Security Challenges in Smart Grids: An Overview

Hasnaat Khan
Faculty of Engineering and Informatics
University of Bradford
Bradford, UK
hkhan79@bradford.ac.uk

***Abstract*— The need for smart grids, which digitize energy distribution, monitoring, and control, becomes increasingly linked through increasing smart devices, increased wireless access, and lower cost data, as they also make possible two-way communication between the customer and the energy providers. The problems for modern power grids include the growing demand for electricity, the rapid development of renewable energy and generation of decentralized electricity, the adaptation of (Internet of Things) IoT devices, smartphones, evolving security threats toward cyber-physical systems and the main aim of preserving system stability and efficiency. The intelligent grid incorporates information technology power to deliver electricity intelligently by using two-way communication to allow green technologies to be implemented and to fulfill environmental standards with great knowledge. There are many research activities in the field of smart grid security and data privacy. This paper gives a brief survey of security challenges and weaknesses of smart grids.**

Keywords—Smart grids, Security, Privacy, SCADA.

I. INTRODUCTION

Energy efficiency is the cornerstone of today's energy situation, as conventional power production systems continually find it difficult to fulfill the global power requirements. In many other nations, intelligent networks have substituted traditional power grids. The next wave of power transmission and storage, combined with developments in the data communication technology, combines existing power grids and improves overall performance, which is a smart grid. A smart grid seeks to improve grid performance and reliability in every area, such as production, transmission, delivery and usage, and to reduce cost. Market exposure and market access-related information benefit consumers to monitor their usage proactively.

The intelligent grid has improved the way electricity is generated, transmitted and used through the incorporation of advanced sensing, interaction, and control technologies in the operation of the power grid. It provides the benefits of improved efficiency, quality, safety and pollution mitigation. This improves efficiency through the implementation of RES, good control of production, and the introduction of strategies for increasing losses along power lines [1]. Table 1 shows the main variations of the intelligent grid compared to the traditional system. Unlike the conventional network, the smart grid achieves stability without fuel availability. The intelligent grid will also allow the protection of resources including substations, overhead lines, generators and consumer facilities, as well as stable connectivity and reliable software tools that protect customer data and infrastructure [2].

The smart grid enables two-way power and data transfer interactions. The (Advanced metering infrastructure**)** AMI infrastructure, which involves communications networks, smart meters, and data management systems, facilitates two-way interaction between providers and users, is one of the key components of an integrated grid system [4], [8]. The grid will collect data from consumers using AMI software on their energy consumption, electricity efficiency and demand profiles. The intelligent meters will relay usage data automatically to the service center. Customers can also be aware of their intake of electricity and important peak price times [3]. Table one shows the differences between the traditional grid and smart grids.

Table 1*: Difference between traditional and smart grid*

Traditional grid	**Smart grid**
Mechanized One-way communication Centralized power generation	Digitized Two-way communication Distributed power generation
Small number of sensors	Large number of sensors
Less security and privacy issues	Prone to security and privacy issues
Fewer user choices	More user choices

This paper provides a new approach to challenges in smart grids. The remaining of this paper is organized as the rest of the sections will cover the Smart Grids basics, the system security issues with the approach as well as the challenges. In addition to this, countermeasures will be addressed followed by a conclusion.

II. SMART GRIDS – BASICS

In terms of reliability, connectivity, productivity, and control, the smart grid is a major improvising of the conventional network. It's the electricity network used to provide access to customers and to track, analyze, and manage the use of resources by digital communications technologies. This utilizes intelligent meters to connect with the user in 2 directions. DR provides enticing arrangements to ensure coordination among customers with regard to the adjustment of energy demand. Apply the performance and usefulness of intelligent grid systems for non-conventional energy types. The effective use of EVs is the same [5].

The use of the same asset for the old system and installing a smart grid in the case of a conventional grid raises different challenges. When conventional grids must be turned into intelligent grids, adaptive approaches must be built to achieve the optimum network for the output of the smart grid features. Graph theory theories are often used to determine the best network model and topological framework enabling an intelligent grid [6]. Intellections, computing technology and automatic control systems are the three main elements of the cognitive network [15], [18]. The foundation of connectivity for the smart grid includes standardized duration, frequency scope, data rates, and transit standards to satisfy smart grid components, communications requirements.

The transmission and storing of data must be conducted in a secure way so that cyber-attacks are stopped [23]. For this reason, cryptographic protocols and algorithms shall be used.

Intelligent grid technology for information exchange includes power line connectivity, wireless communication, telephone phones, digital private Internet networks [7]–[12]. Such innovations face their application problems. There are several issues with the engineering of sensing, measuring, control and automation. Adaptive meters are commonly used in adaptive grids. Each part and system in a smart meter network need special Identifiers, making it more difficult to connect new devices with more and more clients. Types of flaws in intelligent measurement include the planning of smart meter readings and the control of energy costs [13], [14].

Changes to the existing structure must be considered in the development of an intelligent network. The new infrastructure is in most situations expanded or enhanced. The right topology must be calculated [26], [29]. It is a real challenge to set up the communications infrastructure to ensure correct data management and protection. Another problem to be addressed is the consistency of the grid. The network must always supply energy by using renewability / dispersed battery storage, energy resources, plug-in cars, etc. The network also must ensure that all elements are interoperable because it is made possible to coexist with technology from widely varying engineering disciplines [16].

III. Security Systems and Issues

There are multiple security issues associated with smart grids. The involvement of IoT and computations changed the way of working of tradition grids. There are multiple changes for IoT based smart grids. The most frequently debated and studied risks to the smart grid were cyber vulnerabilities or cyber-attacks [17]. A large number of known weaknesses are responsible for the growing increase in the analysis of cyber threats in 230 the smart grid [19]. Cyber-attacks could lead to a full breakdown of leading power systems. These cyber-attacks are usually divided into two main types: passive and active attacks [20]. They may be for different purposes. Eavesdropping, hacking, and traffic monitoring involve reactive threats; while aggressive attacks comprise Denial of Service (DoS) and ransomware attacks [21].

A spoofing attack is one of the common and serious attacks for smart grids. There are multiple types of spoofing attacks like (internet protocol) IP spoofing, (Address Resolution Spoofing) ARP spoofing, and (global Positioning System) GPS spoofing. IP spoofing utilizes the updated DNS, which is the first step of a dynamic attack, to push across security systems [22]. Nevertheless, GPS spoofing is focused on the propagation of incorrect signals more effective than satellite spoofing to mislead offenders. ARP spoofing is used to connect the (Media Access Control) MAC address of the intruder to the IP of the victims using falsified ARP messages [24]. All the information in the impacted device is sent by this intruder. GPS spoofing due to the use of GPS receivers for measuring systems is the most common type of spoofing assault in the smart grid [25].

Replay attacks are designed to intercept information about authentication. Replay attacks intercept the pattern for use along the various intelligent meters in the smart grid and play the data to perform an undetected intrusion [33]. IoT devices integrated into intelligent grid networks lead to a greater risk of this attack. The perpetrator can insert improper information into the process which could result in an incorrect energy price or forecast [27], [28]. ARP mapped a protocol address to a MAC address. Man in the middle attack uses the ARP [30]. That attack aims to connect the MAC address of the attackers with the IP address of the server, activating any traffic that would deliver that specific IP to the attacker [31]. It makes it possible for an intruder to monitor contact in the (Supervisory Control And Data Acquisition) SCADA network [32].

DoS attacks usually come about by flooding device-specific node information which causes large amounts of reply and request packets to be produced and sent [34]. Several methods can trigger a system failure to produce these assaults [35]. The attacks can also be carried out via smart grid IoT phones. Further IoT system deployment has culminated in greater concern in DoS assaults. Another possible security threat to the smart grid is the proliferation of ransomware, defined as malware [36]. There are safety strategies for three specific malware types, pandemic malware, malware persistent, and contagion malware. Pandemic malware is an offensive malware that infects all computers with a topological search technique as quickly as possible [38]. However, end-user malware is the smarter type, which sacrifices stealth by using a less striking hit list. In the end, contagion malware is particularly resistant and does not facilitate network connections but rather contributes to the legal stream of interaction [39]. In the interaction network of the intelligent system, the risks of ransomware are accentuated. Hundreds of intelligent meters have the same hardware and software. It has been noted. Although that decreases the maintenance price and automates it, the proximity of device and software types leads to the propagation of malware [40].

False data assaults require the insertion of false software into meters. A linear factor of the Jacobian power system matrix can be used to manipulate measurements across the network for FDI attacks [37], [42]. The current state approximation methods do not notice this shift in the calculation. In addition, these attacks can be generated with minimal knowledge of the topology of the power system in different strategies. These attack types are therefore extensively studied in the field of intelligent grid cybersecurity [41]–[54].

IV. Security Challenges in Smart Metering Systems

The idea of smart cities is increasingly expanding in many modern societies, together with the rapid growth of the use of smart devices. Today, intelligent grids are an important part of the intelligent city because they offer tremendous functionality that enriches both the customer and energy utilities. To be revealed to malicious behaviors, such as security attacks by terrorists, there can also be a risk aside from the high-end characteristics of smart grids. Multiple vendors developed and produced advanced intelligent metering systems on the consumer side which play an important role in smart grids [55]. The best clever meters on the market provide sensors, energy usage tracking and viewing, in a customer-friendly way so that users can reduce their usage without increasing the use of heavy-energy machines [56].

Smart meters were susceptible to various attacks that can even be initiated on the consumer side by different parties.

Many meters allow customers to monitor and watch the real-time use on their home screen, in which the type of information shown varies from one device to the next. With a power grid-connected device installed on a consumer side, those users can either steal their electricity or even bypass the principal grid system using their smart meter to engage in illegal activities [57]. The biggest threat is the diversion of energy, where dishonest users seek to exploit resources in any imaginable forms without payment. The assault may be used to deprive another customer of the service or use power by having another user compensate for it [47]. In DoS, the intruder appears to restrict the connection to other users or databases. Sporting and fitness intelligence, as well as ransomware spoofing conducted by sophisticated hackers, pose more serious threats to smart meters [58].

Consumers may use commercial equipment or even create their own for smart grid interaction as if they are genuine intelligent energy meters for transmitting false data to minimize bills [59]. The conventional power grid networks, as well as new intelligent measurement devices, were used to this kind of assault. Czechowski and Kosek, for instance, divide fraud methods into four primary groups, including secret connections to the meter, physical control of terminals or the bridging of instruments, physical manipulation of the analog meter system and exploitation of electronic meter code [61]. Researchers are suggesting different methods to combat this threat [62], [63].

Likewise, in computer networking systems they would execute identity spoofing, they may target the identities of another intelligent meter belonging to a legitimate user likewise. In so doing, fake data may be sent to the power grid, contributing to a power cut or malfunction of both the intelligent grid management system and the actual smart-meters consumer [64]. Cimpanu, for instance, shows that the GSM network often utilizes smart meters, although newly built, to transmit the data easily as the introduction of soft authentication techniques. Even beginners may buy and use multiple computers that allow the detection and handling of GSM correspondence easily. Effective encryption algorithms with sophisticated authentication mechanisms should be introduced, and full transition in the LTE network should be enforced to ensure that protection is retained to restrict these attacks [66].

Attackers can attack the smart meter or the smart grid with a denial of service. The power cut would cause enormous damage in both cases. Attackers send a huge number of questions to the intelligent meter or to the intelligent grid leading them to crash. Yi et al states and demonstrates how the conventional DoS attacks might trigger the packet transmission frequency to collapse to 34 percent by flooding the smart meter. However, a new type of attack known as a puppet attack may hit a frequency of 11 percent for the packet distribution. Good communication protocols and packet filtering intrusion protection systems may restrict these attacks [34]. Some other attacks include sniffing and traffic analysis, and malware spreading.

V. COUNTERMEASURES

There are multiple ways that are currently being utilized by different organizations. We will discuss some of them briefly. Well-configured firewalls may be used as a barrier to restrict access to SCADA devices. Strict policies can also restrict the scope of an opponent's attack. USB drives and laptops cannot be used inside or outside the SCADA system by operators. The assault by Ukraine would have been avoided if workers were skilled in phishing e-mail detection or if encryption with two factors during VPN connections were used.

Users should encrypt sensitive data in order to maintain confidentiality. More broadly, recent cybersecurity research has explored methods to avoid disclosure of sensitive data. Users can use stream analyses for privacy promotion [67]. Examination of the data flow is a set of tools of security software designed to avoid unauthorized data flows through computer systems. Several tools for preventing invalid data flows [68] and quantification of information leaking when occurring were taken into consideration [69]. Authentication mechanisms can be used to check the identity and authenticity of the communications of the different devices, modules and operators. In particular, encrypted encryption may provide confidentiality of messages and prevent attacks on integrity. It facilitates safe contact between devices, the SCADA device, energy supplies and smart meters, hardware and field staff, for example [60], [65]. Cryptographic keys are the source of trust in such a process. The mere scale of the network renders it a non-trivial task to build a vital management system that allows key production, distribution, replacement and recovery. It is a challenging problem to identify computer alteration. Typical security software is inefficient and could be compromised against zero-day vulnerabilities. Remote testing is an outstanding way of detecting code quality attacks. Finally, earlier work explored ways of ensuring information accessibility. Which include prevention of door interference and jamming.

Numerous systems ensure safety and protection against the above assaults and challenges. Safety measures are grouped into the “7D template” or the 7 cybersecurity stages of literature. These include discovery, detection, denial, disruption, deception, and degradation or destruction.

VI. BLOCKCHAIN APPLICATIONS IN SMART GRID

Blockchain technology's distinct and attractive strengths generated substantial interest in exploring and applying the software on intelligent grids [71]. Blockchains applications can be divided into different parts of the intelligent grid in the intelligent grid [72]. Blockchain technology enables consigning agencies to fully understand the overall operational status of an electricity grid in real-time. This helps them to build strategies to increase profits. For Blockchain networks, distributed structures will take over the major challenges in the conventional hierarchical frameworks in the management and control centers. Blockchain could be useful on this site by the director for exchanging the electricity between the consumer and the different energy storage systems as well as the power vehicles, close to production and transmission sides.

Blockchain technology is being used in energy trading in today's society. Energy sharing platform via blockchain which is free for long-term investments and efficient. To guarantee the selling mechanism on the energy market a certificate of origin has been released [73]. The use of blockchain in the energy market trading process helps to reduce the time and effort that the entities need to be removed from the business [70]. Therefore, the energy trading system of Peer to Peer (P2P) is becoming a highly promising method in the future

[74]. Through P2P trading systems, the blocks in the chain document energy units, which authorize holders and purchasers to work with them instantly and immediately. Instead of depending on an intermediary broker, it allows users (owners and buyers) to have a free choice, choice and cost [75].

VII. Conclusion

In terms of energy performance, flexibility, load management, and customer satisfaction, the smart grid has surpassed traditional power grids. This paper addressed the features, innovations and performance of the smart grid. To increase its stability and performance, (Information and communications technology) ICT and clean energy are built into the smart grid. The intelligent network is vulnerable to security problems, including cyber-attacks. Adequate precautions of data security and privacy during transfer and processing must be provided. For that function, encryption and security of data techniques must be used. In this paper, we have also discussed from a technical and an industrial viewpoint the latest developments and use of the blockchain in the Smart grid market. In contrast, this demonstrated the different benefits of the electricity network blockchain. In the years to come, though, significant obstacles must be addressed for the order to implement the blockchain effectively within the smart grid.

References

[1] S. Adderly, T. Peterson, D. Manukian, T. Sullivan, M. Son, and R. Mickey, "Evaluating the Potential Impact of Smart Grid Funding on Reducing the Economic Impact of Large Outage Events in the United States from 2003 to 2017," Technol. Econ. Smart Grids Sustain. Energy, vol. 4, no. 1, p. 6, Dec. 2019.

[2] M. Ghorbanian, S. H. Dolatabadi, M. Masjedi, and P. Siano, "Communication in Smart Grids: A Comprehensive Review on the Existing and Future Communication and Information Infrastructures," IEEE Syst. J., vol. 13, no. 4, pp. 4001–4014, Dec. 2019.

[3] A. Sun, A. Wu, X. Zheng, and F. Ren, "Efficient and privacy-preserving certificateless data aggregation in Internet of things–enabled smart grid," Int. J. Distrib. Sens. Networks, vol. 15, no. 4, p. 155014771984206, Apr. 2019.

[4] I. Ghafir, V. Prenosil, M. Hammoudeh, F. J. Aparicio-Navarro, K. Rabie and A. Jabban, "Disguised Executable Files in Spear-Phishing Emails: Detecting the Point of Entry in Advanced Persistent Threat." International Conference on Future Networks and Distributed Systems. Amman, Jordan, 2018.

[5] G. A. Pagani and M. Aiello, "From the grid to the smart grid, topologically," Phys. A Stat. Mech. its Appl., vol. 449, pp. 160–175, May 2016.

[6] M. Babakmehr, F. Harirchi, A. Al-Durra, S. M. Muyeen, and M. G. Simoes, "Compressive System Identification for Multiple Line Outage Detection in Smart Grids," IEEE Trans. Ind. Appl., vol. 55, no. 5, pp. 4462–4473, Sep. 2019.

[7] E. Inga, M. Campaña, R. Hincapié, and O. Moscoso-Zea, "Optimal Deployment of FiWi Networks Using Heuristic Method for Integration Microgrids with Smart Metering," Sensors, vol. 18, no. 8, p. 2724, Aug. 2018.

[8] I. Ghafir, V. Prenosil, M. Hammoudeh and U. Raza, "Malicious SSL Certificate Detection: A Step Towards Advanced Persistent Threat Defence," International Conference on Future Networks and Distributed Systems. Cambridge, United Kingdom, 2017.

[9] W. Meng, R. Ma, and H.-H. Chen, "Smart grid neighborhood area networks: a survey," IEEE Netw., vol. 28, no. 1, pp. 24–32, Jan. 2014.

[10] X. Cheng, L. Feng, F. Zhou, L. Wei, P. Yu, and W. Li, "Cost- and reliability-oriented aggregation point association in long-term evolution and passive optical network hybrid access infrastructure for smart grid neighborhood area network," Opt. Eng., vol. 57, no. 02, p. 1, Feb. 2018.

[11] I. Colak, S. Sagiroglu, G. Fulli, M. Yesilbudak, and C.-F. Covrig, "A survey on the critical issues in smart grid technologies," Renew. Sustain. Energy Rev., vol. 54, pp. 396–405, Feb. 2016.

[12] H. Jiang, K. Wang, Y. Wang, M. Gao, and Y. Zhang, "Energy big data: A survey," IEEE Access, vol. 4, pp. 3844–3861, 2016.

[13] L. M. Camarinha-Matos, "Collaborative smart grids – A survey on trends," Renew. Sustain. Energy Rev., vol. 65, Nov. 2016.

[14] M. Emmanuel and R. Rayudu, "Communication technologies for smart grid applications: A survey," J. Netw. Comput. Appl., vol. 74, pp. 133–148, Oct. 2016.

[15] I. Ghafir, V. Prenosil, and M. Hammoudeh, "Botnet Command and Control Traffic Detection Challenges: A Correlation-based Solution." International Journal of Advances in Computer Networks and Its Security (IJCNS), vol. 7(2), pp. 27-31, 2017.

[16] K. R. Anjana and R. S. Shaji, "A review on the features and technologies for energy efficiency of smart grid," Int. J. Energy Res., vol. 42, no. 3, pp. 936–952, 2018.

[17] A. O. Otuoze, M. W. Mustafa, and R. M. Larik, "Smart grids security challenges: Classification by sources of threats," J. Electr. Syst. Inf. Technol., vol. 5, no. 3, pp. 468–483, 2018.

[18] I. Ghafir and V. Prenosil, "Malicious File Hash Detection and Drive-by Download Attacks," International Conference on Computer and Communication Technologies, series Advances in Intelligent Systems and Computing. Hyderabad: Springer, vol. 379, pp. 661-669, 2016.

[19] P. McDaniel and S. McLaughlin, "Security and Privacy Challenges in the Smart Grid," IEEE Secur. Priv. Mag., vol. 7, no. 3, pp. 75–77, May 2009.

[20] S. Goel and Y. Hong, "Security Challenges in Smart Grid Implementation," 2015, pp. 1–39.

[21] V. Delgado-Gomes, J. F. Martins, C. Lima, and P. N. Borza, "Smart grid security issues," in 2015 9th International Conference on Compatibility and Power Electronics (CPE), 2015, pp. 534–538.

[22] P. Jokar, N. Arianpoo, and V. C. M. Leung, "Spoofing detection in IEEE 802.15.4 networks based on received signal strength," Ad Hoc Networks, vol. 11, no. 8, pp. 2648–2660, Nov. 2013.

[23] I. Ghafir and V. Prenosil. "Proposed Approach for Targeted Attacks Detection," Advanced Computer and Communication Engineering Technology, Lecture Notes in Electrical Engineering. Phuket: Springer International Publishing, vol. 362, pp. 73-80, 9, 2016.

[24] P. Risbud, N. Gatsis, and A. Taha, "Vulnerability Analysis of Smart Grids to GPS Spoofing," in 2018 IEEE Power & Energy Society General Meeting (PESGM), 2018, pp. 1–1.

[25] P. Pradhan, K. Nagananda, P. Venkitasubramaniam, S. Kishore, and R. S. Blum, "GPS spoofing attack characterization and detection in smart grids," in 2016 IEEE Conference on Communications and Network Security (CNS), 2016, pp. 391–395.

[26] I. Ghafir, J. Svoboda, V. Prenosil, "A Survey on Botnet Command and Control Traffic Detection," International Journal of Advances in Computer Networks and Its Security (IJCNS), vol. 5(2), pp. 75-80, 2015.

[27] J. Zhao, J. Wang, and L. Yin, "Detection and Control against Replay Attacks in Smart Grid," in 2016 12th International Conference on Computational Intelligence and Security (CIS), 2016, pp. 624–627.

[28] T.-T. Tran, O.-S. Shin, and J.-H. Lee, "Detection of replay attacks in smart grid systems," in 2013 International Conference on Computing, Management and Telecommunications (ComManTel), 2013, pp. 298–302.

[29] I. Ghafir and V. Prenosil, "Advanced Persistent Threat and Spear Phishing Emails." International Conference Distance Learning, Simulation and Communication. Brno, Czech Republic, pp. 34-41, 2015.

[30] G. Jinhua and X. Kejian, "ARP spoofing detection algorithm using ICMP protocol," in 2013 International Conference on Computer Communication and Informatics, 2013, pp. 1–6.

[31] D. Sharma, O. Khan, and N. Manchanda, "Detection of ARP Spoofing: A command line execution method," in 2014 International Conference on Computing for Sustainable Global Development (INDIACom), 2014, pp. 861–864.

[32] Y. Yang et al., "Man-in-the-middle attack test-bed investigating cyber-security vulnerabilities in smart grid SCADA systems," in International Conference on Sustainable Power Generation and Supply (SUPERGEN 2012), 2012, pp. 138–138.

[33] J. Svoboda, I. Ghafir, V. Prenosil, “Network Monitoring Approaches: An Overview,” International Journal of Advances in Computer Networks and Its Security (IJCNS), vol. 5(2), pp. 88-93, 2015.

[34] P. Yi, T. Zhu, Q. Zhang, Y. Wu, and J. Li, “A denial of service attack in advanced metering infrastructure network,” in 2014 IEEE International Conference on Communications (ICC), 2014.

[35] Y. Guo, C.-W. Ten, S. Hu, and W. W. Weaver, “Modeling distributed denial of service attack in advanced metering infrastructure,” in 2015 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), 2015, pp. 1–5.

[36] C. Bekara, “Security Issues and Challenges for the IoT-based Smart Grid,” Procedia Comput. Sci., vol. 34, pp. 532–537, 2014.

[37] I. Ghafir and V. Prenosil, “DNS query failure and algorithmically generated domain-flux detection,” International Conference on Frontiers of Communications, Networks and Applications. Kuala Lumpur, Malaysia, pp. 1-5, 2014.

[38] E. M. Dovom, A. Azmoodeh, A. Dehghantanha, D. E. Newton, R. M. Parizi, and H. Karimipour, “Fuzzy pattern tree for edge malware detection and categorization in IoT,” J. Syst. Archit., vol. 97, pp. 1–7, Aug. 2019.

[39] P. Eder-Neuhauser, T. Zseby, and J. Fabini, “Malware propagation in smart grid networks: metrics, simulation and comparison of three malware types,” J. Comput. Virol. Hacking Tech., vol. 15, no. 2, pp. 109–125, Jun. 2019.

[40] P. Eder-Neuhauser, T. Zseby, and J. Fabini, “Malware propagation in smart grid monocultures,” e i Elektrotechnik und Informationstechnik, vol. 135, no. 3, pp. 264–269, Jun. 2018.

[41] J. Tian, B. Wang, and X. Li, “Data-Driven and Low-Sparsity False Data Injection Attacks in Smart Grid,” Secur. Commun. Networks, vol. 2018, pp. 1–11, Sep. 2018.

[42] I. Ghafir, J. Svoboda and V. Prenosil, “Tor-based malware and Tor connection detection,” International Conference on Frontiers of Communications, Networks and Applications. Kuala Lumpur, Malaysia, pp. 1-6, 2014.

[43] H. Karimipour and V. Dinavahi, “On false data injection attack against dynamic state estimation on smart power grids,” in 2017 IEEE International Conference on Smart Energy Grid Engineering (SEGE), 2017, pp. 388–393.

[44] Y. Li, D. Shi, and T. Chen, “False Data Injection Attacks on Networked Control Systems: A Stackelberg Game Analysis,” IEEE Trans. Automat. Contr., vol. 63, no. 10, pp. 3503–3509, Oct. 2018.

[45] B. Chai and Z. Yang, “Impacts of unreliable communication and modified regret matching based anti-jamming approach in smart microgrid,” Ad Hoc Networks, vol. 22, pp. 69–82, Nov. 2014.

[46] X. Liu and Z. Li, “False data attack models, impact analyses and defense strategies in the electricity grid,” Electr. J., vol. 30, no. 4, pp. 35–42, May 2017.

[47] I. Ghafir, M. Husak and V. Prenosil, “A Survey on Intrusion Detection and Prevention Systems,” IEEE/UREL conference, Zvule, Czech Republic, pp. 10-14, 2014.

[48] X. Liu and Z. Li, “False Data Attacks Against AC State Estimation With Incomplete Network Information,” IEEE Trans. Smart Grid, vol. 8, no. 5, pp. 2239–2248, Sep. 2017.

[49] Y. Wang, M. M. Amin, J. Fu, and H. B. Moussa, “A Novel Data Analytical Approach for False Data Injection Cyber-Physical Attack Mitigation in Smart Grids,” IEEE Access, vol. 5, 2017.

[50] H. Zhong, D. Du, C. Li, and X. Li, “A Novel Sparse False Data Injection Attack Method in Smart Grids with Incomplete Power Network Information,” Complexity, vol. 2018, pp. 1–16, Nov. 2018.

[51] B. Wang, P. Zhu, Y. Chen, P. Xun, and Z. Zhang, “False Data Injection Attack Based on Hyperplane Migration of Support Vector Machine in Transmission Network of the Smart Grid,” Symmetry (Basel)., vol. 10, no. 5, p. 165, May 2018.

[52] L. Lei, W. Yang, C. Yang, and H. B. Shi, “False data injection attack on consensus-based distributed estimation,” Int. J. Robust Nonlinear Control, 2016.

[53] L. Che, X. Liu, Z. Li, and Y. Wen, “False Data Injection Attacks Induced Sequential Outages in Power Systems,” IEEE Trans. Power Syst., vol. 34, no. 2, pp. 1513–1523, Mar. 2019.

[54] J.-W. Kang, I.-Y. Joo, and D.-H. Choi, “False Data Injection Attacks on Contingency Analysis: Attack Strategies and Impact Assessment,” IEEE Access, vol. 6, pp. 8841–8851, 2018.

[55] A. Monzon, “Smart cities concept and challenges: Bases for the assessment of smart city projects,” in International Conference on Smart Cities and Green ICT Systems (SMARTGREENS), 2015.

[56] D. B. Rawat and C. Bajracharya, “Cyber security for smart grid systems: Status, challenges and perspectives,” in SoutheastCon 2015, 2015, pp. 1–6.

[57] K. Shuaib, Z. Trabelsi, M. Abed-Hafez, A. Gaouda, and M. Alahmad, “Resiliency of Smart Power Meters to Common Security Attacks,” Procedia Comput. Sci., vol. 52, pp. 145–152, 2015.

[58] J. Wurm, K. Hoang, O. Arias, A.-R. Sadeghi, and Y. Jin, “Security analysis on consumer and industrial IoT devices,” in 2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC), 2016.

[59] S. S. S. R. Depuru, L. Wang, and V. Devabhaktuni, “Electricity theft: Overview, issues, prevention and a smart meter based approach to control theft,” Energy Policy, vol. 39, no. 2, pp. 1007–1015, Feb. 2011.

[60] I. Ghafir, V. Prenosil, M. Hammoudeh, T. Baker, S. Jabbar, S. Khalid and S. Jaf, “BotDet: A System for Real Time Botnet Command and Control Traffic Detection,” IEEE Access (IF=4.098), vol. 6, pp. 1-12, 2018.

[61] R. Czechowski and A. M. Kosek, “The most frequent energy theft techniques and hazards in present power energy consumption,” in 2016 Joint Workshop on Cyber- Physical Security and Resilience in Smart Grids (CPSR-SG), 2016, pp. 1–7.

[62] W. Luan, G. Wang, Y. Yu, J. Lin, W. Zhang, and Q. Liu, “Energy theft detection via integrated distribution state estimation based on AMI and SCADA measurements,” in 2015 5th International Conference on Electric Utility Deregulation and Restructuring and Power Technologies (DRPT), 2015, pp. 751–756.

[63] R. Jiang, R. Lu, Y. Wang, J. Luo, C. Shen, and X. Shen, “Energy-theft detection issues for advanced metering infrastructure in smart grid,” Tsinghua Sci. Technol., vol. 19, no. 2, pp. 105–120, Apr. 2014.

[64] C. Cimpanu, “Smart meters are laughably insecure, are a real danger to smart homes.” Retrieved from Bleeping Computer: www. bleepingcomputer. com/news/security~…, 2017.

[65] I. Ghafir and V. Prenosil, “Blacklist-based Malicious IP Traffic Detection,” Global Conference on Communication Technologies (GCCT). Thuckalay, India: pp. 229-233, 2015.

[66] B. Schneier, Data and Goliath: The hidden battles to collect your data and control your world. WW Norton \& Company, 2015.

[67] I. Dorothy E. Denning Purdue Univ., West Lafayette, “A lattice model of secure information flow,” Communications of the ACM, New York, NY, USA, pp. 236–243, May-1976.

[68] S. Weerakkody, X. Liu, S. H. Son, and B. Sinopoli, “A Graph-Theoretic Characterization of Perfect Attackability for Secure Design of Distributed Control Systems,” IEEE Trans. Control Netw. Syst., vol. 4, no. 1, pp. 60–70, Mar. 2017.

[69] “Covert Misappropriation of Networked Control Systems: Presenting a Feedback Structure,” IEEE Control Syst., vol. 35, no. 1, Feb. 2015.

[70] U. Raza, J. Lomax, I. Ghafir, R. Kharel and B. Whiteside, “An IoT and Business Processes Based Approach for the Monitoring and Control of High Value-Added Manufacturing Processes,” International Conference on Future Networks and Distributed Systems. Cambridge, United Kingdom, 2017.

[71] Z. DONG, F. LUO, and G. LIANG, “Blockchain: a secure, decentralized, trusted cyber infrastructure solution for future energy systems,” J. Mod. Power Syst. Clean Energy, vol. 6, no. 5, pp. 958–967, Sep. 2018.

[72] F. Gao, Advances in polymer nanocomposites: types and applications. Cambridge: Woodhead, 2012.

[73] I. S. Bayram, M. Z. Shakir, M. Abdallah, and K. Qaraqe, “A survey on energy trading in smart grid,” in 2014 IEEE Global Conference on Signal and Information Processing (GlobalSIP), 2014, pp. 258–262.

[74] K. N. Khaqqi, J. J. Sikorski, K. Hadinoto, and M. Kraft, “Incorporating seller/buyer reputation-based system in blockchain-enabled emission trading application,” Appl. Energy, vol. 209, pp. 8–19, Jan. 2018.

[75] F. Imbault, M. Swiatek, R. de Beaufort, and R. Plana, “The green blockchain: Managing decentralized energy production and consumption,” in 2017 IEEE International Conference on Environment and Electrical Engineering and 2017 IEEE Industrial and Commercial Power Systems Europe (EEEIC / I&CPS Europe), 2017, pp. 1–5.