Threat Landscape of Next Generation IoT-Enabled Smart Grids

Theodoros Mavroeidakos(✉) and Vasilis Chaldeakis

Hellenic Telecommunications Organization S.A., 99 Kifissias Avenue, Athens, Greece
tmavroeid@ote.gr, vchaldeak@cosmote.gr
http://www.ote.gr

Abstract. The Smart Grids (SGs) consist of an emerging paradigm that pave the way for the power grids' modernization and seek novel techniques for improving the transmittion and distribution of power to consumers, as well as achieving end- to-end real-time governance. Thus, the prospect of SGs are to behave intelligently, through the deployment of advanced technologies, applications and standards. A subset of such technologies and applications consists of Software Defined Netowrks (SDNs), Cloud Computing (CC), Machine-to-Machine (M2M) communications, Big Data applications, Internet-of-Things (IoT), 5G and wireless standards such as IEEE 802.15.4g and IEEE 802.16.1. The SGs, the CC and the IoT paradigms' convergence lie on satisfying the clients' needs, improving efficiency and in the same time maintaining overall control. However, the coupling of diverse technologies under a unified architecture raise multiple interdependencies which pose new challenges, ranging from the reliability of the whole power system to novel cyber-security risks. This paper sheds new light in the overall definition of the threat landscape that emerges by the convergence of CC and IoT in a SG.

Keywords: Smart Grid · IoT · Cloud Computing · Threat landscape

1 Introduction

Electricity is the most valuable resource of social structure supporting the operation of health care, banking, means of transportation and the provision of public utilities such as natural gas and water. Electricity is generated on large power plants consisting of steam, hydro and combustion turbines which require energy sources such as water, oil, coal, gas and thereupon the produced energy is routed into an interconnected high voltage transmission network. Following its generation, it is transferred through a series of distribution transformers to the consumers. The power transmission network has progressively developed for over a century, from the original design of local low-voltage DC networks, to AC three-phase high voltage networks deployed over Supervisory Control and Acquisition (SCADA) System and eventually to modern massive interconnected networks with various voltage levels and complex electrical components such as

Published by Springer Nature Switzerland AG 2020
I. Maglogiannis et al. (Eds.): AIAI 2020 Workshops, IFIP AICT 585, pp. 116–127, 2020.
https://doi.org/10.1007/978-3-030-49190-1_11

substation transformers and Phasor Measurement Units (PMUs). Throughout the power grid's evolution, several industrial challenges have been dealt in view of provisioning power to the customer premises fast and uninterruptedly. In light of the SG's technological innovations and novel communication links amongst its architectural components, the security risk is increased due to the expansion of the points of interests from the attackers' perspective.

Nowadays, the complexity of power grid is multifaceted and depends on the interconnection of heterogeneous electrical and electronic components, the integration of Renewable Energy Resources (RES), the Energy Management System (EMS), the Distribution Management System (DMS), the Intelligent Electronic Devices (IEDs) and systems operations. Furthermore, in view of encountering periods of peak demand, the Transmission System Operator (TSO) balances supply and demand across the transmission network by deploying automation systems. The automation and control capabilities of transmission and distribution networks, add a new layer of complexity that burdens the power grid with new challenges concerning reliability and performance.

By exploiting the emergence of telemetry technologies, the already deployed conventional static networks controlled so far by SCADA systems, evolve into modern and dynamic smart grids. The SGs' telemetry technologies, lead to the deployment and control of energy sources such as wind, solar, geothermal, which pave the way for disburdening the strained power grid suffering from serious problems such as power outages, voltage drops and overloads, leading to greatly reduce power quality. To this end, SGs are comprised of many moving parts leading to the challenge that the exposure of a component may result to cascading failures across the power grid.

The correlation of SDNs, CC, M2M, IoT, 5G and Big Data on SGs, as well as the insufficiencies residing on previous conventional cyber-security models that are utilized on power grids compel the industry and the relevant national authorities to advise upon safeguards and best practices to encounter vulnerabilities and security risks. On the grounds that the power grid's role is very important for the social structure, the SGs' security safeguards and measures, should be treated with caution and be placed high in the priority hierarchy set by the organizational operations. To this end, security challenges, threats and requirements should be classified side by side with performance and functionality issues prior the SG's deployment.

2 Background

In recent years there has been growing interest in threat analysis and security model propositions in support of SG infrastructure. The current threat landscape of SGs is largely addressed by standards and solutions both by the academia and the industry, as described below. However, the next generation SGs are characterized by the addition of new technologies that introduce novel threats.

A systematic study on cyber security guidelines for smart grid was conducted by the National Institute of Standards and Technology (NIST) aiming to close

the gaps, scrutinizes security requirements, a framework for assessing risks, an evaluation of privacy issues, and additional information about strategies to protect the modern power grids from their attack surface. This study was later reviewed due to the emergence of novel technologies and standards [11]. Following the initial approach of NIST, the European Network and Information Security Agency (ENISA) puts forward 10 recommendations, in order to resolve concerns about cyber-security in modernized power grids consisting of a SGs [14]. These recommendations provided practical advice aimed at improving current initiatives, raising awareness, developing new countermeasures and good practices with scope to reduce barriers, which are encountered amidst the sharing of information intelligence. More work on securing SGs has been carried out by ENISA in [6,19], where the cyber security certification process of the SG is analysed and several aspects of it are scrutinized such as, architectural guidelines, recommendations and good practices.

In a cutting edge survey, Mahmud et al. [13], presented a classification of attacks on the communication networks of SGs and henceforth proposed a security framework for the SG's metering infrastructure which consists of a variety of requirements that ensure effective preservation of the Confidentiality, Integrity and Availability (CIA) triad. A more recent survey, Tong et al. [22], highlights the role of Intrusion Detection Systems on Advanced Metering Infrastructure (AMI) by analysing the attack surface, penetration techniques and consequences in AMI components. Then, security recommendations and guidelines are proposed on the basis of designing an IDS architecture suitable for AMI.

According to [8], a cyber-physical security framework that incorporates Cyber-Physical System (CPS) aspects into the security aspects is proposed for the protection of SGs. The framework captures the methodology behind attacking scenarios and their consequences on the physical domain of a CPS and accordingly effective controls and solutions can be deployed to eliminate cyber-physical attacks. With regards to [2], a breakdown of security and energy big data analytics issues is carried out with scope to determine critical attacks based on malware targeting metering data and big data from the distributed databases. Over and above this, Pour et al., argue in [18] about the vulnerabilities of SG infrastructure (i.e. the lack of standards and regulations), different kinds of attacks in the system (i.e. false data injection attack) and countermeasures (i.e. IP fast hopping mechanism) to increase the security level of the future power grid.

3 Next Generation Smart Grid Apparatus

3.1 Smart Grid Infrastructure

The SG apparatus upon which the core idea of this paper is illustrated, has developed on the basis of the Smart Grid Architecture Model (SG-AM) framework which is the reference architecture of SG use cases. The SG-AM framework consists of five interoperability layers namely, Business, Functions, Information, Communications and Components. Each one of these layers address different

aspects of SG and encompass services, operations, assets and devices in support of the power grid's functionality.

Across the SG, the main architectural element is the communication infrastructure which interconnects the interoperability layers of the SG-AM framework architecture and comprises of four networking sectors as indicated in Fig. 1 the core or backbone network, the middle-mile or backhaul network, the last-mile or access network and the Premises Area Network (PAN). The four interconnected sectors are supported by various technologies and substantially aggregate the communication infrastructure of SG.

- The core network supports the link between the numerous substations and the seats of public utilities.
- The backhaul network bridges data concentrators to the AMI with distribution automation systems and control centers related to the operation of public utilities. This sector provides broadband following a cost-efficient economy concerning its deployment and operation. In addition, the communication paths through which operational and sensorial data traverse, must be flexible and uninterrupted. To that end, this network may be owned and managed by operators and may utilize wired or wireless technologies such as Wi-Fi, WiMAX and mobile networks such as LTE and 5G.
- The last-mile network is supported by Neighborhood Area Network (NAN) and the Field Area Network (FAN), as well as the AMI. This network facilitates the collection of data from smart energy meters and their propagation to the concentrators back to the control center of AMI.
- The PAN is implemented by Home Area Networks (HANs), which are based on IEEE 802.15.4, IEEE 802.11 and PLC standards. The HAN regulate several components such as thermostats, HVAC (heating, ventilation and air conditioning), smart devices, lighting control, home automation and PHEV/EV (Plug-in Hybrid Electric Vehicle/Electric Vehicle).

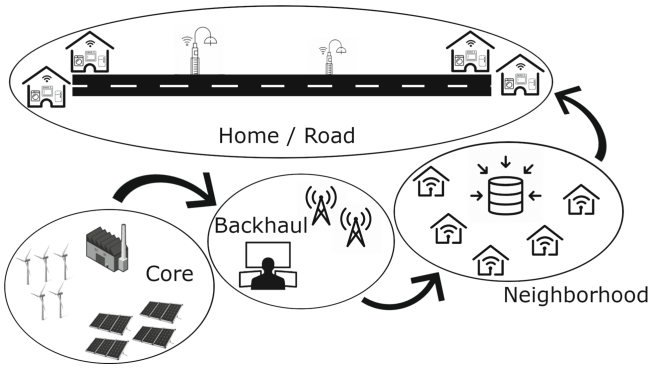

Fig. 1. Smart grid infrastructure

3.2 Cloud Computing Infrastructure

By virtue of the distributed nature of SG's communication infrastructure and the multiple data generation sources, it is required a highly scalable and elastic computing infrastructure in order to support the deployment of industrial applications. The CC infrastructure is the best computing structure in the case of SG due to the fact that provides scalable storage, appropriate processing capabilities for data analysis and cost-efficient services throughout the SG's operation. Moreover, this paradigm can handle the data generation rhythm of sensors, actuators and IoT devices in general.

The most useful applications in the context of SG, are big data analytics and remote control of components such as PMUs. The CC paradigm offers ideal conditions for the deployment of big data applications. The integration of CC applications in the operations of SGs, is comprised by development of big data Application Programming Interfaces (APIs), implementation of interoperability standards that will link the already deployed computing infrastructure with the CC applications, as well as configuration of the SG's components.

3.3 IoT Infrastructure

Cellular technology has been continually evolving with the aim of unlocking new possibilities to the industry. The advent of the Low-Power Wide-Area Network (LPWAN) technologies serve the IoT paradigm; therefore this paradigm's integration in a SG architecture is supported by LPWAN equipment and protocols.

The IoT infrastructure resides at the edge of the SGs and consists of four layers [1], namely the perception, the network, the processing and the application. The network layer is the SG's PAN, which facilitates governance over IoT devices deployed in houses. Across the SG, the intermediate link between the IoT devices and the SC controller, is the smart meter. Beyond the time-based consumption data, billing interval data and data related to the clients' usage history resulted by the smart meters operation, the IoT devices generate huge streams of data daily. Thus, many measurements and logs may be concentrated in Data Lakes residing in the backend CC environment.

4 Threat Landscape

4.1 Smart Grid Attacks

The attack vectors and threats that emerge in the Next Generation SG apparatus can be classified in the following categories as illustrated also in Fig. 2: [5,14,15,17,20,24]:

– *Physical Layer Attacks:* The interference channel is one of the most effective ways to initiate a physical-layer DoS attack, especially for wireless communications. The intruders only need to connect to communication channels where it is easy to unleash DoS attacks on the physical layer. In SGs, where wireless technologies are used, the main objective is to achieve wireless interference.

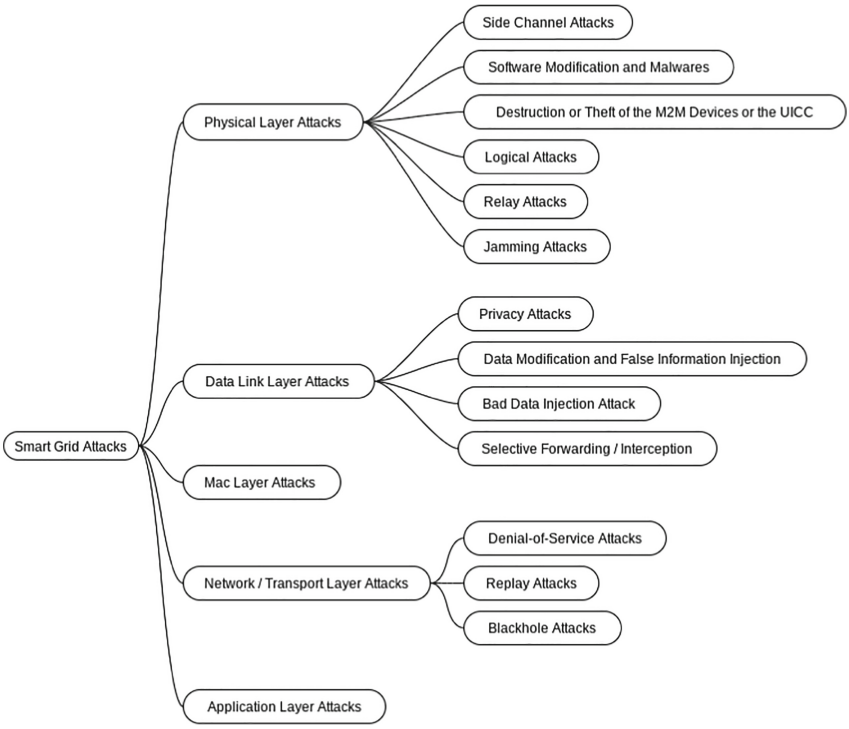

Fig. 2. Smart grid attacks

- *Side Channel Attacks:* M2Ms are located in accessible locations that attackers can easily access and perform attack on the channel side. These attacks could be based on any power consumption, timing information, error or electromagnetic leakage and allow the recovery of secret keys.
- *Software Modification and Malwares:* Software modifications can be performed by an attacker, or even a malicious user, affecting the expected operation of M2M devices. Malicious users can do so in order to reduce the amount of fees they have to pay. But the impact of these threats is even worse when it comes to e-health or automotive applications.
- *Destruction or Theft of the M2M Device or the Universal Integrated Circuit Card (UICC):* M2M or UICC devices can be easily stolen because they are placed in accessible locations. However, this is somewhat solved by welding the integrated UICC known as eUICC to the M2M.
- *Logical Attacks:* Targeting the correct operation of the system without changes to the device software when dealing with M2M communications, an intruder may forge the identity of a back-end server, an M2M device or a gateway, and so on. These attacks can lead to significant economic and human losses. For example, an attacker who manages to forge a smart gauge identity can make his owner pay for the charges himself without

his permission. In the case of electronic health, such attacks can pose a threat to human life.
  - *Relay Attacks:* An attacker can carry out an attack and disguise an entity to make others believe it is in the sender or receiver area. This attack can target the device, gateway or network domain.
  - *Jamming Attacks:* This attack is channel-based in which the legitimate signal is overwhelmed by noise [21].
- *Data Link Layer Attacks:* In this layer, the attackers target the exchange of intra-operational information.
  - *Privacy Attacks:* Because of the deployment models followed on M2M architecture concerning the utilized equipment in its device domain, malicious users can invade M2M devices and thus infer user habits, but also tamper with Personally Identifiable Information (PII).
  - *Data Modification and False Information Injection:* The data may be violated during transport, as well as in a resting state of an application's device or server. Taking into account the case of e-Health or e-Call, modyfying the measured values of information tracking can endanger the lives of people. On the other hand, in some applications, the introduction of false data can cause financial losses.
  - *Bad Data Injection Attacks:* This attack aims at making inferences of the power network topology from the correlations in line measurements using independent component analysis. The inference results can then be utilized to design stealth attacks [7].
  - *Selective Forwarding/Interception:* An attacker can track and delay or intercept the received packets. The impact of such a threat depends on the content of rejected packages. Such attacks are launched from the network infrastructure, but they could also be carried out by the M2M gateway.
- *Mac Layer Attacks:* Through the Mac Layer, reliable point-to-point communication is achieved. An attacker (e.g., a dangerous device) can deliberately modify MAC parameters and have better opportunities for network access and downgrading the performance of others who share the same communications channel. Therefore, Mac Layer can lead to a weak version of DoS attacks. In Smart Grid, spoofing is a relatively harmful threat to the MAC layer because it targets both availability and integrity. An attacking spoofing, can be disguised as another device and send false information to other devices.
- *Network/Transport Layer Attacks:* Under the TCP/IP protocol, these two layers must provide audit reliability for providing information on a multi-hop communications network. Due to the fact that SGs are comprized by multiple internal and external networks (e.g. core, backhaul, last-mile, etc.), attacking methodology can be realized remotely or localy.
  - *Denial-of-Service (DoS):* DoS attacks targeting the network and transport layers can significantly degrade the end-to-end communication between the systems and the end-users, by flooding the network with illegitimate network traffic.

  - *Replay Attacks:* The Killerbee framework can be utilized to target security vulnerabilities existing in ZigBee and IEEE 802.15.4 networks. This framework enables exploitation of in-band signaling mechanisms in digital radio protocols. To stage a replay attack, interception of network traffic should be implemented in order to delay or misdirect it; therefore the networks deployed closer to the clients are far more susceptible to this type of attack.
  - *Blackhole Attacks:* This attack threatens the smart meters; following it, several measurements gathered in the clients' premises never reach the SG core infrastructure leading to billing or logistics inconsistencies.
- *Application Layer Attacks:* These attacks focus primarily on damaging the bandwidth of communication channels. However, over and above their primary goal, they also intend to exhaust computing resources, such as CPU or Input/Output (I/O) bandwidth. Moreover, attacks against integrity and confidentiality generally occur in the application layer and enable the manipulation of information. Attacks to data integrity can be considered less violent than DoS. These attacks attempt to disclose data in order to disturb the exchange of information across the SG.
  - *Social Network Misinformation:* This attack focuses on diffusing misinformation in social networks in order to damage the SG's operations as illustrated in [16] by leveraging the Misinformation Attack Problem in Social-smart grid (MAPSS).

4.2 Cloud Attacks

The most daunting CC threats are associated to data loss, interception and tampering with the network traffic, insecure Application Programming Interfaces (APIs), malicious insiders, hijacking of virtualization technologies and threats against the end-services confidentiality, integrity and availability.

Due to the existence of multiple abstraction layers on any given CC infrastructure, the cloud consumers acquire access in-depth for the purpose of the end-services utilization. In the context of this paper, the cloud consumers are the personnel of the SG provider but also the IoT devices. To this end, the attackers leverage a huge number of attacks, aiming to target different points of the CC infrastructure. Despite the large number of attacks against CC, the impact and the risk of successful penetrations in SG assisted by CC and IoT, is greater.

Overall, following the initial stages of any attack (e.g. passive and active information gathering), the attackers are in position to coordinate their penetration methodology by exploiting vulnerabilities across the whole infrastructure. To this end, new attack vectors emerge due to the conjunction of these technologies and as a result the threats' impact on the end-service, is hazardous.

A taxonomy of threats [9,10] targeting the industrial environment of SGs where CC solutions are utilized is the following:

- *SQL Injection:* In this attack, malicious queries target the production database aiming to gain unauthorized access.

- *Malware Injection:* In this attack, malicious code is implanted in legitimate software or systems aiming to give remote Control & Command to the attacker in order to control services and extract data.
- *XML Signature Wrapping:* The SOAP protocol facilitates communication amongst different systems. The communication is secured by XML signatures where vulnerabilities can be exploited.
- *Deep Packet Inspection:* In this attack, analysis of internal and external network traffic is performed with scope to acquire sensitive network information about the data circulating the network architecture.
- *Denial of Service:* In this attack, the policies of CC services concerning scalability and elasticity are leveraged maliciously in order to misuse the CC resources and exhaust them.
- *Eavesdropping:* In this attack, network information is captured and malicious actions such as interruption of network packets propagation to reach their destination.

4.3 IoT Attacks

The security issues and concerns surrounding the IoT, occur as a consequence of threats emerging due to unaccounted vulnerabilities and 0-day exploits extended both on hardware and software, sensitive data circulating the IoT architecturte (i.e. clinical health data, spatial data) and weak communication paths facilitating interconnection of sensors and devices through a diversity of protocols and standards.

The majority of IoT attacks are based on the weaponization of Proof of Concepts (PoC) exploits with malicious payloads against known vulnerabilities. Many vulnerabilities are left unpatched due to performance, cost related issues, or because of the fact that the implementation of proper security controls on IoT devices is a costly process requiring part of the limited energy resources.

The most dangerous IoT attacks, focusing on vulnerabilities laying on the paradigm itself, are classified in the following categories:

- *Malware:* is malicious software that hijacks the sensors' functions and spreads in the IoT infrastructure in order to gather operational intelligence, which can be leveraged to exploit critical components linked to the IoT devices such as smart meters. Having integrated IoT devices in the SG, several malwares capable to damage both the clients and the SG provider. For example, the IoT reaper was a malware botnet that gathers and assesses information in order to use ideal exploits with regard to the discovered vulnerabilities. Already infected two million devices and growing at rate of 10,000 new devices per day.
- *Botnet:* is a network of infected devices spread across the world and controlled remotely from a master following the client-server architecture. For example, the Mirai was a self-replicating and self-propagating botnet worm based on telnet scanning, which launches Distributed Denial-of-Service (DDoS) attacks and targets Linux-based embedded systems such as IP cameras, home routers

and home automations simiral to those, which are met in an industrial environment such as SGs, where the same principles are applied. Since its source code publication, many blackhat groups utilize it in the midst of malware development. The Botnets can be utilized by the master not only for DDoS, but also to achieve cascading failures in the SG, leading even to physical damages (i.e. stuxnet).
- *Ransomware:* targets data storage both in the IoT and CC paradigm and blocks access to the collected data by encrypting them. A good example of ransomware is CryptoWall that generates and stores a key on the backend IoT infrastructure and then sends the key to Command-and-Control (C&C) server which is behind a proxy chain and controlled by the attacker. Moreover, the Curve-Tor-bitcoin Locker (CTB-Locker) uses AES encryption by compression step using ZLib and communicates with the C&C server through proxy websites (Tor2web).

Having overviewed these attacks, there are several threats that emerge by the adoption of Narrowband 5G and the mesh topology of IoT devices. A synopsis of threats and attacks is presented.

- *Physical Layer Attacks on 5G:* In this layer several threats exist [12], which exploit vulnerabilities of the physical channel over which the communication paths between devices are established.
  - *Selectively Jamming PSS/SSS:* Similar to the Long-Term Evolution (LTE) standard, the 5G also consists of the Primary Synchronization Signal (PSS) and the Secondary Synchronization Signal (SSS) which can be interrupted by a jammer transmitting fake signals with greater power immitating those.
  - *Sniffing and Spoofing Vulnerability of the PBCH:* The Physical Broadcast Channel (PBCH) is utilized by the System Information Block (SIB) messages, which overlay information about the power thresholds responsible for the handover process of a device from a cell to another. The information that the SIB messages carry, is transmitted unencrypted, leaving it vulnerable to malicious acivities.
- *Network Attacks* [3]*:*
  - *Traffic Analysis:* In this attack, network information is captured and analysed in order to acquire useful information about the operation of the IoT architecture.
  - *Sleep Deprivation:* This type of attack targets to the power reserves of wireless nodes by keeping them busy with useless request which are broadcasted recursively by the perpetrator.
  - *Sybil:* This attack lies on exploiting the identity verification process of Wireless Sensor Networks (WSNs) where the malicious node disguises its identity with multiple others.
  - *Resource Consumption:* In this attack, the main aim is to degrade the network's latency and capacity by broadcasting Route Request (RREQ) packets.

- *Key Reinstallation Attacks (KRACKs)*: In this series of attacks, the propagated network packets are captured and then are decrypted [23]. Most of WiFi devices are vulnerable of installing zero encryption key, this is feasible due to a fault in the WPA2 protocol. Upon this fault, the KRACKs are enabled during 4-way handshakes of IoT devices with the network Access Point (AP).
- *Man in the Middle:* In this attack, interception of data flowing from a source to a destination is implemented by the attacker in order to read them and extrack useful knowledge. In several occasions, the attacker focuses on modifying the data in-transit from the source to the destination.
- *Kr00k*: This attack leverages a bug in order to decrypt the WiFi network traffic [4]. Many IoT devices are equiped with Broadcom and Cypress wifi chips', which are affected by this bug. According to this bug, a short wifi disconnection, called disassociation, is enforced by the attackers leading the devices to reset the session key which can be all-zero.

5 Conclusion and Future Work

This work scrutinizes the threat landscape that exist in next generation SGs. The main point to focus is that there is a huge number of attack vectors against a next generation SG due to its architectural components and its distributed functionality. By summarizing the majority of threats, proper security guidelines would be possible to be set up in order to protect modern applications on top of SGs. Future reaserch should focus on analysing the majority of these attacks in depth for the purpose of formulating ideal security measures that will mitigate this landscape.

References

1. Ali, I., Sabir, S., Ullah, Z.: Internet of things security, device authentication and access control: a review. arXiv preprint arXiv:1901.07309 (2019)
2. Chin, W.L., Li, W., Chen, H.H.: Energy big data security threats in IoT-based smart grid communications. IEEE Commun. Mag. **55**(10), 70–75 (2017)
3. Deogirikar, J., Vidhate, A.: Security attacks in IoT: a survey. In: 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), pp. 32–37. IEEE (2017)
4. ESET INTERNET SECURITY: a serious vulnerability deep inside Wi-Fi encryption. https://www.eset.com/int/kr00k/. Accessed 28 Feb 2020
5. European Union Agency for Network and Information Security (ENISA): Ad-hoc & sensor networking for M2M communications - threat landscape and good practice guide. https://www.enisa.europa.eu/publications/m2m-communications-threat-landscape. Accessed 27 Feb 2020
6. European Union Agency for Network and Information Security (ENISA): Smart grid security certification in Europe challenges and recommendations. https://www.enisa.europa.eu/publications/smart-grid-security-certification-in-europe. Accessed 27 Feb 2020

7. Huang, Y., et al.: Bad data injection in smart grid: attack and defense mechanisms. IEEE Commun. Mag. **51**(1), 27–33 (2013)
8. Humayed, A., Lin, J., Li, F., Luo, B.: Cyber-physical systems security–a survey. IEEE Internet Things J. **4**(6), 1802–1831 (2017)
9. Islam, T., Manivannan, D., Zeadally, S.: A classification and characterization of security threats in cloud computing. Int. J. Next-Gener. Comput. **7**(1) (2016)
10. Khan, N., Al-Yasiri, A.: Cloud security threats and techniques to strengthen cloud computing adoption framework. In: Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications, pp. 268–285. IGI Global (2018)
11. Lee, A.: Guidelines for smart grid cyber security. NIST Interagency/Internal Report Revision 1, pp. 15–26 (2016)
12. Lichtman, M., Rao, R., Marojevic, V., Reed, J., Jover, R.P.: 5G NR jamming, spoofing, and sniffing: threat assessment and mitigation. In: 2018 IEEE International Conference on Communications Workshops (ICC Workshops), pp. 1–6. IEEE (2018)
13. Mahmud, R., Vallakati, R., Mukherjee, A., Ranganathan, P., Nejadpak, A.: A survey on smart grid metering infrastructures: threats and solutions. In: 2015 IEEE International Conference on Electro/Information Technology (EIT), pp. 386–391. IEEE (2015)
14. Mattioli, R., Moulinos, K.: Communication network interdependencies in smart grids. In: EUA FNAI Security, (ed.) EU: ENISA (2015)
15. Nazir, S., Patel, S., Patel, D.: Assessing and augmenting scada cyber security: a survey of techniques. Comput. Secur. **70**, 436–454 (2017)
16. Pan, T., et al.: Threat from being social: vulnerability analysis of social network coupled smart grid. IEEE Access **5**, 16774–16783 (2017)
17. Pidikiti, D.S., Kalluri, R., Kumar, R.S., Bindhumadhava, B.: Scada communication protocols: vulnerabilities, attacks and possible mitigations. CSI Trans. ICT **1**(2), 135–141 (2013)
18. Pour, M.M., Anzalchi, A., Sarwat, A.: A review on cyber security issues and mitigation methods in smart grid systems. In: SoutheastCon 2017, pp. 1–4. IEEE (2017)
19. Ruland, K.C., Sassmannshausen, J., Waedt, K., Zivic, N.: Smart grid security-an overview of standards and guidelines. e&i Elektrotech. Informationstechnik **134**(1), 19–25 (2017)
20. Sanjab, A., Saad, W., Guvenc, I., Sarwat, A., Biswas, S.: Smart grid security: threats, challenges, and solutions. arXiv preprint arXiv:1606.06992 (2016)
21. Tazi, K., Abdi, F., Abbou, M.F.: Review on cyber-physical security of the smart grid: attacks and defense mechanisms. In: 2015 3rd International Renewable and Sustainable Energy Conference (IRSEC), pp. 1–6. IEEE (2015)
22. Tong, W., Lu, L., Li, Z., Lin, J., Jin, X.: A survey on intrusion detection system for advanced metering infrastructure. In: 2016 Sixth International Conference on Instrumentation & Measurement, Computer, Communication and Control (IMCCC), pp. 33–37. IEEE (2016)
23. Vanhoef, M., Piessens, F.: Key reinstallation attacks: forcing nonce reuse in WPA2. In: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, pp. 1313–1328 (2017)
24. Wang, W., Lu, Z.: Cyber security in the smart grid: survey and challenges. Comput. Netw. **57**(5), 1344–1371 (2013)