system is targeted with a large error (i.e., phase angle at bus 5). In Fig. 2b, the attacker manages to manipulate the value of the final estimated phase at bus 6 because he has enough access to the grid information. If the attacker can target a large number of sensors, then all estimators illustrated in the figure will become vulnerable. In Fig. 2a, RA represents the popular "3σ" rejection rule applied to normalized WLS residuals. The curve labeled "clean" gives the estimation errors in the absence of cyber attacks. In Fig. 2b, WLSc denotes the WLS applied to the clean non-attacked topology and the curve labeled "true" gives the value obtained with the power flow solution, which represents the real state. LNR denotes the popular largest normalized residual rejection [8]. LTS represents the diagnostic of the measurements using the least trimmed squares estimator (LTS). The LTS is a robust estimator that is adapted to handle false data in the topology [8, 16, 23, 25, 26]. It was shown in [20, 22, 23] that the classical commercial BDD



(a) Monte Carlo average absolute error of the SE estimate in the IEEE 30 bus system.



(b) Monte Carlo replications of the SE estimate of the voltage phase angle (deg) at bus 6 in the IEEE 14 bus system.

Fig. 2 Errors of AC power phase angle estimation caused by stealthy cyber attacks targeting the topology (©2015 IEEE. Reprinted with permission from [20, 21])

based on analyzing the residual of the WLS is not effective against random errors and attacks on the topology. Application of robust estimation techniques needs further verification.

3.3 Cyber Security of the PMU-Based State Estimation

Recently, phasor measurement units (PMUs) are being deployed due to the incentives provided by the US Department of Energy [27–29]. PMUs have higher reporting rate (30–120 measurements every second) and are better synchronized than SCADAs due to their use of the Global Positioning System (GPS) clocks [29, 30]. According to the North American SynchroPhasor Initiative (NASPI), around 1800 synchrophasor units or PMUs were available across North America in 2015 [31].

PMUs measure directly the states, i.e., voltage magnitudes and phase angles. The number of available PMUs is, however, still limited in practice because of their associated high costs. Power companies are interested in combining both their existing SCADAs and the newly installed PMUs in estimating the system state using the so-called hybrid state estimator. The state of the grid is estimated at regular intervals, i.e., every several seconds to a few minutes. Novel state estimation algorithms exploiting PMUs are gaining a lot of interest in the recent literature [29, 32–35]. These PMU-based state estimators are important to control the grid using the wide area measurement system (WAMS) technologies [27]. In [33], the authors proposed to buffer the data from PMUs to resolve the disparity in the reporting frequency between SCADAs (every few seconds) and PMUs (every 1/30 s). An optimal buffer length could be derived to ensure a good trade-off between tracking the fast changes in the grid states versus maximizing the time interval of the data exploited from PMUs to increase the accuracy of the estimates [33, 36].

Monitoring the grid with PMUs that are capable of delivering large amounts of real-time data creates cyber-vulnerabilities. Indeed, PMUs are vulnerable to both random bad data and cyber attacks [27, 35, 37, 38]. For example, intruders could create attacks by spoofing the GPS clocks of PMUs. However, the delivered data could be exploited in a clever way to improve both the cyber security and the operation of the grid. Practical and novel algorithms could be exploited to notify the operator at the control center when abnormal measurements are detected [39]. Furthermore, these techniques could correct the bad data introduced by cyber attacks automatically and secure the control in the power grid. One important research direction consists of proposing data-driven algorithms and power system model-based approaches that improve the cyber security of the whole power system operation.

Modeling time and space dependencies in multiple PMUs and estimating the existing correlation could be used in order to detect outliers or cyber attacks in PMU signals [38, 40, 41]. This approach improves also the accuracy of the hybrid state estimation. The technique proposed in [38] provides a sophisticated defense mechanism against stealthy cyber attacks and was shown to make the task of cyber attackers extremely complicated and tedious. The preliminary simulation results have

considered an SE resolution of 2 s. This implies that every 2 s, a new estimate of the grid state is obtained, which might be considered to be a low resolution in the future power grid. Several authors have recently proposed to reconstruct the power states from PMU measurements to increase the SE resolution in order to track the rapid changes expected in the future smart grid [34, 42]. The SE will be refreshed very frequently (i.e., every few fractions of a second), which will completely change the real-time control of the power systems. This is an important emerging area for future studies.

Furthermore, the dynamic state estimation, which has gained interest thanks to the available PMU measurements, is executed in a nonlinear context using extended Kalman filters (EKF) [43] or unscented Kalman filters (UKF) [44]. Using a dynamic SE in the WAMS context enables the anticipation of power system dynamics and necessary fast controls. To improve the practical implementation of the dynamic SE, the authors in [45] proposed a decentralized algorithm that uses the UKF. Both the EKF and the UKF are vulnerable to bad data [25, 46] and cyber attacks [47]. The reference [48] shows the possibility of generating stealthy attacks in the general case of networked control systems obeying a dynamic linear state space representation. The theoretical results could be adapted to the case of power state estimation problem. Recently, some authors have implemented robust versions of both EKF and UKF using robust methods such as the Generalized M-estimator [46] and the least absolute value [35]. Offline PMU-based diagnostic techniques that improve the detection of cyber attacks [49] and errors on the topology or parameters are also being developed [50]. These techniques consist generally in identifying vulnerable sensors to be secured. Exploiting forecasts of PMUs and loads could improve the robustness and cyber security of the SE as proposed recently in [51]. Effective cyber security solutions considering realistic large power systems and hybrid state estimation for both static and dynamic approaches that handle attacks on PMU signals remain necessary for future grid operation security.

3.4 Assessing SE Cyber-Vulnerabilities and Their Consequences on the Power Grid Operation

So far, our discussion on security has been limited to SE on its own. However, assessing the impacts of cyber attacks targeting the power state estimation is very important in order to evaluate the danger of the different cyber attack types and configurations. That is, we must go beyond quantifying the power state modification to analyze the real cascading consequences of cyber attacks on contingency analysis, control actions, power markets, and power flows. While this issue is very vast and is outside the scope of this chapter, we would like to mention a few important directions for future research.

Developing and implementing metrics to assess the cyber security of practical power systems is necessary. Such metrics could be developed considering not only

the impacts on the security of the operation but also the economic impacts on power markets. Some authors are starting to study cyber attacks consequence on power markets [14, 17], system operation [19] and tools to quantify cyber security [52]. Cyber attacks consequences will be quantified by static and dynamic studies on realistic systems. To reach this goal several universities are developing cyber security testbeds for the smart grid that emulate the real-time behavior of a large power system [53–56]. Testbeds are necessary to research the cyber-vulnerabilities that account for the complexity and the different interactions between the system part and the cyber part of the smart grid in real-time conditions. Fluctuations in frequency and power flows, oscillation modes, and voltage magnitudes will be considered in deriving these metrics for cyber security quantification. This will allow to rank the proposed cyber security methods and enable combining different solutions in an optimal and cost-effective way in order to secure the grid operation.

4 Future Directions

Here, we outline several future research directions related to the SE problem from a slightly broader perspective.

The cyber security solutions discussed so far can be classified into two main categories, online and offline solutions [51]. The offline solutions are remedial actions developed offline with no time constraints on the computation. An example of such methods consists of finding the minimum number of sensors to be secured and their positions in order to make a stealthy attack unfeasible [11, 17, 49]. On the other hand, online solutions are techniques that update their capabilities and models in real time using available sensed data. An example of the latter solutions consists of implementing robust estimation tools that detect an attack by comparing the modified measurement to a majority of clean data collected and analyzed in real time.

Sophisticated robust estimation tools have been developed recently in the signal processing and statistics literature [16, 25]. These methods are becoming practical thanks to the fast-evolving computation power. Novel techniques could be developed or adapted from robust statistics and signal processing to improve the detection of cyber attacks. This has the advantage of providing online adaptable methods that could reduce investments in expensive secure sensors. Robust signal processing methods and machine learning techniques exploit newly available data to update their models and detection procedures [57, 58].

For example, to enhance the overall cyber security of the static AC SE, the work in [39] introduces an approach that runs several robust least trimmed squares (LTS) estimators with different breakdown points or rejection percentages in parallel to improve the detection of cyber attacks targeting both the measurements and the topology of the grid. This approach allows us to not only robustly estimate but also accurately identify the presence of attacks. Also, as an alternative approach to detect the presence of stealthy cyber attacks, machine learning techniques are exploited in [57, 58]. The work in [59] introduces a statistical outlier detection approach

using a recently proposed machine learning technique called density ratio estimation (DRE) [60]. Combining such different techniques should be further investigated.

While the proposed methods in the literature are effective and promising on computer simulated data and theoretically justified, their performance and implementation rely heavily on the power system complexity and collected data used during the estimation or the learning process. The collected data should be as realistic as possible to validate the effectiveness of the proposed methods in practical control centers allowing their real implementation. Cyber security testbeds are necessary to collect large amounts of data from SCADAs and PMUs to assess the performance of the proposed methods in real-life conditions. Investigating the sensitivity of the proposed machine learning methods, for example, when attacks are present in the learning process is of great interest. Furthermore, decomposing the grid in several subsystems (Fig. 1) and executing the proposed algorithms in a distributed fashion to reduce the computational burden allows the implementation of the online defense. Some authors proposed distributed state estimation methods [29, 61–63]. A trade-off should be ensured between a decomposition that maximizes detection versus a decomposition that reduces execution times. Finally, power systems are very sparse, i.e., each bus is connected only to a limited number of buses. Sparsity should be considered when adapting the robust techniques both to evaluate their robustness characteristics [26] and their implementation algorithms.

Moving target defense (MTD) is useful to defend the SE against cyber attacks. The objective of the MTD is to increase the complexity of the system so as to increase the attack cost for the intruder by reducing his knowledge of the system. This objective is achieved in [64] by randomizing the set of measurements and the topology of the grid. The topology of the grid change is reflected by a few changing line impedances thanks to distributed flexible AC transmission system (D-FACTs). The work [65] proposed to randomize the set of measurements as well and obtained an improved cyber security of the SE. This research direction could be explored further by improving the randomization and integrating PMUs as well.

For the case of an increased SE resolution to track fast changes in the future power systems, cyber security becomes even more challenging since the procedure will be fully automatic and the algorithms implemented to secure the operation need to converge very fast. Reference [34] proposed a method that provides robustness against random errors occurring in PMU sensors but sophisticated cyber attacks were not studied. Furthermore, the dynamic state estimation, which is also gaining interest and is vulnerable to both bad data and cyber attacks [46, 47], will allow even the anticipation of the control in the wide area measurement systems (WAMS).

The state estimation at distribution level is also a very interesting research topic for future investigation [66]. It may improve the monitoring of distribution systems especially with increased distributed generation and storage such as photovoltaic panels (PVs) and electric vehicles. The SE at the distribution level has been considered as more challenging because of the limited measurements redundancy and

the imbalance at the distribution level requiring to consider the three phases separately [66]. This research could also enhance the control of the distribution systems which are vulnerable to cyber attacks [67, 68].

Finally, control is evolving with the development of wide area measurement system (WAMS) technologies [27, 69]. The authors in [70] have shown the vulnerability of the automatic generation control (AGC) module at the EMS toward cyber attacks. The AGC provides automatic frequency regulation of the power system while insuring that the scheduled power exchanges between adjacent power areas and utilities are met. In [37], the authors studied the effect of cyber attacks spoofing the GPS clocks of PMUs. They proposed algorithmic solutions to secure the damping of inter-area oscillation modes in the WAMs that will be deployed to control the future grid. The classical (N-1) secure operation of the grid criteria is not sufficient in the context of cyber-intrusions. Since the consequences of cyber attacks are tremendous on the grid, several layers of defense measures should provide resistance against the effects of cyber attacks. If a cyber attack is missed by the sophisticated data-analytic tools or a cyber attack is introduced directly in the control orders sent to controllers, relays, tap changers or Industrial Control Systems (ICS) at Remote Terminal Units (RTUs), the power system should be able to mitigate or limit the bad consequences using resilient and robust control.

5 Conclusions

The state estimation problem has significantly raised the concerns in the last decade about its vulnerability and security toward cyber attacks. The importance of state estimation is significant in the operation of the smart grid where it can be exploited not only in creating vulnerabilities and intrusions but also in implementing security measures. In this chapter, the critical current and future research applied to improve the state estimation safety against threats from the cyberspace has been discussed. Improving the cyber security of the state estimation combines multilayer defense systems. Novel robust signal processing and data-analytic methods could be very effective especially with the presence of synchrophasor measurements. Assessing the cyber security of the grid by evaluating the impact of undetected attacks is crucial. Proposing techniques for resilient control that limits and mitigates the impact of undetected attacks would complement the detection of attacks to ensure a secure and efficient operation of the grid. In general, the discussed research could be adapted to many engineering fields where industrial control systems are implemented. Hence, these directions should be explored further for the enhancement of the cyber security for the safety and well-being of the society.

Acknowledgements This work was supported by Japan Science and Technology Agency under the CREST Program, Grant No. JPMJCR15K3.

References

1. Terrorism and the electric power delivery system. Technical Report (National Academy of Engineering Press, U.S., 2012)
2. S.K. Khaitan, J.D. McCalley, C.C. Liu, *Cyber Physical Systems Approach to Smart Electric Power Grid* (Springer, Heidelberg, 2015)
3. IR-ALERT-H-16-056-01-Cyber-attack against Ukrainian critical infrastructure. Technical Report Industrial Control Systems Cyber Emergency Response Team, https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01, Feb 2016
4. Strengthening America's energy security with offshore wind. Technical Report (U.S. Department of Energy (DoE)), http://www.nrel.gov/docs/fy12osti/49222.pdf, Apr 2012
5. T.G. Lewis, *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation* (Wiley, New Jersey, second edition, 2015)
6. M. Govindarasu, P.W. Bauer (eds.), Special section on keeping the smart grid safe. IEEE Power Energy Mag. **10**(1) (2012)
7. Y. Mo, T.H.-H. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, B. Sinopoli, Cyber-physical security of a smart grid infrastructure. Proc. IEEE **100**(1), 195–209 (2012)
8. A. Abur, A. Gomez-Exposito, *Power System State Estimation: Theory and Implementation* (CRC Press, New York, 2004)
9. A. Monticelli, Electric power system state estimation. Proc. IEEE **88**(2), 262–282 (2000)
10. Y. Liu, M.K. Reiter, P. Ning, False data injection attacks against state estimation in electric power grids, in *Proceedings of 16th ACM Conference on Computer and Communications Security* (2009), pp. 21–32
11. Y. Liu, P. Ning, M.K. Reiter, False data injection attacks against state estimation in electric power grids. ACM Trans. Inf. Syst. Secur. **14**(1), 1–33 (2011)
12. A. Teixeira, S. Amin, H. Sandberg, K.H. Johansson, S.S. Sastry, Cyber security analysis of state estimators in electric power systems, in *Proceedings of 49th IEEE Conference on Decision and Control (CDC)* (2010), pp. 5991–5998
13. G. Hug, J.A. Giampapa, Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks. IEEE Trans. Smart Grid **3**(3), 1362–1370 (2012)
14. L. Jia, J. Kim, R.J. Thomas, L. Tong, Impact of data quality on real-time locational marginal price. IEEE Trans. Power Syst. **29**(2), 627–636 (2014)
15. W. Wang, Z. Lu, Cyber security in the smart grid: survey and challenges. Comput. Netw. **57**(5), 1344–1371 (2013)
16. R.A. Maronna, R.D. Martin, V.J. Yohai, *Robust Statistics: Theory and Methods* (Wiley Series in Probability and Statistics. Wiley, Chichester, 2006)
17. O. Kosut, L. Jia, R.J. Thomas, L. Tong, Malicious data attacks on the smart grid. IEEE Trans. Smart Grid **2**(4), 645–658 (2011)
18. J. Kim, L. Tong, On topology attack of a smart grid: undetectable attacks and countermeasures. IEEE J. Sel. Areas Commun. **31**(7), 1294–1305 (2013)
19. A. Ashok, M. Govindarasu, Cyber attacks on power system state estimation through topology errors, in *IEEE Power Energy Society General Meeting* (2012), pp. 1–8
20. Y. Chakhchoukh, H. Ishii, Coordinated cyber-attacks on the measurement function in hybrid state estimation. IEEE Trans. Power Syst. **30**(5), 2487–2497 (2015)
21. Y. Chakhchoukh, H. Ishii, Cyber attacks scenarios on the measurement function of power state estimation, in *Proceedings of American Control Conference (ACC)*, June 2015, pp. 3676–3681
22. M.G. Cheniae, L. Mili, P.J. Rousseeuw, Identification of multiple interacting bad data via power system decomposition. IEEE Trans. Power Syst. **11**(3), 1555–1563 (1996)
23. L. Mili, M.G. Cheniae, P.J. Rousseeuw, Robust state estimation of electric power systems. IEEE Trans. Circuits and Syst. I Fundam. Theory Appl. **41**(5), 349–358 (1994)
24. Y. Chakhchoukh, H. Ishii, Robust estimation for enhancing the cyber security of power state estimation, in *IEEE PES General Meeting*, July 2015, pp. 1–6

25. A.M. Zoubir, V. Koivunen, Y. Chakhchoukh, M. Muma, Robust estimation in signal processing: a tutorial-style treatment of fundamental concepts. IEEE Signal Process. Mag. **29**(4), 61–80 (2012)
26. L. Mili, C.W. Coakley, Robust estimation in structured linear regression. Ann. Statist. **24**(6), 2593–2607 (1996)
27. A. Chakrabortty, P.P. Khargonekar, Introduction to wide-area control of power systems, in *Proceedings of American Control Conference*, June 2013, pp. 6758–6770
28. F. Aminifar, M. Fotuhi-Firuzabad, A. Safdarian, A. Davoudi, M. Shahidehpour, Synchrophasor measurement technology in power systems: panorama and state-of-the-art. IEEE Access **2**, 1607–1628 (2014)
29. M. Kezunovic, S. Meliopoulos, V. Venkatasubramanian, V. Vittal, *Application of Time-Synchronized Measurements in Power System Transmission Networks* (Springer, Heidelberg, 2014)
30. A.G. Phadke, J.S. Thorp, *Synchronized Phasor Measurements and Their Applications, Power Electronics and Power Systems*, 2nd edn. (Springer, New York, 2008)
31. Map of PMUs in North America. Technical Report (North American Synchrophasor Initiative, March 2015)
32. B. Xu, A. Abur, Optimal placement of phasor measurement units for state estimation. Technical Report (Power Systems Engineering Research Center (PSERC), 2005)
33. Q. Zhang, Y. Chakhchoukh, V. Vittal, G.T. Heydt, N. Logic, S. Sturgill, Impact of PMU measurement buffer length on state estimation and its optimization. IEEE Trans. Power Syst. **28**(2), 1657–1665 (2013)
34. M. Göl, A. Abur, A hybrid state estimator for systems with limited number of PMUs. IEEE Trans. Power Syst. **30**(3), 1511–1517 (2015)
35. A. Rouhani, A. Abur, Linear phasor estimator assisted dynamic state estimation. IEEE Trans. Smart Grid **9**(1), 211–219 (2018)
36. V. Murugesan, Y. Chakhchoukh, V. Vittal, G.T. Heydt, N. Logic, S. Sturgill, PMU data buffering for power system state estimators. IEEE Power Energy Technol. Syst. J. **2**(3), 94–102 (2015)
37. Y. Wang, A. Chakrabortty, Distributed monitoring of wide-area oscillations in the presence of GPS spoofing attacks, in *Proceedings of IEEE Power and Energy Society General Meeting (PESGM)*, July 2016, pp. 1–5
38. Y. Chakhchoukh, V. Vittal, G.T. Heydt, H. Ishii, LTS-based robust hybrid SE integrating correlation. IEEE Trans. Power Syst. **32**(4), 3127–3135 (2017)
39. Y. Chakhchoukh, H. Ishii, Enhancing robustness to cyber-attacks in power systems through multiple least trimmed squares state estimations. IEEE Trans. Power Syst. **31**(6), 4395–4405 (2016)
40. Y. Chakhchoukh, V. Vittal, G.T. Heydt, PMU based state estimation by integrating correlation. IEEE Trans. Power Syst. **29**(2), 617–626 (2014)
41. M. Wu, L. Xie, Online identification of bad synchrophasor measurements via spatio-temporal correlations, in *Proceedings of Power Systems Computation Conference (PSCC)*, June 2016, pp. 1–7
42. M. Glavic, T. Van Cutsem, Reconstructing and tracking network state from a limited number of synchrophasor measurements. IEEE Trans. Power Syst. **28**(2), 1921–1929 (2013)
43. E. Ghahremani, I. Kamwa, Dynamic state estimation in power system by applying the extended Kalman filter with unknown inputs to phasor measurements. IEEE Trans. on Power Syst. **26**(4), 2556–2566 (2011)
44. S. Wang, W. Gao, A.P.S. Meliopoulos, An alternative method for power system dynamic state estimation based on unscented transform. IEEE Trans. Power Syst. **27**(2), 942–950 (2012)
45. A.K. Singh, B.C. Pal, Decentralized dynamic state estimation in power systems using unscented transformation. IEEE Transa. Power Syst. **29**(2), 794–804 (2014)
46. J. Zhao, M. Netto, L. Mili, A robust iterated extended Kalman filter for power system dynamic state estimation. IEEE Trans. Power Syst. **32**(4), 3205–3216 (2017)
47. O. Kosut, Malicious data attacks against dynamic state estimation in the presence of random noise, in *Proceedings of IEEE Global Conference on Signal and Information Processing*, Dec 2013, pp. 261–264

48. A. Teixeira, I. Shames, H. Sandberg, K.H. Johansson, A secure control framework for resource-limited adversaries. Automatica **51**, 135–148 (2015)
49. J. Kim, L. Tong, On phasor measurement unit placement against state and topology attacks, in *Proceedings of IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Oct 2013, pp. 396–401
50. Y. Lin, A. Abur, Strategic use of synchronized phasor measurements to improve network parameter error detection. IEEE Trans. Smart Grid **9**(5), 5281–5290 (2018)
51. A. Ashok, M. Govindarasu, V. Ajjarapu, Online detection of stealthy false data injection attacks in power system state estimation. IEEE Trans. Smart Grid **9**(3), 1636–1646 (2018)
52. A. Teixeira, K.C. Sou, H. Sandberg, K.H. Johansson, Secure control systems: a quantitative risk management approach. IEEE Control Syst. **35**(1), 24–45 (2015)
53. C.M. Davis, J.E. Tate, H. Okhravi, C. Grier, T.J. Overbye, D. Nicol, SCADA cyber security testbed development, in *Proceedings of 38th North American Power Symposium*, Sept 2006, pp. 483–488
54. A. Hahn, A. Ashok, S. Sridhar, M. Govindarasu, Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid. IEEE Trans. Smart Grid **4**(2), 847–855 (2013)
55. T. Yardley, R. Berthier, D. Nicol, W.H. Sanders, Smart grid protocol testing through cyber-physical testbeds, in *Proceedings of IEEE PES Innovative Smart Grid Technologies Conference (ISGT)*, Feb 2013, pp. 1–6
56. V. Venkataramanan, A. Srivastava, A. Hahn, Real-time co-simulation testbed for microgrid cyber-physical analysis, in *Proceedings of Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES)*, April 2016, pp. 1–6
57. M. Esmalifalak, N.T. Nguyen, R. Zheng, Z. Han, Detecting stealthy false data injection using machine learning in smart grid, in *Proceedings of IEEE Global Communications Conference (GLOBECOM)*, Dec 2013, pp. 808–813
58. M. Esmalifalak, L. Liu, N. Nguyen, R. Zheng, Z. Han, Detecting stealthy false data injection using machine learning in smart grid. IEEE Syst. J. **11**(3), 1644–1652 (2017)
59. Y. Chakhchoukh, S. Liu, M. Sugiyama, H. Ishii, Statistical outlier detection for diagnosis of cyber attacks in power state estimation, in *Proceedings of IEEE PES General Meeting*, July 2016, pp. 1–5
60. M. Sugiyama, T. Suzuki, T. Kanamori, *Density Ratio Estimation in Machine Learning* (Cambridge University Press, 2012)
61. L. Xie, D.H. Choi, S. Kar, H.V. Poor, Fully distributed state estimation for wide-area monitoring systems. IEEE Trans. Smart Grid **3**(3), 1154–1169 (2012)
62. W. Jiang, V. Vittal, G.T. Heydt, A distributed state estimator utilizing synchronized phasor measurements. IEEE Trans. Power Syst. **22**(2), 563–571 (2007)
63. V. Kekatos, G.B. Giannakis, Distributed robust power system state estimation. IEEE Trans. Power Syst. **28**(2), 1617–1626 (2013)
64. M.A. Rahman, E. Al-Shaer, R.B. Bobba, Moving target defense for hardening the security of the power system state estimation, in *Proceedings of the First ACM Workshop on Moving Target Defense*, Nov 2014, pp. 59–68
65. Y. Yao, Z. Li, MTD-inspired state estimation based on random measurements selection, in *North American Power Symposium (NAPS)*, Sept 2016, pp. 1–6
66. R. Singh, B.C. Pal, R.A. Jabr, Choice of estimator for distribution system state estimation. IET Gener. Trans. Distrib. **3**(7), 666–678 (2009)
67. Y. Isozaki, S. Yoshizawa, Y. Fujimoto, H. Ishii, I. Ono, T. Onoda, Y. Hayashi, Detection of cyber attacks against voltage control in distribution power grids with PVs. IEEE Trans. Smart Grid **7**(4), 1824–1835 (2016)
68. A. Teixeira, G. Dan, H. Sandberg, R. Berthier, R.B. Bobba, A. Valdes, Security of smart distribution grids: Data integrity attacks on integrated volt/var control and countermeasures, in *Proceedings of American Control Conference*, June 2014, pp. 4372–4378
69. A. Chakrabortty, Co-designing communication and control systems for wide-area control of power systems, in *Proceedings of American Control Conference (ACC)*, July 2016, pp. 2667–2667
70. S. Sridhar, M. Govindarasu, Model-based attack detection and mitigation for automatic generation control. IEEE Trans. Smart Grid **5**(2), 580–591 (2014)