Energy Big Data Security Threats in IoT-Based Smart Grid Communications

Wen-Long Chin, Wan Li, and Hsiao-Hwa Chen

To deal with security threats, energy big data should be thoughtfully stored and processed to extract critical information, and security and blackout warnings should be given in an early stage. The authors present a comprehensive tutorial and survey to highlight research challenges related to these issues in the IoT-based smart grid.

Abstract

Increased intelligence and automation in smart grid results in many heterogeneous applications benefiting from the Internet of Things, such as demand response, energy delivery efficiency/reliability, and fault recovery. However, vulnerabilities in smart grid arise due to public communication infrastructure and Internet-based protocols. To deal with security threats, energy big data should be thoughtfully stored and processed to extract critical information, and security and blackout warnings should be given in an early stage. This work gives a comprehensive tutorial and survey to highlight research challenges on the aforementioned issues in the Internet-of-Things-based smart grid. We demonstrate that a stealthy and blind energy big data attack can be launched using a replay scheme. Also, we elucidate an intuitive geometric viewpoint for this type of attack. The proposed attack can bypass bad data detection successfully using either DC or AC state estimation.

Introduction

The Internet of Things (IoT) is an emerging technology expected to change our daily life rapidly. Via interworking of different devices, any physical object/thing can be integrated seamlessly for exchanging and collecting data. Objects in the physical world, including fridges, heaters, televisions, and so on, could be easily accessible and manageable. The IoT allows devices to be sensed and controlled remotely across existing networks, resulting in improved efficiency and economic benefits. With the IoT technology, smart grid (SG) becomes an instance of cyber-physical systems [1, 2] The development of most parts of SG can be enhanced by applying IoT. Through IoT, the whole power grid chain, from electricity generation to consumption, will enable intelligence and two-way communication capabilities to monitor and control the power grid anywhere and anytime.

While the IoT technology is very important in the context of SG, it could also lead to disasters since the operations of SG are based on Internet-based protocols [3, 4]. Therefore, the utility is exposed to general information and communication technology (ICT) threats, such as denial of service (DoS) attacks and domain-specific attacks (e.g., targeted malware such as Stuxnet). As a consequence, an attacker could create huge financial losses and damages to the utility by inducing real-time imbalance between energy consumption and generation through data manipulation. If the operators cannot locate the vulnerabilities of the SG rapidly and accurately, it is easy to trigger serious events leading to a breakdown of a power grid. Therefore, secure, reliable, and real-time situational awareness is critical for future power grids.

The pervasive deployment of smart metering in IoT-based SG will generate energy big data in terms of its huge volume, large scale, and structural variety. Three categories of grid business data are listed as follows [5]:

1. Grid operation and equipment testing or monitoring data, such as supervisory control and data acquisition (SCADA) data and sampling data of smart meters
2. Electric power marketing data, such as transaction price and electricity sales data
3. Electric power management data, such as internal grid data

These data must be processed in a parallel and distributed fashion to extract critical information for decision making processes within a limited time. According to inherent data structure, energy data are divided into structured and unstructured data. Structured data includes data mainly stored in relational databases.

The growth rate of structured data is extremely high. Big data will lead to the challenges in distributed storage of power systems, and a distributed storage system for managing structured data that is designed to scale to a very large size is desirable. There are many potential advantages to be derived from energy data for the goal of optimal operation, including real-time monitoring of energy consumption data generated by advanced metering infrastructure (AMI) and smart meters, detection of energy losses by fault or fraud, early blackout warning, fast detection of disturbances in energy supply, and intelligent energy generation, planning, and pricing. Huge data generated at the second level and concurrent peak demands from different homes may cause blackouts at some substations due to power imbalance introduced by inaccurate energy forecast. Energy big data are also very useful for realizing situational awareness. Based on long-term monitoring, security-related information can also be characterized.

In this work, we demonstrate a stealthy and blind energy big data attack using a replay mechanism without requiring the information of power grid topology and transmission-line admittances. In contrast to conventional data falsification attacks using cumbersome mathematical approaches, we elucidate an intuitive geometric approach for this

This work was supported in part by the Ministry of Science and Technology of Taiwan (105-2221-E-006-019-MY2 and 104-2221-E-006-081-MY2).

Digital Object Identifier: 10.1109/MCOM.2017.1700154

The authors with National Cheng Kung University.

type of attack. The proposed attack can bypass bad data detection (BDD) successfully via either direct current (DC) or alternating current (AC) state estimation. Interesting readers can refer to [6] for more information about the state estimation.

The major contributions of this work are outlined as follows.

- We survey the security and energy big data analytics issues of IoT-based SGs. The potential applications of energy big data analytics are also introduced. Future research challenges are outlined for the IoT-based SG applications.
- We demonstrate a new energy big data attack employing a replay approach with both DC and AC state estimations. To the best of our knowledge, no works have been done to study data falsification attacks using an AC power flow model. No reports have appeared on launching blind AC attacks without grid parameters, such as transmission-line admittances.
- The effectiveness of the proposed big data attack is verified by simulations.

The rest of this article can be outlined as follows. Security and energy big data analytics issues are discussed. We illustrate the proposed big data attack, and we evaluate the performance and vulnerability of IoT-based SG. We highlight future research challenges. Finally, we draw the conclusions of this article.

Security and Energy Big Data Analytics Issues

IoT-Based Smart Grid Security Issues

Security in critical utility infrastructure is a very serious concern and involves many factors, including physical security of plants and facilities, SCADA, intelligent electronic devices (IEDs) and meters, cyber security for networking and computing, and security management for the utility. The SG will encompass billions of smart objects via IoT networks, including smart meters, smart appliances, sensors, actuators, and so on. However, there have been a lot of concerns regarding vulnerabilities of the SG. The security threats outlined below are the major factors impeding rapid and wide deployment of the IoT-based SG [7–9].

Impersonation: The attacker acts on behalf of a legitimate user in an unauthorized way. To solve this problem, a framework of machine-to-machine authentication in SG via a two-layer approach was proposed in [10].

Eavesdropping: Since the IoT uses public communication networks, an attacker can easily intercept the energy consumption information of households.

Data manipulation: Modifying exchanged data may cause service impairment threats, such as DoS, compromise of service, and corruption of energy data. Recently, a DC blind false data attack [11] was reported without knowing power grid topology and transmission-line admittances.

Access and authorization: Distributed devices can be accessed and controlled remotely. Meters and other devices can be compromised by malicious software codes. The infiltration threat relates to the penetration of a secure perimeter by an unauthorized access, and can allow other threats to be exercised.

Availability: Large-scale IoT-based SGs are vulnerable to IP-based attackers, making them partially or totally unavailable as a result of DoS attacks [12].

Energy Big Data Analytics Issues in IoT-Based Smart Grid

Upgrading utility networks will force electricity providers to process far more information than ever before [13]. To make full use of the new data, the utility companies will need complex event-processing capabilities as listed below.

Scalable, interoperable, and distributed computing infrastructure: As SG is a highly distributed system, a huge amount of data is collected from every section, including energy generation, transmission, distribution, and renewal energy powered vehicles and smart meters. It is very challenging to store, share, and process such volume, velocity, and variety (3V) big data.

Real-time big data intelligence: Real-time decision is essential for both system operation and real-time pricing. Intelligent decision making needs to process current and past data. With the real-time constraints, it will be extremely challenging to design new algorithms that can provide intelligence for processing such big data.

Big data knowledge representation and processing: Big data analytics requires new machine learning and artificial intelligence theories. However, the outputs from machine learning and artificial intelligence typically lack intuitive interpretation and unified representation. Such a data mining task is challenging due to the huge data nature of smart energy data.

Big data security and privacy: Although many security solutions have been proposed for SGs, they were not designed or customized specifically for energy big data. Attacks that make inferences directly from the energy big data can mislead the BDD so that fake data are unable to be detected. Also, the data can contain sensitive and private information of the customers and lead to usage pattern attacks. Most importantly, such data can be used to impact decision making on safe operation of the critical infrastructure.

Cyber-physical coupling modeling: One of the best known security features in SGs is tight cyber-physical coupling between the physical grid and cyber information, which exhibit multiple and distinct behavioral modalities and are deeply intertwined. A good understanding of it will be essential for ensuring the security of SG infrastructures.

One of the best known security features in SGs is a tight cyber-physical coupling between the physical grid and cyber information, which exhibit multiple and distinct behavioral modalities and are deeply intertwined. A good understanding of it will be essential for ensuring the security of SG infrastructures.

Big Data Analytics and Applications in Smart Grid

Energy big data analytics is a very important research topic involving large distributed infrastructures, such as big data generation, transmission, storage, sharing, and processing. In addition to traditional challenges of big data analytics, energy big data analytics will also encounter difficulties in dealing with the unique features arising from tight cyber-physical coupling.

The required techniques involve a number of disciplines, including artificial intelligence, statistics, pattern recognition, machine learning, data mining, signal processing, and optimization and visualization methods. Big data analytics includes classification, aggregation, clustering, and data mining, as briefly described below.

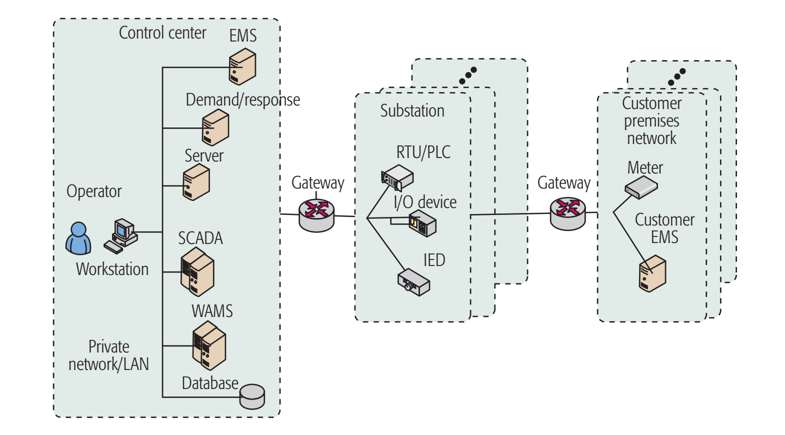

Figure 1. The management and control network of power grids with an emphasis on the distribution level.

Classification: Classification of a large volume of data is the process of organizing data according to its categories for its most effective and efficient use, also referred to as mining classification rules, a major application of data mining technology.

Aggregation: Data aggregation is a kind of data and information mining technique, where data is explored and presented in a report-based or shortened format to reduce computational cost.

Clustering: Clustering analysis can be used as an independent tool to obtain data distribution. Based on feature extraction and classification, the accuracy and efficiency of data mining can be improved.

Data mining: Via various methods, including artificial intelligence, machine learning, statistics, and database systems, useful patterns in large datasets can be extracted and transformed into a convenient and concise form.

To improve the reliability and efficiency of SG operation, power utilities are employing IT technology to develop big data applications [14].

We summarize some potential applications based on big data analytics in SG as follows:
- Load management with demand response
- Performance and efficiency analyses for power generation and storage systems
- Power grid optimization and capital expense minimization
- Large-scale and distributed state estimation based on AMI and smart devices
- Asset management by distributed islanding and aging transformer replacement
- Prediction and analysis of economic situation and social impact
- Pricing analysis and energy utilization
- Information provision for customers to better manage energy usage and bills, customer service enhancement, and customer behavior analysis
- Restoration spatial view of customer information, including trouble tickets, troubleshooting and fault localization, and real-time outage indication
- Scientific reasoning for policy making processes

Energy Big Data Attacks

System Model

The SG is a new electricity network, which encompasses advanced sensing and measurement technologies, ICTs, analytical and decision-making technologies, as well as the current power grid infrastructure. Figure 1 illustrates the management and control network of power grids with an emphasis on its distribution level. In the control center, the energy management system (EMS) consisting of BDD is a system of computer-aided tools used by operators to monitor, control, and optimize the performance of generation, transmission, and distribution of electrical power; the SCADA system is responsible for monitoring and control functions of the grid; wide area monitoring systems (WAMSs) employ new data acquisition technology based on phasor measurement and allow monitoring the conditions of a power system over a large-scale area to counteract grid abnormalities; and the database stores meter data, transmission admittance, topology information, system state, and so on. As a part of EMS applications, demand response provides an opportunity for consumers to play a role in the operation of the electric grid by reducing their electricity usage during peak load hours to save cost.

The programmable logic controllers (PLCs) and remote terminal units (RTUs) control devices autonomously without a master computer; the I/O devices are sensors and actuators; and the IEDs are microprocessor-based controllers of circuit breakers, feeders, substation transformers, capacitor banks, and phasor measurement units (PMUs). The EMS allows a customer to track its energy use in an easy format on computers or handheld devices.

Energy Big Data Replay Attack

The evolution from old power grids to SG brings new challenges in security. Hackers can eavesdrop or intercept metering data or steal big data from the distributed databases via malware. Normally, the grid parameters are unlikely to be known and often critically protected. Exposure of the structured data can cause losses in utilities or even a severe power imbalance problem. We demonstrate that a stealthy attack with both DC and AC state estimations can be successfully launched for misleading a power system through a replay mechanism. We call it an energy big data replay attack. The problem of interest can be formulated as follows.

Given a measurement vector set $\mathbf{z}_d$, $d = 1, 2, \ldots, D$, obtained from the energy big data, an energy big data attack can cheat the BDD as if no fabricated data exist. Or it can be detected by the BDD with a negligible probability. In addition to DC state estimation, the nonlinear AC state estimation is used inevitably in power systems because the AC state estimation has its advantages, including accuracy, ability against data manipulation attacks, and so on. Therefore, the attack should be able to pass the BDD using either DC or AC state estimation. For practicality, the power grid topology and transmission line admittances are not necessarily known to the attacker; therefore, this is a type of blind attack [11].

According to the criteria of a stealthy attack against AC state estimation, a perfect attack vector, $\mathbf{a}$, should follow [6]

$$\mathbf{a} = \mathbf{h}(\mathbf{x}_a) - \mathbf{h}(\mathbf{x}), \tag{1}$$

where $\mathbf{h}(\cdot)$ denotes a general AC power flow model, and $\mathbf{x}_a$ and $\mathbf{x}$ denote the targeted and original state vectors of power systems, respectively.

The compromised measurement, $\mathbf{z}_a$, can be written as [6]

$$\mathbf{z}_a = \mathbf{z} + \mathbf{a} = \mathbf{h}(\mathbf{x}) + \mathbf{a} = \mathbf{h}(\mathbf{x}_a), \tag{2}$$

where $\mathbf{z}$ denotes the original measurement vector. Figure 2 shows a geometric representation of the measurement vector $\mathbf{z}$, attack vector $\mathbf{a}$, and measurement vector under attack $\mathbf{z}_a$ in the AC power grid model between buses *i* and *j*. Notably, the AC power grid model is inherently nonlinear. For illustration purposes, the voltage amplitudes of two buses are normalized, the conductance and susceptance of the transmission line are 1.1350 and –4.7600, respectively, and a two-dimensional surface for the active power measurement vector $\mathbf{z}$ is assumed and presented. A similar two-dimensional surface for the reactive power measurement vector can also be demonstrated but omitted here. In view of the geometric representation, Eq. 2 indicates that the compromised measurement should lie on the surface of the AC power grid model, as shown in Fig. 2. Moreover, if a new compromised measurement is desirable and different from those in the observed data set, a tolerance mechanism can be introduced, provided that it is within a tolerable residue from the compromised measurement, which is typically related to a threshold of BDD.

Similarly, the criteria of a stealthy attack against the DC state estimation give the following relation [11]:

$$\mathbf{a} = \mathbf{Hc}, \tag{3}$$

where $\mathbf{H}$ denotes the Jacobian matrix of the DC power flow model, and $\mathbf{c}$ is an arbitrary nonzero vector. Accordingly, substitute Eq. 3 into Eq. 2 and apply the DC model expression of $\mathbf{z}$. The compromised measurement in Eq. 2 also suggests that $\mathbf{z}_a$ should lie on the surface of the DC power grid model, which is inherently linear, as shown in Fig. 3. This is not surprising because the DC power flow model is a special case of the AC one.

Based on the aforementioned discussions, considering the measurement vector set $\mathbf{z}_d$, we propose an energy big data replay attack by formulating the attack vector as the difference between an observed measurement, $\mathbf{z}_d$, and the original measurement, vector $\mathbf{z}$. Here, the observed measurement $\mathbf{z}_d$ is treated as the compromised measurement $\mathbf{z}_a$. With the proposed attack vector, the compromised measurement will be positioned definitely on the surface of the power grid model. The selection of a specific $\mathbf{z}_d$ in the whole dataset can be done based on the maximum Euclidean distance between the compromised measurement and the original measurement vectors to impose a large abrupt change in the power system states. Or, on the contrary, the minimum distance rule can be adopted here to introduce a small change in the power system states and to reduce the possibility of being detected by an advanced detection mechanism.

Performance Evaluation

Monte Carlo simulations were conducted to assess the performance of the proposed big data attack (Big), random attack (Random), conventional DC attack (DC Conventional), and no attack (Ideal), which is used as a benchmark. The introduction of random, DC conventional, and Ideal attacks was already done in [11], and thus we do not repeat them here. The simulation results are evaluated in the IEEE 14-Bus electrical grid model. The measurements consist of active and reactive power flows at all branches. The number of simulations and the number of measurement vectors for each simulation run are 500 and 200, respectively. The impacts of measurement noise with zero-mean Gaussian distribution were evaluated.

Figures 4 and 5 plot the probability of missed detection, P_{miss}, vs. the decision threshold γ of BDD over the IEEE 14-Bus grid model against the DC and AC state estimations, respectively. The maximum distance rule for selecting the compromised measurement is adopted. As shown in Fig. 4, the random attack without taking the Jacobian matrix into consideration has the lowest P_{miss}; hence, it is not stealthy. The performance of the DC conventional attacks and that of the proposed big attacks

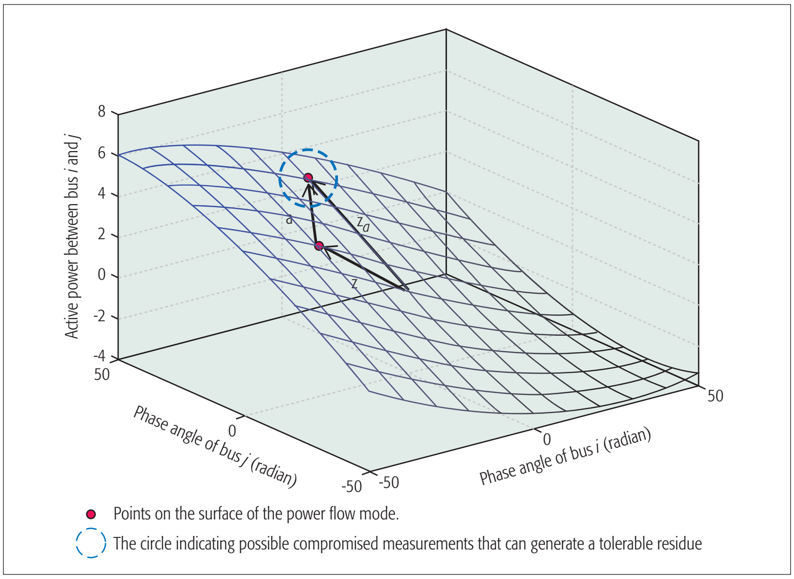

Figure 2. Geometric representation of the measurement vector $\mathbf{z}$, attack vector $\mathbf{a}$, and measurement vector under attack $\mathbf{z}_a$ in the AC power grid model.

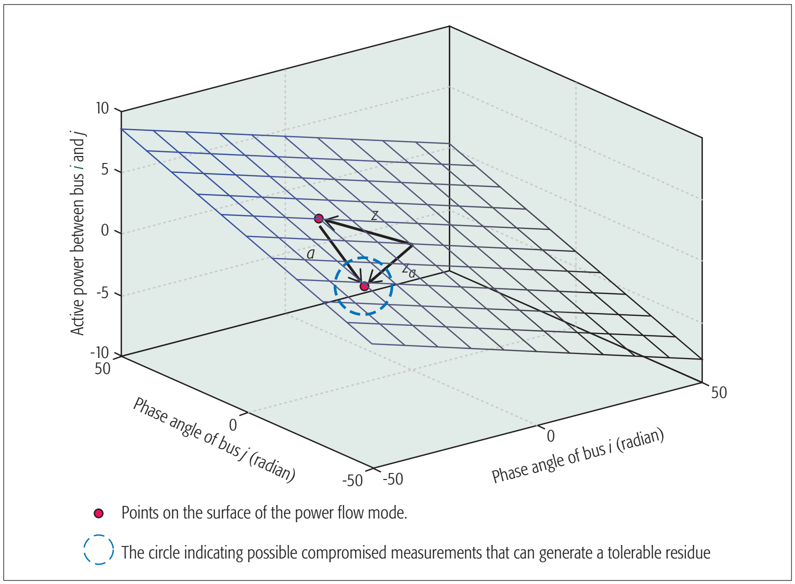

Figure 3. Geometric representation of the measurement vector $\mathbf{z}$, attack vector $\mathbf{a}$, and measurement vector under attack $\mathbf{z}_a$ in the DC power grid model.

coincide with that of the Ideal condition; therefore, they are indeed stealthy and perfect attacks. It is not surprising because the residue is ensured to be unaltered by the proposed scheme. To simplify the analysis, the proposed attack **a** satisfies Eq. 1. Then Eq. 2 guarantees that the compromised measurement lies on the surface of the power flow model so that the residue is unchanged. The proof follows. As shown in Fig. 5, the DC conventional and random attacks using a wrong power flow model have the lowest P_{miss}. The performance of the proposed big data attack is almost the same as that of the Ideal condition; therefore, it is still considered to be stealthy under the AC state estimation.

Therefore, the proposed algorithm is proved to be very flexible, requiring only measurement data, and applicable under DC or AC state estimations.

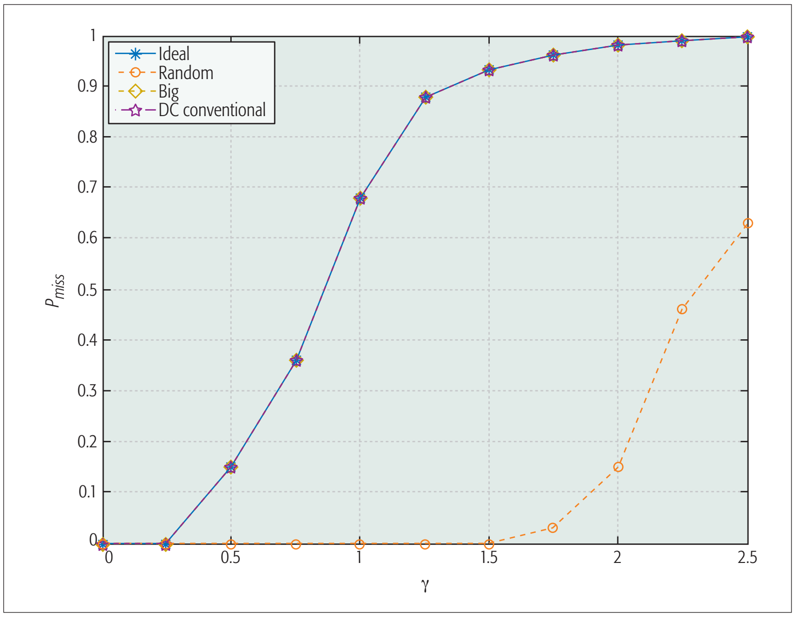

Figure 4. Probability of missed detection, P_{miss}, vs. decision threshold γ of BDD over the IEEE 14-Bus grid model against DC state estimation.

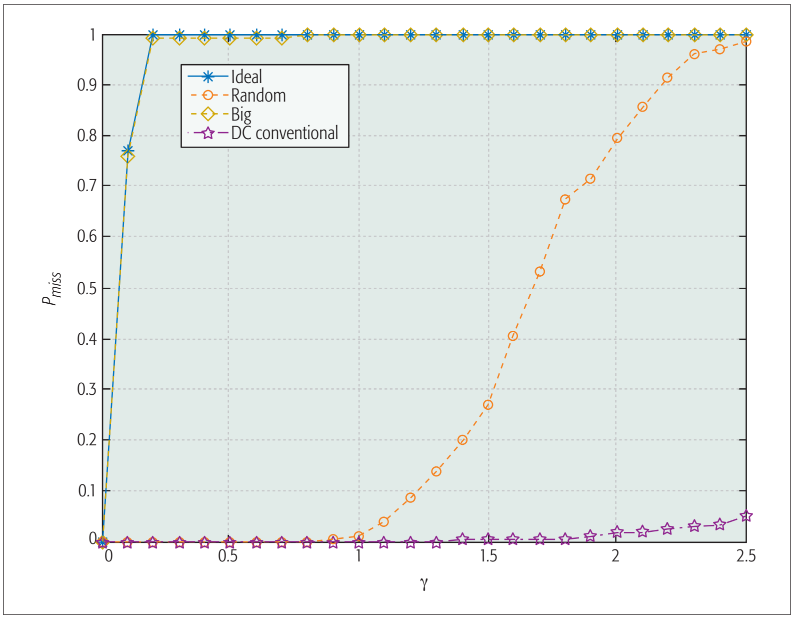

Figure 5. Probability of missed detection, P_{miss}, vs. decision threshold γ of BDD over the IEEE 14-Bus grid model against AC state estimation.

The future challenges of the big data attacks are outlined as follows:

- Sophisticated selection rules for the compromised measurement that can significantly confuse a power system need to be investigated further. For example, a random selection approach can be one of them.
- New powerful metrics might exist in addition to the proposed one based on the Euclidean distance.
- The proposed attack opens a new research direction from the attackers' viewpoints. New defense mechanisms are required to deal with it efficiently.

Future Research Directions in IoT-Based Smart Grid

In addition to removal of business and political barriers, governmental efforts should pursue several goals concurrently, including regulations, universal standards, failure recovery mechanisms, and so on. Several challenges can be identified as follows [9].

Communication technologies: The success of IoT-based SG depends strongly on uninterrupted communications of its connected devices. A huge amount of energy big data related to monitoring and control will be transmitted using wireless and wireline communication infrastructures, such as Wi-Fi, Bluetooth, ZigBee, cellular, WiMAX, PLC, and fiber optics. Cognitive radio (CR) networking was recognized as a prominent technology to address communication requirements of IoT-based SGs [15].

Heterogeneity: Due to the discrepancy on the resources that the devices and communication technologies use in the SG, achieving end-to-end security and connectivity is a challenging task, requiring a complex cyber-physical coupling model. Co-design of energy big data analytics and security mechanism can minimize security risk. Moreover, regional differences in electric grid topologies require diverse technologies to resolve interconnection issues.

Scalability: Independent random events can aggregate to yield large-scale catastrophic failures in the grid and trigger cascading events. Particularly, scalable key management, authentication [10], and privacy solutions are required for the large-scale deployment of SG.

Constrained resources: SG devices are resource constrained. Security solutions, such as authentication, for a large number of nodes in SG have become a challenging issue [10].

Interoperability: Legacy systems were deployed based on proprietary hardware and software. The implementation of IoT-based SG should also be coordinated with governmental efforts under national energy policies, national security, economic growth, and energy independence. As a result, they pose unique challenges to create a suite of standards for the interoperability and backward compatibility in SG.

Trust management: Trust must be established across different SG domains and/or levels, including different utilities and electricity generation chains. Building the trust between different domains is a challenge, especially in a large-scale IoT network with a large number of low-end SG devices.

Latency constraint: Essential information should be stored, processed, and extracted in a timely manner. Therefore, modern big data analytics is an important method for the intelligence and decision making in the SG.

Service on demand: Cloud computing architecture provides shared processing resources and data for energy big data analytics, as shown in Fig. 6. A new platform is needed to deal with big data and security concerns in a prompt fashion. The cloud control center can provide different levels of service, such as infrastructure as a service, platform as a service, and software as a service for traditional utility and local control centers, and even customers. The third party services may include a weather forecast and authentication center with the key generator. Based on historical data and information from the third party service, big data analytics are applied at the cloud control center for energy forecast, security analysis, and so on. The local control centers are distributed for better scalability and reliability. If a local control center is unavailable due to maintenance, attacks, or natural disasters, other local control centers can take over the control.

Network-based threats detection: We have shown a new big data attack in this work. Additional attacks can also appear. Besides, we need to rely on automated detection schemes to respond to network-based threats. The vulnerabilities of grids should be detected early enough. Quick and auto-recovery mechanisms need further research efforts. Furthermore, the mindset of utilities is still focused on reliability under natural disasters instead of security threats from adversaries. Also, very few studies have been carried out on key management schemes for AMI and wide area measurement network entities. Besides, a distributed security solution is needed to protect essential/privacy information.

Self-healing protection systems: Relay applications for the protection of power systems have been used for over 100 years. Advanced algorithms, such as islanding protection employing IEDs and PMUs with sensors, are important for SG.

Conclusions

The SG can benefit from the IoT technology, where smart devices are integrated with pervasive connectivity. Security is the main concern for the IoT-based SG, which works in a complex cyber-physical model. In this article, we have reviewed the main security issues and challenges for the IoT-based SGs, and discussed the problems with energy big data analytics. While enjoying the benefits of SG, we have to prevent individual privacy intrusion and keep the data from being abused. In particular, we have demonstrated a big data attack that can be launched by knowing only limited information. The work presented in this article can raise awareness of the security concerns in the IoT-based SG.

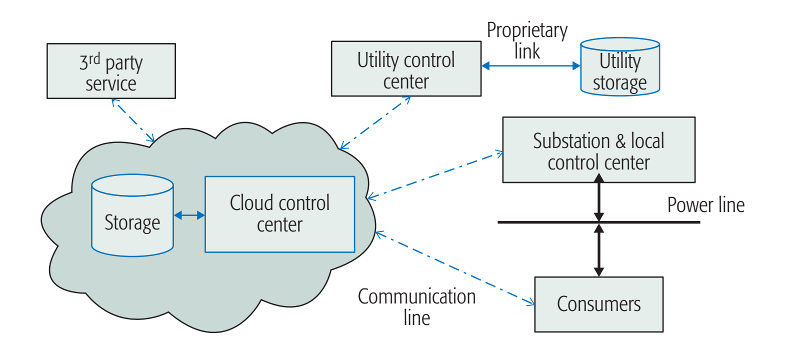

Figure 6. A cloud computing platform for smart grid applications with an emphasis on the distribution level.

References

[1] Y. Yan *et al.*, "A Survey on Smart Grid Communication Infrastructures: Motivations, Requirements and Challenges," *IEEE Commun. Surveys & Tutorials*, vol. 15, no. 1, 1st qtr. 2013, pp. 5–20.

[2] F. Ghavimi and H. H. Chen, "M2M Communications in 3GPP LTE/LTE-A Networks: Architectures, Service Requirements, Challenges, and Applications," *IEEE Commun. Surveys & Tutorials*, vol. 17, no. 2, 2nd qtr. 2015, pp. 525–49.

[3] C. Lai *et al.*, "Toward secure Large-Scale Machine-to-Machine Communications in 3GPP Networks: Challenges and Solutions," *IEEE Commun. Mag.*, vol. 53, no. 12, Dec. 2015, pp. 12–19.

[4] Y. Yan *et al.*, "A Survey on Cyber Security for Smart Grid Communications," *IEEE Commun. Surveys & Tutorials*, vol. 14, no. 4, 4th qtr. 2012, pp. 998–1010.

[5] N. Li *et al.*, "Researches on Data Processing and Data Preventing Technologies in the Environment of Big Data in Power System," *Proc. DRPT '15*, Nov. 2015, pp. 2491–94.

[6] Md. A. Rahman and H. Mohsenian-Rad, "False Data Injection Attacks Against Nonlinear State Estimation in Smart Power Grids," *Proc. IEEE PES General Meeting '13*, July 2013, pp. 1–5.

[7] X. Li *et al.*, "Securing Smart Grid: Cyber Attacks, Countermeasures, and Challenges," *IEEE Commun. Mag.*, vol. 50, no. 8, Aug. 2012, pp. 38–45.

[8] R. Ma *et al.*, "Smart Grid Communication: Its Challenges and Opportunities," *IEEE Trans. Smart Grid*, vol. 4, no. 1, Mar. 2013, pp. 36-46.

[9] C. Bekara, "Security Issues and Challenges for the IoT-Based Smart Grid," *Elsevier Procedia Computer Science*, vol. 34, 2014, pp. 532–37.

[10] W. L. Chin, Y. H. Lin, and H. H. Chen, "A Framework of Machine-to-Machine Authentication in Smart Grid: A Two-Layer Approach," *IEEE Commun. Mag.*, vol. 54, no. 12, Dec. 2016, pp. 102–07.

[11] Z. H. Yu and W. L. Chin, "Blind False Data Injection Attack Using PCA Approximation Method in Smart Grid," *IEEE Trans. Smart Grid*, vol. 6, no. 3, May 2015, pp. 1219–26.

[12] K. Wang *et al.*, "Strategic Honeypot Game Model for Distributed Denial of Service Attacks in the Smart grid," *IEEE Trans. Smart Grid*, DOI: 10.1109/TSG.2017.2670144, 2017.

[13] H. Jiang *et al.*, "Energy Big Data: A Survey," *IEEE Access*, vol. 4, 2016, pp. 3844–61.

[14] C. S. Lai and L. L. Lai, "Application of Big Data in Smart Grid," *Proc. IEEE SMC '15*, Hong Kong, China, Sept. 2015, pp. 665–70.

[15] T. N. Le, W. L. Chin, and H. H. Chen, "Standardization and Security for Smart Grid Communications Based on Cognitive Radio Technologies – A Comprehensive Survey," *IEEE Commun. Surveys & Tutorials*, vol. 19, no. 1, 2st qtr. 2017, pp. 423–45.

Biographies

WEN-LONG CHIN (wlchin@mail.ncku.edu.tw) received his M.S. degree in electrical engineering from National Taiwan University and his Ph.D. degree in electronics engineering from National Chiao Tung University in 1996 and 2008, respectively. He is now an associate professor in the Department of Engineering Science, National Cheng Kung University. Before holding this faculty position, he worked at Hsinchu Science Park, Taiwan. He serves as an Associate Editor of *IEEE Access*.

WAN LI (kghs980824@yahoo.com.tw) received her B.Sc. degree in electrical engineering from National University of Tainan, Taiwan, in 2016. Now she is a first-year graduate student in engineering science at National Cheng Kung University, Tainan City, Taiwan. Her research interests include the Internet of Things and smart grid.

HSIAO-HWA CHEN [S'89, M'91, SM'00, F'10] (hshwchen@ieee.org, hshwchen@mail.ncku.edu.tw) is currently a Distinguished Professor in the Department of Engineering Science, National Cheng Kung University. He is the founding Editor-in-Chief of Wiley's *Security and Communication Networks Journal*. He was the recipient of the 2016 IEEE Jack Neubauer Memorial Award. He served as Editor-in-Chief of *IEEE Wireless Communications* from 2012 to 2015, and as an elected Member at Large of IEEE ComSoc from 2013 to 2016. He is a Fellow of IET.