SAKARYA ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ
DERGİSİ

Sakarya University Journal of Science
SAUJS

ISSN 1301-4048 | e-ISSN 2147-835X | Period Bimonthly | Founded: 1997 | Publisher Sakarya University |
http://www.saujs.sakarya.edu.tr/

Title: Investigation of Cyber-Attack Methods and Measures in Smart Grids

Authors: İsa AVCI

Recieved: 2021-06-22 12:29:25

Accepted: 2021-07-13 15:35:21

Article Type: Research Article

Volume: 25
Issue: 4
Month: August
Year: 2021
Pages: 1061-1074

How to cite
İsa AVCI; (2021), Investigation of Cyber-Attack Methods and Measures in Smart Grids. Sakarya University Journal of Science, 25(4), 1061-1074, DOI: 10.16984/saufenbilder.955914
Access link
http://www.saujs.sakarya.edu.tr/en/pub/issue/64755/955914

Sakarya University Journal of Science 25(4), 1061-1074, 2021

Investigation of Cyber-Attack Methods and Measures in Smart Grids

İsa AVCI*[1]

Abstract

Smart grids have been developing rapidly with the development of technologies in recent years. In the field of critical infrastructures such as natural gas, electricity, water, and energy systems, which are among the smart grids, its use has been increasing in Turkey and all over the world in recent years. With the increase in the use of smart grids, security problems have also gained importance. Cybersecurity attacks against these networks are increasing every year. In this research study, smart cities, smart networks, and the most common cybersecurity attack methods against these systems were investigated. The studies on security in smart grids in the last 10 years have been examined and presented in a table. As a result of these researches, cyber-attacks that are experienced and likely to occur in smart networks were determined. The 20 most used cyber-attack methods were analyzed. In addition, the measures that can be taken against cyber-attacks are analyzed in detail. In addition, in this article, studies on security problems in smart grids are examined and evaluated.

Keywords: Smart grid, smart grid security, cyber-security, security measures

1. INTRODUCTION

Emerging information and communication technologies, in addition to the increasing population in big cities, due to the increase in construction investments and megacities in energy demand, comes to the fore the need for intelligent networks. Optimum operation of the natural gas grid has been a major challenge, particularly in the energy sector, but the fact that this goal can be achieved with the smart grid concept underlines the need to invest in the smart grid concept.

Smart grids have become widespread in the last years with the developing technology, and with the developing technology, the risks and security vulnerabilities that may occur come to the fore. Smart grids especially cover electricity, water, and natural gas networks and their usage areas [1].

It is a fact that cyber-attacks already offer an opportunity in terms of anonymity and deniability. In addition, it is difficult to determine who and who are financed by these attacks and which countries are behind these attacks. Therefore, it is very difficult to determine the risks and threats in cyberspace and to take precautions against them. In such an environment, it is no longer mentioned about ensuring absolute cybersecurity but instead aims to make cybersecurity risks manageable and acceptable. It is recognized that being in an open and connected environment such as the Internet carries some risks associated with increased accessibility. It is

* Corresponding author: drisaavci@gmail.com
[1] Karabuk University, Faculty of Engineering, Karabuk, Turkey.
ORCID: https://orcid.org/0000-0001-7032-8018

imperative to be prepared for cyber incidents by managing these risks with a holistic approach involving all stakeholders and to ensure their continuity by eliminating these incidents with the least damage.

This study aims to assist studies that will conduct research, development, and design, especially on smart grids. First, the definitions of the smart grid and city concepts are made. Then, the most common cyber-attacks in smart networks are given. In addition, academic studies on security and cybersecurity in smart networks are examined and given as a table. Here, the main purpose is to present what studies are carried out on security issues in smart networks and which studies are required.

2. SMART CITY

Smart cities are based on the idea of restructuring the situations of cities in a way that provides maximum efficiency with a focus on people and nature. In addition, smart cities have a human-oriented, strategic, development, change, environment that creates and supports a management approach. Due to these reasons, these cities are city structures with improved service areas and living standards. These structures are based on creating new living spaces that are comfortable, healthy, people-oriented, self-sufficient, where resources are consumed efficiently and intelligently, respectful to nature, environmental problems are minimized by using innovative and sustainable methods.

Smart cities encompass energy infrastructure, traffic management, waste management, health, transportation, water supply, and other services. Thus, a smart city has a mutually beneficial interaction between service providers and citizens. Information and Communication Technologies (ICT) are used to increase the quality, efficiency, and consistency of urban services in smart cities. It also aims to reduce the costs of the smart city and reduce resource consumption and improve communication between citizens and the state. Research on smart cities started in the 2000s and there are many definitions of smart cities. For example, smart cities are defined as the combination of reliable infrastructure, data quality, and corporate infrastructure [2]. The main purpose of the development and dissemination of smart cities;

- Suitability of urban vehicles,
- The elegance of the city administration,
- Habitability of the living space,
- The intelligence of infrastructures,
- Long-term network security effectiveness.

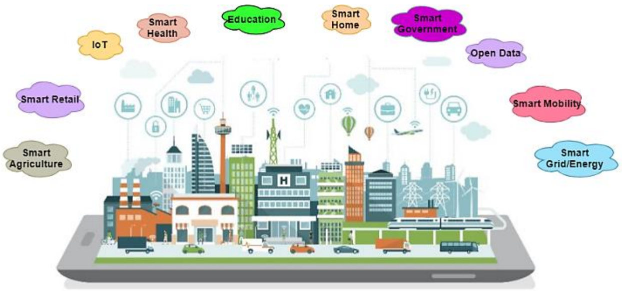

Figure 1 Smart cities overview [3].

The International Telecommunication Union (ITU) analyzed nearly 100 applications and used them to develop the following innovations. Smart, resilient metropolitan areas are modern cities that use ICT and other regulations to make urban operations, utilities, and competitiveness more vibrant and efficient [4].

3. SMART GRID

Infrastructure services are very important as an integral part of urban life. As the urban population continues to increase, control over these facilities becomes critical. Increasing population, Information Technology (IT) makes it impossible to use to manage applications and infrastructure.

The International Electrotechnical Commission (IEC) 61850 standard, which is the smart grid field communication protocol, is the standard protocol for all protection, calculation, testing, and monitoring functions. The fact that the products manufactured by many manufacturers are produced following this protocol protects in terms of security. Otherwise, many different manufacturers cannot use asynchronous or parallel interfaces and protocols. In the technical field, equipment standardization and interoperability have long been practiced together [5].

Siemens reports on the development of the smart grid and the new energy era, where its goals are diverse, chaotic, and competitive. The smart grid will provide energy stability, flexibility, and efficiency, not overloads, reductions, and blackouts. Mechanization will increase significantly and substations will help reduce preparation and operating expenses and labor intensity. Ongoing comprehensive monitoring will improve the way equipment, plant, and network work [6]. In addition, ICT forms the vital link between energy generation, transmission, distribution, and consumption.

The key element that effectively validates the smart grid application is the performance and capacity to execute integrated, scalable, and interoperable responses linked to engineering science. This will track the energy consumption of the smarter in the world, using the mobile devices of the customers, using the internet or private home monitors, and at the same time, these services will be implemented through meter data management systems. The meter also detects power surges and interruptions, and services to be used as a sensor network can also be used to connect or disconnect from a remote connection [7].

Network security, the biggest challenge in smart grid deployment, is maintaining a consistent appearance across all applications. Independent interfaces must be protected by a comprehensive border service that provides multiple layers of protection to prevent attacks. In addition, validating running applications and network architecture with a power management tool called CISCO EnergyWise can improve energy efficiency and significantly reduce costs [8].

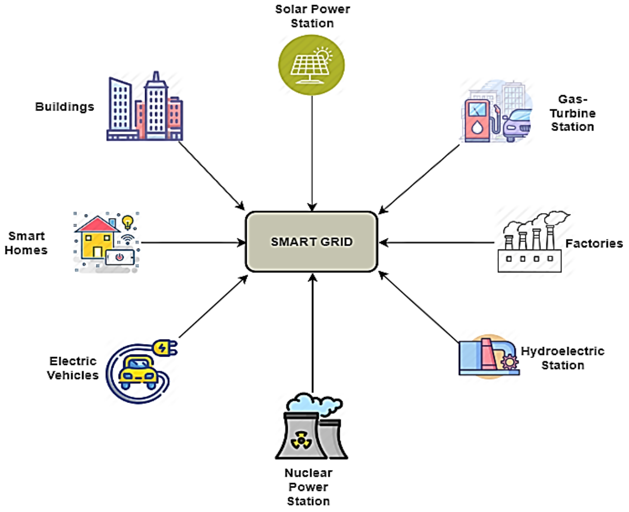

Figure 2 Smart grids overview [9].

A smart grid system should have the following features;

- Digitalization,
- Intelligence,
- Durability,
- Personalization,
- Flexibility.

Digitization means having a digital platform that makes the system fast and reliable. Intelligence means using smart technology. Durability means that the system should not be affected by any attack, Personalization means that the system should be customer-specific. Finally, flexibility means that the smart grid must be compatible, expandable, and adaptable [10].

Figure 3 below shows the ranking of the sectors most affected by cyberattacks in the world as of September 2017. According to the survey, 26% of respondents in the energy sector said that their companies have been exposed to cyber attacks in the last 12 months [11].

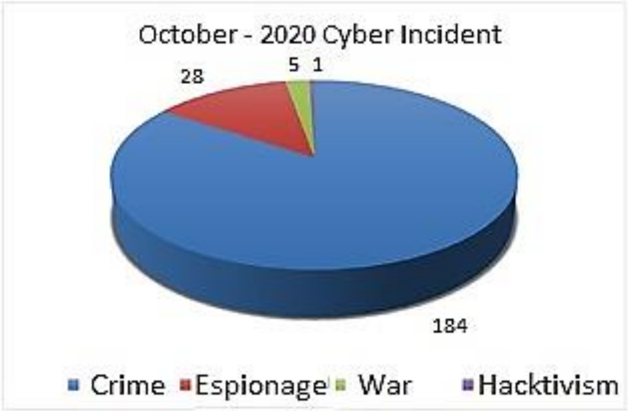

Figure 3 Cyber events that took place in October-2020 [11]

4. MOST FREQUENTLY USED CYBER ATTACK METHODS

Cybersecurity contains much more comprehensive and vital components than viruses infecting personal computers, antivirus programs that need to be updated, blocking of advertisements to e-mails, or the capture of personal information [12]. These and similar situations are of course important, but when it comes to cybersecurity, smart cities and networks should be one of the first things to consider. Because when evaluated in terms of national security; In case of service loss or disruption of services that may occur in smart networks, it may cause large-scale economic damage, loss of life, or national security weaknesses [13]. Therefore, these critical systems are the most important assets to be protected within the scope of cybersecurity. This study has tried to draw attention to this issue.

The most common cyber-attack methods are listed below [14-81];

- Distributed Denial of Service (DDoS)
- Logic Bomb
- Slave Computers (Botnet, Zombie)
- Zero-Day Exploits
- Advanced Persistent Threats (APT)
- Baiting - Phishing Attacks
- Rear Door (Back Door - Trap Door)
- Rootkit
- Spyware (Spyware - Adware)
- Attack Kits
- Ransomware
- Social Engineering
- Sending Unwanted Bulk Messages (Email) (Spam - Bulk - Junk Mail)
- Listening of Network Traffic (Sniffing - Monitoring)
- Use of Malware (Virus - Worm - Trojan horse etc.)
- Cryptographic Attacks
- IP Spoofing - Hiding (IP Spoofing)
- Digital Manipulation
- Open Microphone Listening
- Session Hijacking
- Listening of Network Traffic (Sniffing - Monitoring)
- Use of Malware (Virus - Worm - Trojan horse etc.)
- Cryptographic Attacks
- IP Spoofing - Hiding (IP Spoofing)
- Digital Manipulation
- Open Microphone Listening
- Session Hijacking
- Wire Tapping
- Internet Service Attacks
- Programs that Record Keyboard Operations (Keyloggers)
- SQL Injection

When all studies were examined, these attack types were determined. Especially the most common cybersecurity attacks have been tried to be given in this study.

5. INVESTIGATION OF SECURITY OF SMART GRIDS

Studies on cybersecurity in smart networks are given in chronological order. In recent years, intensive academic studies have been carried out on smart grids in the world and our country.

Dönmez explains the subject of integration, which is indispensable for the efficient operation of smart grids, discusses with practical examples given from structural and technical aspects [5]. Iyer et al. mentioned cyber threats and risks in smart grids in his cybersecurity for smart grid, cryptography, and privacy study [10]. Yan et al. summarize the requirements and potential vulnerabilities in smart grid cybersecurity

Examine the available communication and cybersecurity solutions for smart grid communication [12]. Goel et al. describe the main security threats and cybersecurity in smart grid technologies as well as information about the vulnerabilities of smart grid strategies to protect from security breaches, recommendations on methodologies, and technologies [13].

Kara and Çelikkol discuss the situation in Turkey in terms of the overall structure of the communication protocols of the SCADA system, as well as the precautions that need to be taken for the safe operation of the system in the SCADA transmission and distribution infrastructure of the electricity used [15]. Knap investigates attack vectors, management, and secure network for intelligent networks, SCADA, and other industrial control systems [16]. Burmester et al. provide a framework for modeling the security of cyber-physical systems. In this structure, the behavior of competitors, aspects of cyber-physical aspects is combined [17].

Rice et al. provide systems engineering applied to a cyber-attack scenario on cybersecurity issues and the implementation of an intelligent network system shows the various methods and concepts of the discipline [18]. Ashok et al. propose a game-theoretical formulation model of defense and attack by determining specific attack and defense scenarios of cyber-physical security in smart grids [19]. Anwar et al. provide cyber-attacks and solution methods in smart grid infrastructures are taken into consideration. Especially energy networks and SCADA systems are exemplified [20].

Liu et al. propose a model named ATSE that detects and predicts attacks by scanning and monitoring abnormal data traffic and bad data leaks in network traffic in smart grids [21]. Suleiman et al. propose for data to be safe and realistic in transmission lines and equipment in smart networks, as well as against attacks and leaks for a system security threat model (SSTM) [22]. Arabo explains cyber threats and precautions that may occur on critical infrastructure and smart devices used in smart home ecosystems are listed [23]. Knowles et al. provide the latest preparations and research for this risky and configuration. Implementation of special safety measures for industrial control systems, safety as a barrier to making this equipment [24].

Tawde et al. provide an overview of the structure of security mechanisms for communications SCADA at substation device Bump-in-Wire (BITW). It also provides a security solution that eliminates key management problems by integrating Protocol key distribution and management CDAC Sec-KeyD in IEC 62351 for the protection of the IEC 61850 protocol [25]. Drias et al. provide comprehensive cybersecurity issues for industrial control systems (ICS) are discussed. General SCADA structures and components are described [26]. Cherdyntseva et al. developed methods on cybersecurity risks in SCADA systems and precautions to be taken were investigated [27].

Wei et al. provide that the impact of smart grid data communication network-based attacks are caused examine the results of real-time and electricity. Moreover, the study and research of intelligent network security provide information on both field operations [28]. Mishra et al. present a new model for optimizing protection against burst attacks in smart networks. In addition, a rotation algorithm has been developed [29]. Young et al. offer a framework comprising of cyber insurance sector operating principles to measure risks. The framework for discussing critical infrastructure owners and operators of cybersecurity investments and optimization techniques to propose levels of insurance [30].

Şenol emphasizes that deterrence can be achieved with the cyber power gained by information and communication systems; information was given on the concepts of cyber power, deterrence, cyber attack, and cyber warfare; information technology, especially Internet's development and after the expansion in the world and some of the major events and consequences of cyber attacks experienced in Turkey revised; The content and results of the cyber attacks on Sony in 2014 were evaluated [31].

Stuart Borlase evaluations on infrastructures, technologies, and solutions used in smart networks are discussed [32]. Zhou et al. provide that cybersecurity standards, procedures, and best practices on SCADA are thoroughly reviewed. Thanks to these standards, defense theory in depth is recommended [33]. Do et al. explain that cyber-attacks and vulnerabilities made to the SCADA system were analyzed. In addition, SCADA architectures are given in detail. Measures and approaches to be taken against attacks have been analyzed [34]. Pour et al. provide that vulnerabilities of smart grid systems, possible intentional attacks, and precautions to be taken against these threats are discussed [35]. Antón et al. provide that the cyber-attacks your industry and infrastructure companies have been exposed to in the last 20 years are discussed. In addition, different attack types and their entry points are analyzed [36]. Kuzlu et al. provide that the standards used in intelligent networks and protocols are discussed in detail and explained [37].

Deng et al. explain that on the smart grid cyber-physical attacks and countermeasures (CCPA) are discussed. A vector measuring means for neutralizing the effect of physical attack vectors (PMI) can synthesize data injection attack vectors based on measurements carefully and thus recorded can prevent detecting invalid data before determining the CCP [38]. Shaileshwari et al. provide that the use of SDN network infrastructure against cyberattacks in smart networks and to provide a smart communication network is discussed [39]. Nazir et al. discuss SCADA tools and techniques for detecting security vulnerabilities in the system. A comprehensive summary of the chosen approach is provided, with an indication of feasibility [40].

Bretas et al. present a methodology for the cyber-physical security of smart grids and therefore discusses the possibility of diagnostics, identification, and verification [41]. Eder-Neuhauser et al. defense methods against common malicious software in smart networks are discussed [42]. At the same time, 19 malware types are compared. Baig et al. provide that by identifying specific threats smart cities and intelligent manner realistically with a view, looking around with a holistic view of the city [43]. Anwaar AlDairi et al. provide smart cities to discuss cybersecurity challenges and current solutions [44]. Otuoze et al. explain that cyberattacks can occur in smart networks and the classification of these attacks is discussed [45]. Maglaras et al. provide that security issues and solutions on Industrial Control Systems and IoT are covered [46].

Luo et al. provide that cyberattacks on smart city observers aim to aid detection and isolation. They propose a graph-based algorithm based on the theory of measurements [47]. Ding et al. explain that security control and attack detection approaches and mathematical models are examined. In addition, specific approaches are summarized in the study [48]. Saini et al. discuss how should a better cybersecurity level be in smart cities without too much modeling are discussed [49]. Kurt et al. propose a powerful online false data injection (FDI) and interference attack detection algorithm that provides online estimates and outcome predictions of unknown and time-varying attack parameters [50].

Pate-Cornell et al. cyber risk management and analysis models in smart grids and critical infrastructures are discussed. Especially Markov and Bayesian analysis models are shown. Measures to be taken against risks are discussed [51]. Kurt et al. explore online detection of deceptive attacks and the prevention of service attacks on an intelligent network. The system is modeled as a linear dynamic system with discrete time, and the state is estimated using the Kalman filter. Detectors for intrusion detection and recognition are proposed [52].

Tarıq et al. explain that away smart grid and service-oriented development methodologies such as global networking systems (CPS) offer [53]. Lopez et al. propose a new architecture divided into five subnets, which allows the integration of a cloud infrastructure responsible for executing predictive analytics to conform to the demand response by implementing a load balancing algorithm [54]. Farraj et al. propose an adaptive parametric feedback linearization (PFL) control scheme to achieve the temporal flexibility of smart grids. In addition, data integrity and availability are verified for intelligent network attacks [55]. Che et al. provide that a cyber cascade monitoring system (CCS) is proposed to detect malfunctions triggered by potential data attacks [56].

Şimşek et al.the TPS3 security protocol is recommended to protect data privacy in smart cities [57]. Ni et al. based on reinforcement learning to determine the most appropriate order-based attack on certain targets propose a new solution for a multi-stage game between offensive and defensive [58]. Kim et al. explore the need for smart grids and explores industry initiatives to combat and respond to smart grid security threats [59]. Mrabet et al. reviews security requirements and provide descriptions of various serious cyberattacks and recommend a cybersecurity strategy for detecting and countering these attacks [60]. Kimani et al. examine the basic security IOT-based challenges and problems that prevent the growth of the smart grid [61].

Hossain et al. explore the next generation of the smart grid electricity grid (SG) in the network with the emergence of big data and machine learning applications was conducted as a comprehensive study [62]. Islam et al. explores the vulnerability and hazards associated with the components of the smart energy system and relevant communication standards, including devices with support for the Internet of Things, and explores the measures to be taken against cyber attacks [63].

Sakhnini et al. discuss the object of the Internet to the (IoT) based on bibliometric research articles about security aspects of smart grids provide an overview [64]. Kumar et al. provide that traditional energy networks and smart metering networks in this article provide a brief overview of the targets of cyber attacks in real-world events [65]. De Dutta et al. aim to provide an overview and history of some of the existing solutions for detecting and preventing cyber threats and security issues affecting machine-to-machine communication (M2M), applications in smart grid, M2M data in the smart grid [66]. Gusrialdi et al. is highlighting the close relationship between the physical communication network system, the system offers an overview of the cyber attacks on power systems from a theoretical perspective [67].

Khan et al. provide various critical aspects of Blockchain technology such as operating mode, possible improvement proposals using Proof-of-Stake, and other special options are analyzed in different ways [68]. Mollah et al. provide a comprehensive overview of the implementation of blockchain in a smart grid. So can be solved by the blockchain determines the basic security problem of the intelligent network scenario [69]. Gündüz M. Z. et al. provide a comprehensive overview of the implementation of blockchain in a smart grid. Thus, it detects the basic security problems of smart grid scenarios that can be solved with blockchain [70]. Mathas et al. examine smart grid threat environments, identifies threats specific to that infrastructure, assess the severity of each type of attack, lists features and methods that can be used to detect attacks and should be used to mitigate them [71].

Ferrag et al. base on available smart grid fog SCADA systems to provide a comprehensive overview of cybersecurity solutions [72]. Moghadam et al. the key to overcoming the security weaknesses of the mix at the right time to facilitate coordination and proposes a secure communication protocol based on the private key [73]. Zhang et al. production, transmission, distribution, and improved monitoring of all network components, including consumers, two-way communication to ensure the protection and optimization of digital technology, advanced detection offers examples of their computing infrastructure and software capabilities [74]. Hittini et al. explore a smart grid false data injection protocol to prevent distribution systems (FDIPP) have been proposed. The protocol hierarchy and distribution system is designed to work on many assets matching a new hierarchical network architecture [75].

Amin et al. discuss Naive Bayes offers a new algorithm based on belief propagation (BP), a higher rate of detection than the current machine learning classifiers, such as support vector machines to detect both random and hidden FDIA in intelligent networks [76]. Shrestha et al.

propose a methodology called "Classification of intelligent network security» (SGSC), which focuses on the characteristics of the expanded measurement systems infrastructure (AMI), designed for complex systems, such as intelligent networks [77]. Jeyaraj et al. suggest a deep learning algorithm for multi-dimensional analysis and classification of non-periodic electricity. It should be noted that aid in the detection of power theft consumer intermittent load curve [78].

Gandi et al. explain that renewable energy source (RES) with the increasing use of inertial damping system that affects the stability of the system and the stresses that can cause failure. The protection of these systems with the introduction of renewable energy sources and managing systems has become more complex. Therefore, to solve these problems in a wind energy system with a reliable energy storage system implementing an intelligent control technique is proposed [79]. Khan et al. purpose software-based key elliptic curve cryptography (PALKA) intelligent network unified structure design. Based on a random oracle model and informal security analysis, PALKA's official security review and Avispa simulation based on a formal security analysis of PALKA were tested to return PALKA against man-in-the-middle and duplications. PALKA's lower information and communication about the user compared to other related protocols in the same environment [80]. Tufail et al. discuss attacks by using artificial intelligence (FDIA), which can be very useful by methods such as the prevention and subsequent FDIA through encryption, multifactor authentication, and configuration intrusion detection system. In addition, timely updates and patches can minimize the possibility of invasion [81].

Table 1 Cybersecurity attacks and measures in smart grids

	Cyber-Attack Methods	**Cyber Security Attack Measures**		
		1	**2**	**3**
1	DDoS	Operation-Based Defensive Architecture[15]	IDS[41]	IPS[19]
2	Man in The Middle (MITM)	Operation-Based Defensive Architecture[56]	TARP: Ticket-Based Address Resolution Protocol	TARP: Ticket-Based Address Resolution Protocol
3	APT-Malware (Worm,Trojan,Rootkit, Virus)	IPS/IDS[34]	Signature-Based Prevention[51]	Signature-Based Prevention[67]
4	Replay Attack	Operation-Based Defensive Architecture[48]	Neural Network Based IDS[76]	Single Sign-On Protocol Based on Dynamic Double Password[81]
5	Spoofing(ARP,IP,GPS)	IDS[31]	MAC-IP Database Center[67]	Using AES and RSA Encryption
6	MODBUS/TCP Protocol Attack	IPS/IDS[33]	SSL VPN[66]	Explicitly define a set of allowed MODBUS commands, register values, and binary coils[51]
7	DNP3 Protocol Attack	Encapsulated within TLS[48]	Implement DNP3 Secure[44]	Block the DNP3 based traffic from corporate into control networks through IPS[44]
8	Malicious Command and Software Injection	Signature-Based Prevention[48]	Ensemble of Deep Belief Network (DBN)[45]	PIVOT Algorithm[69]
9	Buffer Overflow	Real-Time Operation System(RTOS)	Hardware/Software Address Protection (HSAP)	Fonksiyon İşaretleyici XOR (HSAP)[65]
10	Social Engineering	Empirical Database[58]	Mean Time-To-Compromise Metric[63]	X
11	Physical Attack (Sensor, Actuator, Camera)	IPS/IDS[22]	Detection Algorithms[60]	A fuzzy-logic-based approach for modeling[59]

12	SQL Injection	Cyber Threat Intelligence (OSINT, SOCMINT, HUMINT)[44]	Create static function calls for external commands[61]	Use library calls implementation technique in programming[55]
13	Zero-Day Attack	Signature detection technique used by intrusion detection and prevention Systems[17]	Anomaly detection based intrusion detection technique[31]	Attack Database[23]
14	Unauthorized Access Activities	Using secret keys, either in a peer-to-peer manner or via a trusted third party[19]	Signature-based intrusion detection technique[35]	Machine Learning-Based IDS[33]
15	Insider-Outsider Attacks	State-based IDS rules	X	X
16	Network Traffic Anomaly	SDN[16]	Automatic Intelligent Cyber Sensor[46]	Intrusion Detection Mechanism[27]
17	Back Doors	IPS/IDS[32]	Luenberger Observers (LOs) and Unknown Input Observers (UIOs)	Machine Learning-Based IDS[28]
18	Reconnaissance Attacks	Ensemble of Deep Belief Network[37]	Machine Learning-Based IDS[17]	State-based IDS rules[44]
19	Sniffing	IPS/IDS[34]	Signature-Based Prevention[48]	X
20	Cryptographic Attacks	State based IDS rules[59]	X	X

With the research and development of security technologies in the details given in the table, smart grid research has been rapid in this area. Especially with the increasing cyber attacks in recent years, we have presented in this article by investigating how experts and institutions in the sector can deal with these attacks and what precautions they should take. As a result of the research, it has been observed that there are more attacks on SCADA, especially in smart networks. For this reason, it should be aimed to take more intensive measures for security studies specific to SCADA, PLC, RTU, HMI and to protect smart grid systems by developing new safe models. In addition to smart grids, critical infrastructures, and industrial control systems (ICS), safe models and methods, must be protected. The methods given in the examinations made in this study are intended to provide convenience to researchers.

6. CONCLUSION

The development of smart grids all over the world and in our country has accelerated in recent years. The rapid increase in technological developments in smart grids makes security problems in this area important. Increasing cybersecurity attacks in recent years draw attention to the importance of these problems in terms of economy, sustainability, and security. In this study, national and international academic studies on the security problems of smart grids were examined. Particular attention was drawn to this issue by providing information about possible and experienced cyber-attacks. When the academic studies conducted in the last 10 years are examined, it has been evaluated that the attacks against SCADA and industrial control systems have increased and that these systems should be protected with more secure hardware and software. In addition, in this study, the most common and possible cyberattack methods in smart networks were examined and 20 attack methods were analyzed. The development of smart grids brings with it security problems. In this article, the importance of these problems and the precautions that can be taken against cyber attacks are researched and given in a table. In addition, in the light of the information obtained here, cyber attacks that may occur in smart networks and the measures that can be taken against them are given by researching. By giving studies on this subject, academicians working on this subject and companies with smart grids were informed. This study aims to shed light on the researches and studies to be done on this subject.

Funding

The author (s) has no received any financial support for the research, authorship, or publication of this study.

The Declaration of Conflict of Interest/ Common Interest

No conflict of interest or common interest has been declared by the authors.

Authors' Contribution

The authors contributed equally to the study.

The Declaration of Ethics Committee Approval

This study does not require ethics committee permission or any special permission.

The Declaration of Research and Publication Ethics

The authors of the paper declare that they comply with the scientific, ethical, and quotation rules of SAUJS in all processes of the paper and that they do not make any falsification on the data collected. In addition, they declare that Sakarya University Journal of Science and its editorial board have no responsibility for any ethical violations that may be encountered and that this study has not been evaluated in any academic publication environment other than Sakarya University Journal of Science.

REFERENCES

[1] İ. Avcı, C. Özarpa, M. A. Aydın, A Survey of International Security Standards for Smart Grids, Industrial Control System and Critical Infrastructure, 12th International Exergy, Energy and Environment Symposium (IEEES-12), December 20-24, Doha, Qatar, 2020.

[2] A. Caragliu, C. Del Bo and P. Nijkamp, Smart cities in Europe (2009), In 3rd Central European Conference in Regional Science, 2009.

[3]Channelpostmea,http://www.channelpostmea.com/2017/03/02/dubai-wants-to-become-a-global-benchmark-for-smart-cities. Accessed Time: 02.03.2017.

[4] Z. Sang, Z. Luo, M. Mulquin, Standardization roadmap for smart sustainable cities. Technical report, International Telecommunication Union (ITU), 2015.

[5] M. Dönmez, Akıllı şebekeler ve entegrasyon (smart grids and integration), BTC Business Technology, 2013.

[6] Siemens Aktiengesellschaft, Smart grids and the new age of energy, http://www.energy.siemens.com/hq/de/stromuebertragung/transformatoren/assets/pdf/siemens-transformers-power-engineering-guide-7-1.pdf, 2014. Accessed Time:01.04.2021

[7] S. Borlase, Smart grids: infrastructure, technology, and solutions, CRC Press, 2016.

[8] Cisco Energy Optimization Service, http://www.cisco.com/web/strategy/docs/energy/energy_optimization_service_aag.pdf, retrieved from CISCO, 2021. Accessed Time:07.05.2021.

[9] F. Feroze, N. Javaid, Towards Enhancing Demand Side Management using Evolutionary Techniques in Smart Grid. 10.13140/RG.2.2.34456.49920, 2017.

[10] S. Iyer, Cyber Security for Smart Grid, Cryptography, and Privacy, International Journal of Digital Multimedia Broadcasting, USA, 2011.

[11]Hacmageddon,https://www.hackmageddon.com/2018/04/17/16-31-march-2018-

cyberattacks-timeline/. Accessed Time:: 21.03.2021.

[12] Y. Yan, et al., A Survey on Cyber Security for Smart Grid Communications, IEEE Communications Surveys & Tutorials, Vol. 14, No. 4, 2012.

[13] S. Goel, and A. Jindal, Evolving Cyber Security Challenges to the Smart Grid Landscape, International Journal of Advance Research, Ideas and Innovations in Technology, 2017.

[14] M. Yıldız, Siber Suçlar ve Kurum Güvenliği, Denizcilik Uzmanlık Tezi, T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2014.

[15] M. Kara, and S. Çelikkol, Kritik Altyapılar: Elektrik Üretim ve Dağıtım Sistemleri SCADA Güvenliği, 4. Ağ ve Bilgi Güvenliği Sempozyumu. Accessed Time:07.05.2021, 2011.

[16] E. Knapp, Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems, Elsevier Inc, 2011.

[17] M. Burmester and et al., Modeling security in cyber-physical systems, https://www.sciencedirect.com/science/journal/18745482, Pages 118-126, 2012.

[18] E. B. Rice, A. AlMajali, Mitigating the Risk of Cyber Attack On Smart Grid Systems, Science Direct, Elsevier, Procedia Computer Science 28, pp. 575 – 582, 2014.

[19] A. Ashok et al., Cyber-physical security of Wide-Area Monitoring, Protection and Control in a smart grid environment, Journal of Advanced Research, Cairo University, 2014.

[20] A. Anwar, A.N. Mahmood, Cybersecurity of smart grid infrastructure, The State of the Art in Intrusion Prevention and Detection, CRC Press, Taylor & Francis Group, USA, pp. 449-472, January 2014.

[21] T. Liu et al, Abnormal traffic-indexed state estimation: Acyber–physical fusion approach for Smart Grid attack detection, Elsevier, 2015.

[22] Suleiman, H. et al., Integrated smart grid systems security threat model, Elsevier, 2015.

[23] A. Arabo, Cyber Security Challenges within the Connected Home Ecosystem Futures, Procedia Computer Science, Volume 61, 2015, pp. 227-232, 2015.

[24] W. Knowles et al., 2015, A survey of cybersecurity management in industrial control systems, International Journal of Critical Infrastructure Protection Volume 9, p. 52-80, June 2015.

[25] R. Tawde et al., Cyber Security in Smart Grid SCADA Automation, IEEE Sponsored 2nd International Conference on Innovations in Information, Embedded, and Communication Systems (ICIIECS), 2015.

[26] Z. Drias et al., Analysis of Cyber Security for Industrial Control Systems, International Conference on Cyber Security of Smart Cities, Industrial Control System, and Communications (SSIC), 2015.

[27] Y. Cherdantseva et al., A review of cybersecurity risk assessment methods for SCADA systems, Computers & Security, Volume 56, February 2016, p.1-27, 2016.

[28] M. Wei, W. Wang, Data-centric threats and their impacts to real-time communications in smart grid, Computer Networks, Volume 104, p. 174-188, 2016.

[29] S. Mishra et al., Optimal packet scan against malicious attacks in smart grids, Theoretical Computer Science, Volume 609, Part 3, pp. 606-619, 2016.

[30] D. Young et al., A framework for incorporating insurance in critical

infrastructure cyber risk strategies, International Journal of Critical Infrastructure Protection Volume 14, p. 43-57, 2016.

[31] M. Şenol, Siber Güçle Caydırıcılık Ama Nasıl?, Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, Cilt:2, No:2, Ankara, pp.10-17, 2016.

[32] S. Borlase, Smart grids: infrastructure, technology, and solutions, 2017.

[33] X. Zhou et al., What should we do? A structured review of SCADA system cyber security standards, Proceedings of 2017 4th International Conference on Control, Decision and Information Technologies (CoDIT'17) , Barcelona, Spain, 2017.

[34] V. L. Do et al., Security of SCADA Systems Against Cyber-Physical Attacks, IEEE A&E System Magazine, 2017.

[35] M. M. Pour et al., A Review on Cyber Security Issues and Mitigation Methods in Smart Grid Systems, IEEE, 2017.

[36] S. D. Antón et al., Two Decades of SCADA Exploitation: A Brief History, IEEE Conference on Application, Information and Network Security (AINS), 2017.

[37] M. Kuzlu et al., A Comprehensive Review of Smart Grid Related Standards and Protocols, ICSG Istanbul, 2017.

[38] R. Deng et al., CCPA: Coordinated Cyber-Physical Attacks and Countermeasures in Smart Grid, IEEE Transactions on Smart Grid, Vol. 8, No. 5, 2017.

[39] M. U. Shaileshwari et al., Software Defined Networking for Smart Grid Communications and Security Challenges, ISGW 2017: Compendium of Technical Papers, p. 103-112, 2017.

[40] S. Nazir et al., Assessing and augmenting SCADA cybersecurity: A survey of techniques, Computers & Security Volume 70, September 2017, pp. 436-454, 2017.

[41] A. S. Bretas et al., Smart grids cyber-physical security as a malicious data attack: An innovation approach, Electric Power Systems Research, Volume 149, pp. 210-219, 2017.

[42] P. Eder-Neuhauser et al., Cyber-attack models for smart grid environments, Sustainable Energy, Grids and Networks Volume 12, p. 10-29, 2017.

[43] Z. A. Baig et al., Future challenges for smart cities: Cyber-security and digital forensics, Digital Investigation Volume 22, pp. 3-13, 2017.

[44] A. AlDairi, L. Tawalbeh, Cyber Security Attacks on Smart Cities and Associated Mobile Technologies, The International Workshop on Smart Cities Systems Engineering, Elsevier, 2017.

[45] A.O. Otuoze et al., Smart grids security challenges: Classification by sources of threats, Journal of Electrical Systems and Information Technology, 2018.

[46] L. A. Maglaras et al., Cybersecurity of critical infrastructures, ICT Express, Volume 4, Issue 1, 2018.

[47] X. Luo et al., Observer-based cyber-attack detection and isolation in smart grids, International Journal of Electrical Power & Energy Systems Volume 101, p. 127-138, 2018.

[48] D. Ding et al., A survey on security control and attack detection for industrial cyber-physical systems, Neurocomputing Volume 275, p. 1674-1683, 2018.

[49] S. Saini et al., Modelling for Improved Cyber Security in Smart Distribution System, International Journal on Future Revolution in Computer Science & Communication Engineering, Volume: 4 Issue: 2, pp.56-59, 2018.

[50] M. N. Kurt et al., Real-Time Detection of Hybrid and Stealthy Cyber-Attacks in

Smart Grid, Cornell University Library, 2018.

[51] M-E. Pate-Cornell et al., Cyber Risk Management for Critical Infrastructure: A Risk Analysis Model And Three Case Studies, Risk Analysis, Vol. 38, No. 2, 2018.

[52] M. N. Kurt, et al., Distributed Quickest Detection of Cyber-Attacks in Smart Grid, IEEE Transactions on Information Forensics and Security, Vol. 13, Number: 8, 2018.

[53] M. U. Tarıq, and M. Wolf, Improving the Safety and Security of Wide-Area Cyber-Physical Systems Through a Resource-Aware, Service-Oriented Development Methodology, Proceedings of the IEEE | Vol. 106, No. 1, 2018.

[54] J. Lopez et al., A Resilient Architecture for the Smart Grid, IEEE Transactions on Industrial Informatics, 2018.

[55] A. Farraj et al., A Distributed Control Paradigm for Smart Grid to Address Attacks on Data Integrity and Availability, IEEE Transactions On Signal and Information Processing Over Networks, Vol. 4, No. 1, 2018.

[56] L. Che et al., Cyber Cascades Screening Considering the Impacts of False Data Injection Attacks, Transactions on Power Systems, IEEE, 2018.

[57] M. U. Şimşek et al., TPS3: A privacy-preserving data collection protocol for smart grids, Information Security Journal: A Global Perspective, p.102-118, 2018.

[58] Z. Ni and S. Paul, "A Multistage Game in Smart Grid Security: A Reinforcement Learning Solution," in IEEE Transactions on Neural Networks and Learning Systems, vol. 30, no. 9, pp. 2684-2695, Sept. 2019, DOI: 10.1109/TNNLS.2018.2885530.

[59] S.-K. Kim, J.-H. A. Huh, Study on the Improvement of Smart Grid Security Performance and Blockchain Smart Grid Perspective, Energies 2018, 2018.

[60] Z. El Mrabet, N. Kaabouch, H. El Ghazi, H. El Ghazi, Cyber-security in smart grid: Survey and challenges. Computers & Electrical Engineering, 67, pp. 469-482, 2018.

[61] K. K. Kimani, O. V. Vitalice, K. Langat, Cybersecurity challenges for IoT-based smart grid networks, International Journal of Critical Infrastructure Protection, Volume 25, Pages 36-49, 2019.

[62] E. Hossain, I. Khan, F. Un-Noor, S. S. Sikander, and M. S. H. Sunny, "Application of Big Data and Machine Learning in Smart Grid, and Associated Security Concerns: A Review," in IEEE Access, vol. 7, pp. 13960-13988, 2019.

[63] S. N. Islam, Z. Baig, S. Zeadally, Physical layer security for the smart grid: vulnerabilities, threats, and countermeasures. IEEE Transactions on Industrial Informatics, 15(12), 6522-6530, 2019.

[64] J. Sakhnini et al., Security aspects of Internet of Things aided smart grids: A bibliometric survey, Internet of Things, 100111, 2019.

[65] P. Kumar, Y. Lin, G. Bai, A. Paverd, J. S. Dong and A. Martin, "Smart Grid Metering Networks: A Survey on Security, Privacy and Open Research Issues," in IEEE Communications Surveys & Tutorials, vol. 21, no. 3, pp. 2886-2927, 2019.

[66] S. De Dutta, R. Prasad, Security for Smart Grid in 5G and Beyond Networks. Wireless Pers Commun 106, 261–273 2019. https://doi.org/10.1007/s11277-019-06274-5, 2019.

[67] A. Gusrialdi, Z. Qu, Smart Grid Security: Attacks and Defenses. In: Stroustrup J.,

Annaswamy A., Chakrabortty A., Qu Z. (eds) Smart Grid Control. Power Electronics and Power Systems. Springer, Cham. https://doi.org/10.1007/978-3-319-98310-3_13, 2019.

[68] F. A. Khan, M. Asif, A. Ahmad, M. Awais, H. A. Alharbi, Blockchain technology, improvement suggestions, security challenges on the smart grid and its application in healthcare for sustainable development, Sustainable Cities and Society, Volume 55, 102018, 2020.

[69] M. B. Mollah et al., "Blockchain for Future Smart Grid: A Comprehensive Survey," in IEEE Internet of Things Journal, DOI: 10.1109/JIOT.2020.2993601, 2020.

[70] M.Z. Gunduz, and R. Das, Cyber-security on the smart grid: Threats and potential solutions, Computer Networks, Volume 169, 107094, 2020.

[71] C.-M. Mathas et al., Threat landscape for smart grid systems. In Proceedings of the 15th International Conference on Availability, Reliability and Security (ARES '20). Association for Computing Machinery, New York, NY, USA, Article 111, 1–7. DOI: https://doi.org/10.1145/3407023.3409229, 2020.

[72] M. A. Ferrag et al., Cybersecurity for fog-based smart grid SCADA systems: Solutions and challenges, Journal of Information Security and Applications, Volume 52, 102500, 2020.

[73] M. F. Moghadam, M. Nikooghadam, A. H. Mohajerzadeh, B. Movali, A lightweight key management protocol for secure communication in smart grids, Electric Power Systems Research, Volume 178, 106024, 2020.

[74] Y. A. Zhang, H. Schwefel, H. Mohsenian-Rad, C. Wietfeld, C. Chen, and H. Gharavi, "Guest Editorial Special Issue on Communications and Data Analytics in Smart Grid," in IEEE Journal on Selected Areas in Communications, vol. 38, no. 1, pp. 1-4, 2020.

[75] H. Hittini, A. Abdrabou, L. Zhang, FDIPP: False Data Injection Prevention Protocol for Smart Grid Distribution Systems. Sensors 2020, 20, 679, 2020.

[76] B. R. Amin, S. Taghizadeh, S. Maric, M. J. Hossain, R. Abbas, Smart Grid Security Enhancement by Using Belief Propagation, IEEE Systems Journal, 2020.

[77] M. Shrestha, C. Johansen, J. Noll, D. Roverso, A Methodology for Security Classification applied to Smart Grid Infrastructures, International Journal of Critical Infrastructure Protection, 28, 100342, 2020.

[78] P. R. Jeyaraj, E. R. S. Nadar, A. Kathiresan, S. P. Asokan, Smart grid security enhancement by detection and classification of non-technical losses employing deep learning algorithm, International Transactions on Electrical Energy Systems, e12521, 2020.

[79] I. Gandhi, L. Ravi, V. Vijayakumar, V. Subramaniyaswamy, Improving Security for Wind Energy Systems in Smart Grid Applications using Digital Protection Technique, Sustainable Cities and Society, 102265, 2020.

[80] A. A. Khan, V. Kumar, M. Ahmad, S. Rana, D. Mishra, PALK: Password-based anonymous lightweight key agreement framework for smart grid, International Journal of Electrical Power & Energy Systems, Volume 121, 106121, ISSN 0142-0615,https://doi.org/10.1016/j.ijepes.2020. 106121, 2020.

[81] S. Tufail, S. Batool, A. I. Sarwat, False Data Injection Impact Analysis In AI-Based Smart Grid, 10.13140/RG.2.2.32994.25282, 2021.