Software-Defined Networking for Improving Security in Smart Grid Systems

Sedef Demirci, Seref Sagiroglu
Gazi University, Engineering Faculty, Computer Engineering Department
Ankara, Turkey
sedefgunduz@gazi.edu.tr, ss@gazi.edu.tr

***Abstract*— This paper presents a review on how to benefit from software-defined networking (SDN) to enhance smart grid security. For this purpose, the attacks threatening traditional smart grid systems are classified according to availability, integrity, and confidentiality, which are the main cyber-security objectives. The traditional smart grid architecture is redefined with SDN and a conceptual model for SDN-based smart grid systems is proposed. SDN based solutions to the mentioned security threats are also classified and evaluated. Our conclusions suggest that SDN helps to improve smart grid security by providing real-time monitoring, programmability, wide-area security management, fast recovery from failures, distributed security and smart decision making based on big data analytics.**

Keywords*— *software-defined networking; SDN; smart grid; cyber security; attacks; big data

I. INTRODUCTION

A Smart Grid system is a network in which the electricity is generated and delivered to the consumer by integrating the actions of all connected users (such as generators, consumers, etc.) intelligently [1]. Smart grid systems use two-way communication technologies to integrate thousands of power elements and ensure the communication among those elements. The communication network part of the current grid systems are based on traditional IP networks. That is, every agent in the grid should know its adjacencies and contact with them using their IP addresses. However, this decentralized approach causes routers to make packet forwarding case by case according to the rules of a pre-defined routing protocol. [2]. In addition, decisions on network functionality are made in design stage in such a network, so reconfiguring network according to its needs in real-time becomes almost impossible. This non-dynamic structure of today's SGs causes bottlenecks in terms of performance and resilience while makes the network vulnerable to many attack types [3]. On the other hand, network components in a SG communication infrastructure are owned and operated by public services and energy companies. Managing these networks becomes very difficult when the scale increases drastically. Moreover, the devices and applications in the infrastructure become incompatible as the number of different vendors increases, and the maintenance and upgrading of these vendor-specific devices require substantial budget and workforce [4].

Due to these reasons, researchers conclude that it is essential to improve current SG infrastructure, make it a reconfigurable network that can take dynamic decisions and more secure against various types of attacks. In line with these objectives the idea of implementing SDN (Software-Defined Networking) paradigm on SG technology has emerged [3, 5]. SDN is a new networking technology that makes the network programmable by abstracting control logic from underlying devices and assigns this task to a logically centralized controller software. With SDN, understanding and provisioning the behavior of the network becomes easier so that managing network security and operation could be achieved in a more effective way.

This work presents a review on how to benefit from SDN to secure SG systems. The rest of the paper is organized as follows: We give a brief explanation of traditional SG architecture in Section 2. In Section 3, we describe the attacks threatening traditional SG systems and classify them in main cyber security objectives. We introduce SDN briefly and re-define the SG architecture with SDN in Section 4. In Section 5, we classify SDN based solutions to security threats in SG systems. Finally, in Section 6, we summarized the paper and give suggestions for future work.

II. TRADITIONAL SMART GRID ARCHITECTURE

A SG system is simply defined as a computer integrated power electric grid that monitor energy distribution and usage with communication network on top of it. SG systems provide real-time bidirectional information transfer at every stage of energy from generation to the consumption. Thus, it offers a sustainable, secure and efficient energy network [6, 7]. A SG system consists of six main components: (i) smart generation, (ii) smart stations, (iii) smart distribution, (iv) smart meters, (v) integrated communication, and (vi) advanced control methods. Smart generation means producing energy by considering feedbacks coming from real-time data flows and using reasonable cause and effect relations in a production and supply chain. It aims to generate power that is able to adjust voltage and frequency automatically. Smart stations are used for controlling critical and non-critical processes such as following transformers, batteries, and power factor performance etc. Smart distribution systems can predict failures by using weather conditions and power history data due to their automatic tracking and analysis capabilities. Smart meters provide two-way communication between consumer and provider by using the communication infrastructure such as GPRS, PLC, and RF etc. They can collect and transmit payment information, electrical failures, deception and consumption data. Integrated communication refers to the

978-1-5386-5982-3/18/$31.00 ©2018 IEEE

user's interaction with smart electronic devices in a system integrated with protection and control systems. Finally, advanced control methods means the devices and algorithms that analyze and predict the status of the grid. They prevent energy failures and power quality problems taken by taking corrective measures automatically [9].

III. Security Issues in Traditional Smart Grid Systems

The information exchange among the components of a SG system relies on the open communication technologies. Hence, cyber security is one of the most crucial topics for reliable and secure operations in SG. In order to provide reliability and security in these systems, it is essential to understand (i) security objectives, (ii) the attacks threaten these objectives and the (iii) precautions that must be taken against these attacks. The high level security objectives for the SG are defined as availability, integrity and confidentiality by the cyber security working group in the NIST SG interoperability panel. In this section, we briefly describe the attacks threatening SG systems and classify them based on main cyber-security objectives as availability, integrity, and confidentiality.

A. Attacks Targeting Availability

The attacks threatening availability attempts to block, delay, or disrupt the operation of the network [10].

1) DoS (Denial-of-Service): The attacker aims to prevent the communication of a particular component in SG with the rest of the network by disrupting one or more routing functions of the network devices [11]. For this purpose, the attacker send unlimited data requests to the targeted unit and consequently leaves it out of service [12].

2) Congestion: The attacker not only listens the data flow between two nodes, but also creates links through other nodes and aims to use all of the available bandwidth capacity. Thus, if the attacker can clog even one of the nodes in the chosen path, the victim's quality of service level decreases and the congestion is created [13].

B. Attacks Targeting Integrity

The attacks aiming to modify or disrupt the data exchanged among the components of the SG targets integrity [10].

1) Compromising: A grid device is compromised in order to use it for further and more sophisticated attacks such as DoS or congestion attacks etc.[14]. For example a compromised power meter may produce false readings and change the grid operation, a compromised circuit breaker may cause power outage by breaking the circuit maliciously [15], or placing a compromised node beside a non-compromised one causes breaking security and secrecy [16]. Furthermore, a compromised node can potentially compromise other nodes [17, 18].

2) ARP Poisoning: The ARP (Address Resolution Protocol) is responsible from resolve IP addresses to the MAC addresses. These matches are stored on the ARP tables. In ARP poisoning attacks, fake MAC addresses is created for the legitimate IP address in the table. Thus, the attacker can change the traffic or stop it completely [5]. In another scenario, the attacker can change the MAC address of a legitimate host with a malicious host's MAC address by modifying the entry in its ARP table, so that the attacker can launch more sophisticated attacks such as DoS or man-in-the middle etc. [19].

3) Session Hijacking: As mentioned in the previous attack type, the host profiles including host location, MAC and IP addresses for each host are kept in the network However, the location update mechanisms suffering from lack of authentication makes the SG systems vulnerable to host hijacking attacks. In this type of attack, the attacker takes control of an authorized node that has a valid connection. Then, he/she uses it for establishing a malicious communication with the victim [20].

C. Attacks Targeting Confidentiality

Finally, the attacks threaten confidentiality tries to acquire the unauthorized data from the grid network [10].

1) Eavesdropping: In SCADA systems, TCP/IP protocol is used to provide reliability, because this protocol guarantees to deliver all the data packets in order and without error. However, this protocol does not consider security issues allowing attackers to monitor or eavesdrop the transmitted data. In addition, SCADA systems are connected to the Internet in a direct or indirect way to control and maintain its components remotely, which results in making them prone to be eavesdropped by suspicious assets [12]. In eavesdropping attack, the attacker listens the data in the asset layer passively. Moreover, he/she can analyze the monitored data flowing among power grid devices to infer meaningful information. The worst aspect of this attack is that it is hard to detect since carried out passively without revealing itself [4].

2) Man-in-the-Middle: It is an active attack on the contrary of eavesdropping. The attacker includes him/herself between two components of the grid and sniffs the sensitive data like login credentials etc. flowing between that components. After capturing the traffic, he/she can compromise a node, and thus can take the full control of the whole network [21, 22].

IV. Re-defining Smart Grid Architecture with Software-Defined Networking

A. Software-Defined Networking (SDN)

SDN is a new paradigm that centralizes network control logically by separating it from the data forwarding devices comprising the network infrastructure and enables the network to be programmed by a central software unit [23]. The primary idea behind SDN is to separate the control plane from the data plane in networks. Control plane, the brain of the network, hosts controller software that defines routing rules and decides where to route the traffic. In the data plane, there are programmable network devices routing the traffic according to the rules defined by the controller. The application layer provides another layer of abstraction, and hosts network functions (e.g. load balancing, firewall, intrusion detection system etc.) implemented on top of the control layer [24]. Figure 1 shows SDN architecture as described by Open

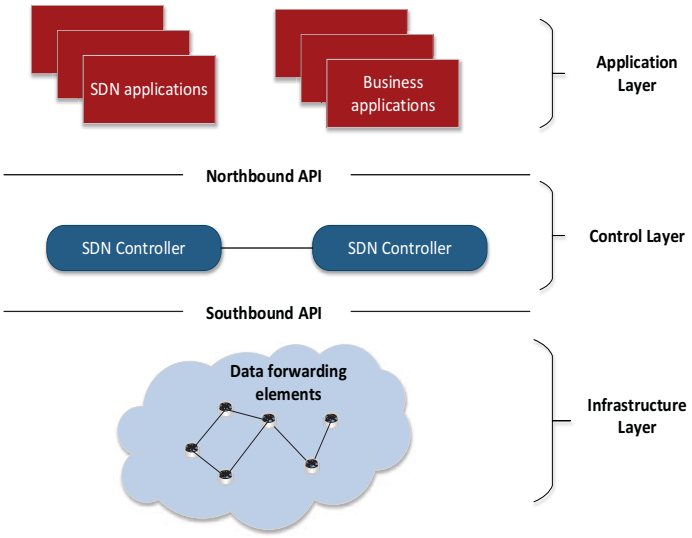

Fig. 1. SDN Layers

Networking Foundation (ONF) [25]. In order to explain SDN principles shown in Figure 1 in detail, we explain the layers and connections between them as follows.

1) Infrastructure Layer: This layer, also known as data plane, is composed of routing elements responsible for packet switching and transmission, similar to traditional network architecture. However, unlike traditional network devices, these elements cannot make autonomous decisions since they do not contain embedded software or a control unit. Instead, these programmable routers and switches forward packets according to the rules defined by the controller [26].

2) Control Layer: In this layer, there are one or more software controllers, which manage the forwarding behavior and are considered the brain of the network. The controller's job is to determine forwarding rules and write these on the flow tables of programmable switches in the data plane via a Southbound API [27]. There are many SDN controllers (NOX, POX, Floodlight, Beacon, DIFANE etc.) developed with varying goals and priorities [23].

3) Southbound API: It provides a protocol for communication between the controller and data forwarding devices. Today, the most common protocol and de facto standard for Southbound API is the OpenFlow protocol developed at Stanford University [28]. OpenFlow enables secure communication in SDN by determining the format of messages owing from the controller to the programmable switches, and vice versa.

4) Application Layer: It contains applications performing various functions such as load balancing, traffic filtering, monitoring, etc., to provide network management, control and orchestration [29]. Each of these applications defines policies to accomplish its function. These policies are conveyed to the controller by a Northbound API and they are used for programming the SDN switches after being converted to OpenFlow rules [23].

5) Northbound API: It is an interface used in communication between the application and control layers. In other words, it enables applications to program the network. With this interface, developers can develop applications using high-level languages such as Python, Java, C++ etc. It abstracts the details of data plane devices and allows a wide range of users such as network administrators, service providers and researchers to customize the control rules and behavior of their networks [30].

B. SDN-Based Smart Grid Architecture

The communication network part of the current grid systems are based on traditional IP networks. That is, every agent in the grid should know its adjacencies and contact with them using their IP addresses. However, this decentralized approach causes routers to make packet forwarding case by case according to the rules of a pre-defined routing protocol. [2]. In addition, decisions on network functionality are made in design stage in such a network, so reconfiguring network according to its needs in real-time becomes almost impossible. This non-dynamic structure of today's SGs causes bottlenecks in terms of performance and resilience while makes the network vulnerable to many attack types [3].On the other hand, network components in a SG communication infrastructure are owned and operated by public services and energy companies. Managing these networks becomes very difficult when the scale increases drastically. Moreover, the devices and applications in the infrastructure become incompatible as the number of different vendors increases, and the maintenance and upgrading of these vendor-specific devices require substantial budget and workforce [4]. Due to these reasons, researchers conclude that it is essential to improve current SG infrastructure. In line with these objectives the idea of implementing software-defined networking paradigm on SG technology has emerged [3, 5]. As mentioned in the previous section, SDN makes the network programmable by abstracting control logic from underlying devices and assigns this task to a logically centralized controller software. In SDN enabled SG approach, switches can be reset and grid control can be reshaped thanks to the programmable structure of the SDN.

The logically centralized nature of the controller makes it easier to analyze and envisage grid behavior. Thus, SG systems become dynamic and optimizable in real-time. In addition, managing the grid becomes easier since vendor dependency is eliminated via SDN, which is a key contribution to facilitating innovation [31]. Besides, the compromised switches in the network can easily be detected and fast recovery from the effects of cyber-attacks is provided in SDN enabled SG systems [5]. The overview of the SDN enabled SG system is given in Figure 2.

1) Asset Layer: There are base elements of SG network (SCADA slaves, sensors, Phasor Measurement Units (PMUs), relays, meters etc.) in this layer. These elements cannot make autonomous decisions since they do not have a control unit. This layer is just responsible to collect critical data and be main repository for the SG system [32].

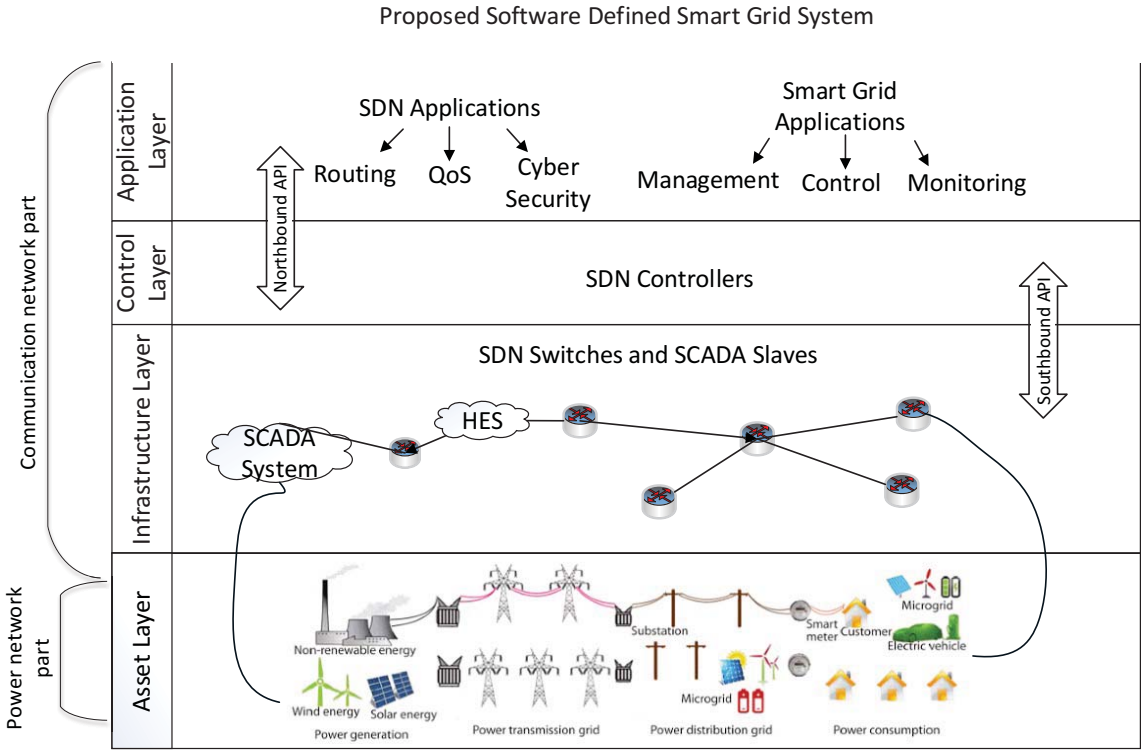

Fig. 2. Proposed SDN-enabled SG system

2) Infrastructure Layer: There are programmable SDN switches in this layer. It is responsible to forward grid data collected by the underlying assets according to the rules defined by the controller residing on control layer. The elements on this layer also cannot take routing decisions independent from the brain of the network [32].

3) Control Layer: In this layer, there are one or more SDN controllers. The task of the controller is to maintain data traffic by determining forwarding rules and write them on the flow tables of programmable SDN switches residing in the infrastructure layer. The communication between control and infrastructure layer is provided by the Southbound API. Today, the de facto standard and the most common protocol for Southbound API is the OpenFlow protocol [33]. It provides a secure communication by determining the format of messages flowing from the controller to the SDN switches, and vice versa.

4) Application Layer: SDN applications and SG applications reside in this layer. SG applications are responsible from performing various grid applications:, managing grid devices, controlling frequency and voltage, and monitoring grid status. On the other hand, SDN applications perform routing functions, QoS functions (such as load-balancing, managing delays etc.), and finally cyber security functions like traffic filtering, intrusion detection/prevention, deep packet inspection etc. The policies defined by all these applications are conveyed to the control layer by means of Northbound API. It converts the application policies to OpenFlow rules to be transmitted to the switches in the infrastructure layer [18].

V. SDN-Based Security Solutions for Smart Grid Systems

In this Section, we discuss how SDN is used for enhancing SG security and classify how to detect, mitigate and prevent the security threats in SG systems by taking advantages of SDN technology. This classification is also depicted in Figure 3.

A. Real-Time Traffic Monitoring

By using SDN concept, the insider attacks can be detected and mitigated effectively in SG networks by monitoring and analyzing the network traffic in real-time. According to Wu and Wei [13] the controller residing in the control plane can act as a traffic monitor. It periodically probes the data about lost, sent, and received data from the OpenFlow switches, and evaluates this data in terms of Quality of Service. In addition, the analysis of users' feedback are conducted by the Quality of Experience application residing in application layer to the controller. Finally, those QoS and QoE evaluation feedbacks are used by the controller to decide whether a malicious behavior exists or not. In this regard, if an attack is detected, the static predefined routes are changed and new reactive routes are defined by the controller so as to update the flow tables of the switches.

B. Programmability

The adoption of SDN makes SG system more resilient to attacks since the SDN facilitates the development and implementation of cyber security functions such as firewall, IDS/IPS (intrusion detection/prevention systems) due to its

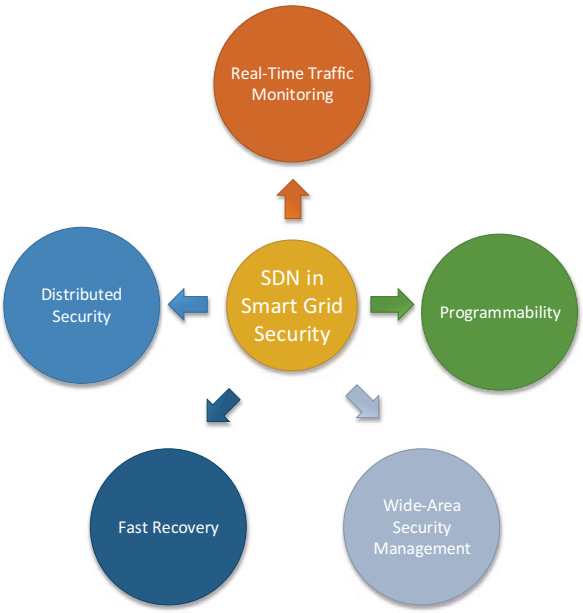

Fig. 3. Classification of SDN-based solutions for providing security in SG systems

programmable nature. The SDN controller can change the routes of the grid flows at runtime by analyzing the link information collected by itself, if a malicious behavior is detected. Thus, the traffic is routed over more reliable, secure and efficient paths [21]. In addition, adding a new security function or upgrading existing ones is much easier when compared with the traditional SG systems, since the SDN enables flexibility and rapid softwarization [12].

C. *Wide-Area Security Management*

Vertical integration which means the production of software and hardware of a SG element from the same company slows down innovation and complicates making changes, which is the case in the communication part of the traditional SG systems. However, with OpenFlow which is the main communication protocol of SDN, this issue is eliminated since it is a standard API allowing to manage SG components produced by different vendors. Thus, management of the different security functions and devices becomes possible, and the threats can be detected, mitigated and prevented more easily than the traditional grid architecture. In addition, this standardization brings along to manage grid elements that are geographically dispersed over wide-areas [12].

D. *Fast Recovery*

In case of an attack, link failure or error, it is very crucial to recover the grid quickly for maintaining its operation and stability. In such a case, the new alternative routes should be established and switch configurations should be created for this routes immediately in order to guarantee transmission and control of the traffic flows. Since the SDN makes SG systems programmable, recovery from the failures becomes possible just with a few clicks while it requires complicated algorithms and processes in traditional SG systems [34].

E. *Distributed Security*

As the grid size grows, it becomes more difficult to manage it in terms of every type of network operation and cyber security. In this case, it makes more sense to cluster the network and managing each cluster separately. Implementing this logic with SDN by assigning a controller to each cluster is much easier and a dynamic solution when compared to the legacy grids. In such an architecture, the controller controls and manages all devices in its own cluster in addition to communicating with other clusters. Each controller is responsible from monitoring, analyzing and securing its own cluster from inside and outside attacks as well as managing the network operation inside that cluster. Thus, cyber security is provided in a distributed manner with SDN when the grid size becomes unmanageable in terms of network operation and security issues [35].

VI. Concluding Remarks

In this paper, we present an overview of the traditional SG architecture and the cyber-security issues threatening these systems. We introduce SDN technology which is the building block of the future information technologies, and present a review on how to benefit from SDN technology to secure SG systems. We re-define the SG architecture with SDN and classify SDN based solutions to security threats in SG systems.

Our conclusions can be listed as follows:

- With SDN, cyber-attacks can be detected and mitigated effectively in SG systems since it provides monitoring and analyzing the traffic in real-time.
- Since SDN makes the networks programmable, it makes the SG systems more resilient and flexible in terms of developing and implementing cyber-security functions and recovering the system from failures.
- Wide-area grid management, in terms of cyber-security and interoperability, becomes easier since SDN provides simplified system management.
- SDN shares many common goals with Network Function Virtualization (NFV). NFV is a new technology that decouples network functions from dedicated hardware and implementing them as software on industrial standard high volume servers. Implementing NFV and SDN technologies together would remove hardware dependency as in SDN, and reduce hardware cost and energy consumption on SG systems.
- The data collected by the OpenFlow switches can be analyzed by the big data analytics module on the control layer, or the modules residing at a new layer in between infrastructure and control layers. Then, the statistical results can be integrated to the decision-making mechanisms of the SG systems.

As a result, in this work, we answer the question of "How to secure SG systems with SDN?" However, Software-Defined SG Systems would also be vulnerable to several attack types. Moreover, new types of security threats would emerge for these new SG architectures. There are not much studies focusing on

this issue. Therefore, "How to secure SDN-based SG systems?" would be a promising line of future research.

REFERENCES

[1] Colak, I., Sagiroglu, S., Fulli, G., Yesilbudak, M., & Covrig, C. F. (2016). A survey on the critical issues in smart grid technologies. Renewable and Sustainable Energy Reviews, 54, 396-405.

[2] N. Dorsch, F. Kurtz, C. Wietfeld, "Communications in distributed smart grid control: Software-defined vs. legacy networks", Conference on Energy Internet and Energy System Integration, pp. 1-6, November 2017

[3] X. Dong, H. Lin, R. Tan, R.K. Iyer, Z. Kalbarczyk, "Software-defined networking for smart grid resilience: Opportunities and challenges", 1st ACM Workshop on Cyber-Physical System Security, pp. 61-68, April 2015.

[4] K. Akkaya, A.S. Uluagac, A.Aydeger, "Software defined networking for wireless local networks i. smart grid", 40th Local Computer Networks Conference Workshops, pp. 826-831, October 2015.

[5] D. Ibdah, M. Kanani, N. Lachtar, N. Allan, B.Al-Duwairi, "On the security of SDN-enabled smartgrid systems" International Conference on Electrical and Computing Technologies and Applications, pp. 1-5, November 2017.

[6] P. McDaniel, S. McLaughlin, "Security and privacy challenges in the smart grid". IEEE Security & Privacy, (3), pp. 75-77, 2009.

[7] R. Bayindir, I. Colak, G. Fulli, K. Demirtas, "Smart grid technologies and applications", Renewable and Sustainable Energy Reviews, 66, pp. 499-516, 2016.

[8] Q.D.Ho, Y. Gao, T.Le-Ngoc, "Challenges and research opportunities in wireless communication networks for smart grid" IEEE Wireless Communications, 20(3), pp. 89-95, 2013.

[9] M. Yenilmez, "Akilli Şebekelrde (Smart Grid) Dağitim Sistem Otomasyondaki Gelişmeler", Karabük Üniversitesi, 2016.

[10] W. Wang, Z. Lu, "Cyber security in the smart grid: Survey and challenges", Computer Networks, 57(5), pp. 1344-1371, 2013.

[11] S. Gunduz, B. Arslan, M. Demirci, "A Review of Machine Learning Solutions to Denial-of-Services Attacks in Wireless Sensor Networks", 14th International Conference on Machine Learning and Applications, pp. 150-155, December 2015.

[12] E.G. da Silva, A.S. da Silva, J.A.Wickboldt, P. Smith, L.Z. Granville, A. Schaeffer-Filho, "A one-class NIDS for SDN-based SCADA systems", 40th Annual Computer Software and Applications Conference Vol. 1, pp. 303-312, June 2016.

[13] Y.Wu, J. Wei, "Towards attack-resilient communications for smart grids with software-defined networking" Power & Energy Society General Meeting, pp. 1-5, July 2017.

[14] X. Li, X. Liang, R. Lu, X. Shen, X. Lin, H. Zhu, "Securing smart grid: cyber attacks, countermeasures, and challenges", IEEE Communications Magazine, 50(8), 2012.

[15] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, K. Poolla, "Smart grid data integrity attacks", IEEE Transactions on Smart Grid, 4(3), pp. 1244-1253, 2013.

[16] Y. Mo, T.H.J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, B. Sinopoli, "Cyber–physical security of a smart grid infrastructure", Proceedings of the IEEE, 100(1), pp. 195-209, 2012.

[17] J. O'Raw, D.M. Laverty, D.J. Morrow, "Software defined networking as a mitigation strategy for data communications in power systems critical infrastructure",Power and Energy Society General Meeting,pp.1-5, 2016

[18] U. Ghosh, P. Chatterjee, S. Shetty, "A security framework for SDN-Enabled smart power grids", 37th International Conference on Distributed Computing Systems Workshops, pp. 113-118, June 2017.

[19] Y. Yang, K. McLaughlin, T.S. Littler, E.G. Im, Z.Q. Yao, H.F. Wang, "Man-in-the-middle attack test-bed investigating cyber-security vulnerabilities in smart grid SCADA systems", 2012.

[20] S. Goel, Y. Hong, V. Papakonstantinou, D. Kloza,"Smart Grid Security", Springer-Verlag London, 2015.

[21] E. Hammad, J. Zhao, A. Farraj, D. Kndur, "Mitigating link insecurities in smart grids via QoS multi-constraint routing", International Conference on Communications Workshops, pp. 380-386, May 2016.

[22] M. Brooks, B. & Yang, "A Man-in-the-Middle attack against OpenDayLight SDN controller", 4th Annual ACM Conference on Research in Information Technology, pp. 45-49, September 2015.

[23] D. Kreutz, F.M. Ramos, P.E., Rothenberg C.E. Verissimo, S. Azodolmolky, S. Uhlig, "Software-defined networking: A comprehensive survey", Proceedings of the IEEE, 103(1), 14-76, 2015.

[24] N. Feamster, J. Rexford, E. Zegura, "The road to sdn: an intellectual history of programmable networks", Computer Communication Reviews, 44(2), pp. 87-98, 2014.

[25] Software-Defined Networking Definition. https://www.opennetworking.org/sdn-definition/, [Accessed 2-April-2018].

[26] B.A.A. Nunes, M. Mendonca, X.N. Nguyen, K. Obraczka, T. Turletti, "A survey of software-defined networking: Past, present, and future of programmable networks", IEEE Communication Survey Tutorials 16(3), pp. 1617-1634, 2014.

[27] ONF. Sdn architecture. https://www.opennetworking. org/images/stories/downloads/sdn-resources/technical-reports/TR SDN ARCH 1.0 06062014.pdf, [Accessed 2-April-2018].

[28] I. Ahmad, S. Namal, M. Ylianttila, A. Gurtov, "Security in software defined networks: A survey", IEEE Communication Survey Tutorials 17(4), pp. 2317-2346, 2017.

[29] H.Kim,N.Feamster,"Improving network management with software defined networking",IEEE Communications Magazine,51(2),114-119,2013.

[30] F. Hu, Q. Hao, K. Bao, "A survey on software-defined network and openow: from concept to implementation", IEEE Communications Magazine, 16(4), pp. 2181-2206, 2014.

[31] J. Kim, F. Filali, Y.B. Ko, "Trends and potentials of the smart grid infrastructure: from ICT sub-system to SDN-enabled smart grid architecture", Applied Sciences, 5(4), pp. 706-727, 2015.

[32] Y. Jararweh, M. Al-Ayyoub, A. Bousselham, E. Benkhelifa, "Software Defined based smart grid architecture. 12th International Conference of Computer Systems and Applications, pp. 1-7, November 2015.

[33] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, J. Turner, "OpenFlow: enabling innovation in campus networks. ACM SIGCOMM Computer Communication Review, 38(2), pp. 69-74, 2008.

[34] N. Dorsch, F. Kurtz, H. Georg, C. Hägerling, C. Wietfeld, "Software-defined networking for Smart Grid communications:Applications, challenges and advantages, SmartGridComm, pp. 422-427, 2014.

[35] C.Gonzalez, S.M.Charfadine, O.Flauzac, F.Nolot, "SDN-based security framework for the IoT in distributed grid", International Multidisciplinary Conference on Computer and Energy Science, pp. 1-5, July 2016.