Software Defined Networking for Wireless Local Networks in Smart Grid

Kemal Akkaya, A. Selcuk Uluagac and Abdullah Aydeger
Dept. of Electrical & Computer Engineering, Florida International University, Miami, FL, 33174 USA
kakkaya@fiu.edu, auluagac@fiu.edu, aayde001@fiu.edu

***Abstract*—Emerging Software Defined Networking (SDN) technology has provided excellent flexibility to large-scale networks in terms of control, management, security, and maintenance. With SDN, network architectures can be deployed and maintained with ease. New trends in computing (e.g., cloud computing, data centers, and virtualization) can seamlessly be integrated with the SDN architecture. On the other hand, recent years witnessed a tremendous growth in the upgrade and modernization of the critical infrastructure networks, namely the Smart-Grid, in terms of its underlying communication infrastructure. From Supervisory Control and Data Acquisition (SCADA) systems to Advanced Metering Infrastructure (AMI), an increasing number of networking devices are being deployed to connect all the local network components of the Smart Grid together. Such large local networks requires significant effort in terms of network management and security, which is costly in terms of labor and hardware upgrades. SDN would be a perfect candidate technology to alleviate the costs while providing fine-grained control of this critical network infrastructure. Hence, in this paper, we explore the potential utilization of the SDN technology over the Smart Grid communication architecture. Specifically, we introduce three novel SDN deployment scenarios in local networks of Smart Grid. Moreover, we also investigate the pertinent security aspects with each deployment scenario along with possible solutions.**

Keywords: SDN; wireless local networks; smart grid; microgrid; security

I. Introduction

The continuous growth of the Internet and the proliferation of smart devices and social networks pose new challenges for networks on keeping up with the dynamicity of the hardware and software. In particular, the switches and routers that are involved in the transmission of the data from these networks and devices are typically developed in a vendor specific fashion, which makes hardware and software updates a significant challenge. The emerging SDN technology is a solution to address such problems that can facilitate updates to the hardware and software used on the networking devices [5]. SDN enables splitting controls of networks and data flow operations. One of the major goals in SDN is to be able to interact with the switches and thus create an open networking architecture for everyone. In this way, one can get a global view of the entire network and will be able to make global changes without having to access to each device's unique hardware.

On the other hand, the existing power grid in the US is going through a massive transformation to make it more reliable and connected with the ability to transfer data and power in two-ways [12]. The data communication motivation necessitated upgrading the existing Smart Grid network infrastructure with different components such as home area networks (HANs), neighborhood area networks (NANs) and wide-area networks (WANs). Each of these networks deploy thousands of network devices that need to be managed continuously. Unfortunately, this massive infrastructure requires additional labor and cost for the utility companies who own these networks. Although minimizing the management cost is one of the goals of the utilities, this cost will always be relevant as long as the customers are served. In fact, the emerging SDN paradigm can provide excellent opportunity for reducing the network management cost by integrating a software-based control that can be flexible with respect to software upgrades, flow-control, security patching, and quality of service (QoS). Nonetheless, while a significant amount of work has been done in the SDN space, most of these efforts targeted the applications in the area of cloud computing, data centers and virtualization [5] and there is a need to adapt SDN for Smart Grid applications.

This work is the result of such an effort to promote the use of SDN for various applications in the Smart Grid. Specifically, we aim three different Smart Grid applications that rely on a local wireless network infrastructure. 1)*AMI applications* where meter data are collected via a mesh network that consists of smart meters and relays. Each of these equipment will have the ability to route the meter data through their routing tables. 2) *SCADA Systems*, which connects field devices such as relays, IEDs (Intelligent Electronic Devices), PLCs (Power Line Communications), and PMUs (Phasor Measurement Units) with the control center using redundant wireless connections. The control center is typically equipped with routers and switches just like a data center. 3) *Microgrid Systems* which integrates distributed power resources with the Smart Grid. The control and monitoring of these networks require the deployment of network devices for collecting data about them.

This paper is organized as follows. In II, we provide some background on SDN. In Section III, we describe how three Smart Grid applications can exploit SDN. Section IV explores potential security threats related to Smart Grid-enabled SDN. Finally, we conclude the paper in Section VI.

II. Background on SDN

SDN's main motivation is to move the control of the lookup tables inside the network devices to a separate location so

978-1-4673-6773-8/15/$31.00 ©2015 IEEE

that it can be controlled more easily. Specifically, this can be described as separation of the packet forwarding and the way how the forwarding tables are created and changed. These two processes are assumed to be on separate layers, which are referred to as *data plane* and *control plane* in SDN technology: *Control Plane* is also referred to as Network Operating System (NOS). This plane is supposed to supply network decisions for packet forwarding or dropping. On the other hand, data plane is responsible for data forwarding. SDN focuses on flow forwarding idea instead of dealing with IP or MAC-address based forwarding.

Main problem in the traditional networks was updating the network elements, which requires too much effort and time [5]. By creating a programming interface to be able to update network elements from a center (i.e., at the control plane) via SDN, such complexity in network management can be eliminated. An illustration of how SDN reorganizes the network architecture with respect to the current ones are is illustrated in Fig. 1. As can be seen from this figure, the control plane is typically controlled by a single center through some applications.

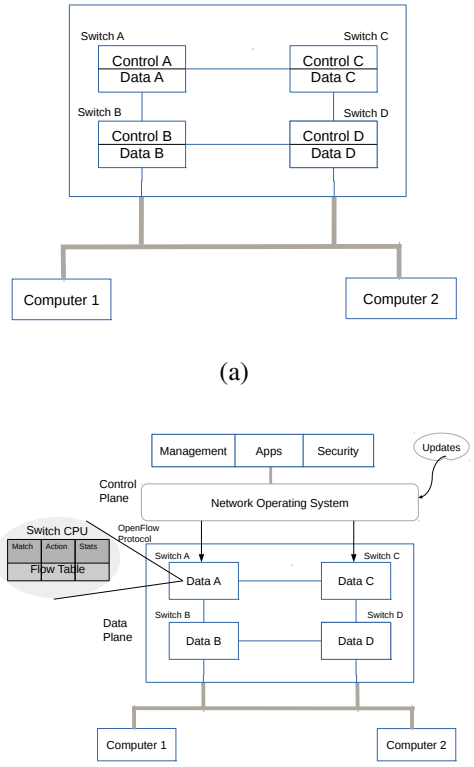

Fig. 1: Current (a) vs SDN-based (b) Networks

Today, SDN is used for a variety of networking settings. For instance, it is used in cloud computing and data centers for ease of network management and control of virtual machines (VMs) [18]. It can connect multiple data center networks by eliminating the problems of proprietary architectures. In this way, the workload can move from one network to another to save time and energy. This idea of workload offloading can also be used for mobile devices which needs more powerful machines with certain security requirements [3]. Finally, SDN can be used for Internet research for testing certain ideas without changing the current network [4].

III. Integration of SDN with The Smart Grid

In this section, we first explain the communication infrastructure for Smart Grid and then detail the applications that can benefit from the use of SDN.

A. Smart Grid Networking Architectures

Before moving into the description of how SDN can be used for Smart Grid applications, we first briefly explain the existing Smart Grid network infrastructure. Basically, there are three major components in a Smart Grid infrastructure [12]: 1) HANs that mainly connect home devices with the smart meters; 2) NANs which collect smart meter data from houses; and 3) WANs which provide long-haul communication with the utility control centers using various technologies including cellular ones. A typical Smart Grid networking infrastructure showing possible infrastructure for generation, transmission, and distribution components of power grid is depicted in Fig. 2. Under this infrastructure, many applications could run simultaneously. In this work, we focus on three different applications that utilize this networking infrastructure at different levels as discussed below.

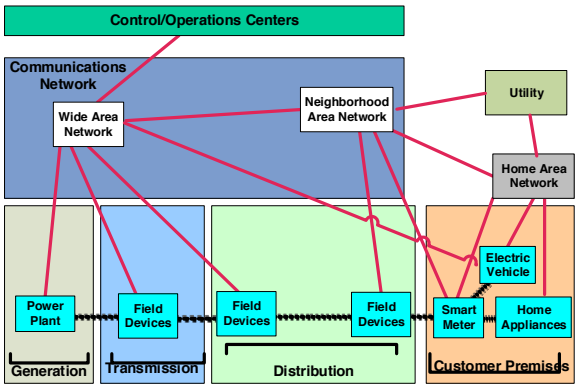

Fig. 2: Smart Grid multi-tier communication network [12]

B. Motivation for SDN-Enabled Smart Grid

Utilities and energy companies own and operate network components that are part of the Smart Grid communication infrastructure. In some cases, they also lease services from telecommunication companies or third party cloud services. In any case, the management of these networks is a great challenge due to the scale. Furthermore, due to devices and applications from different vendors, the equipments may not be interoperable. Therefore, the utilities will need to deal with equipment maintenance and software upgrade, which is costly and laborous. SDN is a promising solution for the aforementioned problems due to following advantages it presents:

- SDN adopts open standards and introduces technology abstraction, which provides a vendor-agnostic approach

to configuring and maintaining various types of network elements that are common in Smart Grid.

- Hardware virtualization through SDN eases the burden of managing different networks while using resources efficiently.
- Due to its holistic view of network, the SDN-based network provides superior control of delay and jitter in the network which is crucial for SCADA systems in terms of power and load state estimation and control.
- SDN's bandwidth-on-demand capabilities can also create opportunities to increase revenue through accelerated service velocity in cases where the utility also serves as a communication service provider in the coverage area. More and more utility companies are functioning as service providers in rural areas.

IV. Proposed SDN Deployment Scenarios in Smart Grid

A. SDN-enabled NANs

Smart Grid's NAN is mainly used for AMI applications. While there has been some wired options for building these communications, recent implementations solely targeted wireless solutions that depended on different standards such as IEEE 802.15.4g, IEEE 802.11s, RF-Mesh, and other proprietary mesh networks [12]. This in turn creates a wireless local network that can be used in a particular neighborhood. As long as different vendors' products support OpenFlow, a NAN using a mixture of these standards can be easily controlled and re-tasked through a standard network control script programming.

In most cases, Smart Grid operators prefer exchanging the information among different NANs in order to get a better load state estimation. Therefore, being able to control such a network in a centralized manner for load balancing, security and QoS services is very valuable. While SDN can provide this novelty, there are still challenges that would require some research to enable the use of SDN in wireless environments.

One of these challenges is the performance of the centralized control. As opposed to wired networking interface among the controller and SDN switches, this will not be the case in wireless-mesh based NANs due to the scalability of the AMI. Therefore, the control will be through wireless communication and most probably using multi-hopping (see Fig. 3). If the same channel is used for data communications, then this may create a lot of interference. While some of the very recent works investigated this issue for wireless mesh networks using [11], these works do not directly apply to AMI NANs where the scale is larger and the variety of nodes is significant in terms of used hardware/software. This suggests investigating the feasibility of distributed control in SDN-based NANs.

B. SDN-enabled SCADA

SCADA systems were designed to collect data from field devices such as PLCs, PMUs, IEDs at substations in real-time and do control decision at the control center in terms of reliability and quality of the power [2]. A substation contains hundreds of different IEDs, each generating and/or consuming information about the status of some aspect of the substation. A standard called IEC 61850 is also used for substation automation [2]. Currently, these systems are not only scalable, but also their sensing coverage is very limited. Proper configuration and maintenance of IED communication requires significant effort. The network complexity further increases with the uses of other protocols.

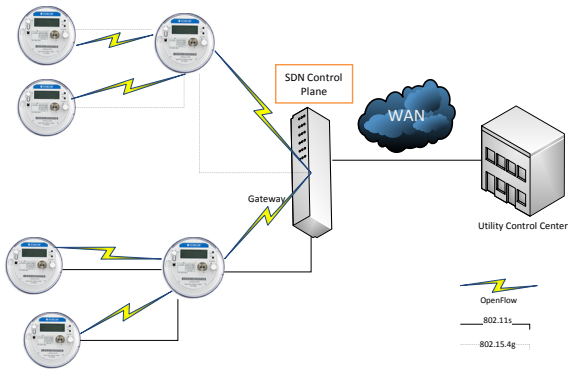

Fig. 3: Proposed SDN for Smart Grid NANs

However, with the modernization of the power grid, there will be opportunities to upgrade these systems based on a mix of wireless and wired infrastructure through the deployment of a large number of modern PMUs. For instance, the design and use of wireless PMUs have already begun [10]. One of the recent works proposed using these wireless PMUs within an SDN architecture so that the network administrator would have a global view of the power grid computer network, which makes it is easier to manage PMU telemetry traffic compared to a traditional IP network [7]. Again, this creates a perfect example of a local network within a substation that is supplemented by wireless communication.

There are also opportunities to reorganize the elements of these SCADA systems especially in terms of exploiting efficient ways to eliminate the complexities of multicasting and broadcasting. Massive amount of data is transmitted through these broadcasts or multicasts. Current architecture is a centralized one with hub-and-spoke model which is inadequate to address too many broadcasts or multicasts. Researchers strived to address this issue by using middleware approaches in the past [6]. The idea in these approaches are to implement publish and subscribe mechanisms where the data sources publish data and the brokers in the middleware (at the application layer) are responsible for delivering this data to subscribers within their QoS requirements. This is in a way a sort of group communications among publishers and subscribers. However, since this was implemented at the application layer, it is not only slower, but also not flexible in terms of hardware requirements. SDN can be used to redesign this middleware by including the control plane in the middleware, but at the network layer [20]. Another advantage of such an SDN-based control is the ability to perform traffic engineering, which cannot be done with layer-2 switches using spanning tree-based routing [1].

C. SDN-enabled Microgrid

A microgrid is a miniaturized version of power grid which can supply electrical load of small communities such as university campuses, malls, camps etc. It includes numerous Distributed Energy Resources (DERs) (e.g., photovoltaic systems, micro-combined heat and power systems (μCHP), and electric vehicles (EVs)), load, storage, and protection devices that are controlled by a central controller. Microgrids are becoming viable options for saving energy and generating clean power along with their reliable electrical services. For instance, Univ. of California San Diego setup a micro grid for its own campus which saved them $850K a month [17].

The major issue with these microgrids is the risk of rapid changes that may cause instability and eventually collapse in the system. Therefore, it is crucial to perform fine-grained real-time monitoring and control. This can only be achieved via reliable communications that can provide QoS in support of low data latency, packet prioritization and traffic engineering. These features can be supported via the SDN technology to stabilize and optimize system operation. Another opportunity for the use of SDN in microgrids is on the problem of DER management and aggregation. Basically, the DERs are grouped together for different purposes and any mobility related group changes will affect the system. Most of the DERs are expected to connect via a wireless link (e.g., EVs) which will create a local network consisting of wireless DERs and other wired IEDs connected with the microgrid. Currently, DER mobility and group management are done at the application layer. The complexity can be reduced by exploiting SDN capabilities that will be implemented at the network layer [20].

V. Security of SDN-Enabled Smart Grid

In this section, we discuss the security of the SDN-enabled smart grid. First, we articulate the threat model, then we list the desired security services for the SDN-enabled smart grid.

A. Threat Model

Conceptually, the threats to the SDN-enabled smart grid could be listed from four different complementary perspectives: (1) *Method-specific*; (2) *target-specific*; (3) *software-specific*; and (4) *identity-specific*.

Method-specific threats define how the threats are executed. The method-specific threats can be either passive or active. In the passive method, the attacker only monitors (or eavesdrops), records the communication data occurring in the SDN-enabled smart grid, and analyzes the collected data to gain meaningful information. In the active one, the attacker tries to send fake authentication messages, malformed packets, or replay a past communication to the components of the the SDN-enabled smart grid. As passive threats are surreptitious, it is harder to catch their existence. However, it is easier to catch the existence of an active attacker, but its damage to the smart grid can be relatively higher than the passive threats.

Target-specific threats classify the attacks according to which device the threats target. In an SDN-enabled smart grid, any device such as IEDs, PMUs, PLCs, Smart Meters could be valuable targets for potential malicious activities.

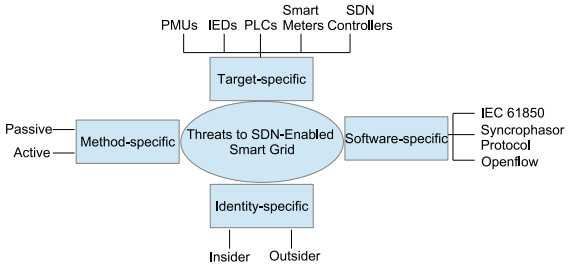

Fig. 4: A threat model for the SDN-enabled smart grid

In software-specific threats, the attackers aim to exploit the vulnerabilities associated with the networking protocols, software suits (IEC 61850, IEEE C37.118 Syncrophasor Protocol, Openflow of SDN) that run in the smart grid.

Finally, depending on the identity of the attacker, i.e., whether an attacker is a legitimate member of the network during an attack or not, she can be defined as insider or outsider attacker. Insiders are more dangerous than the outsiders as they have more knowledge about the internal architecture of the SDN-enabled smart grid.

In reality, there is no hard line between these attacking models and they complement each other because an insider could be a passive attacker trying to exploit IEC 61850 on an IED in the SDN-enabled smart grid. The threat model for the SDN-enabled smart grid is presented in Fig. 4.

B. Desired Security Mechanisms

Desired security mechanisms are usually defined by the national and international standardization bodies (e.g., National Institute of Standards and Technology, International Telecommunication Union (ITU)) and are used by many researchers and practitioners who aim to develop secure systems. In this sub-section, we use the security architecture suggested by the ITU's Recommendation X.800 [19] documentation, which is referred to as the Security Architecture for Open Systems Interconnect (OSI) as our guideline in addressing the threats discussed in the previous sub-section.

Confidentiality: Confidentiality refers to the protection of the exchanged content (e.g., gathered data, reports, commands) among the components of the smart grid such as IEDs, PMUs, PLCs, Smart Meters. A malicious entity which has the privilege to access the content, should not be able to decode the exchanged messages in the network. Confidentially also entails the protection against any unintended *information leakage* from the applications, controllers, and devices within the SDN-enabled smart grid. This is particularly important because the data generated and collected by the smart grid equipment, e.g., PMUs, IEDs are very periodic in its nature. Data forwarding policies or flow rules associated with the collected data may be discovered with simple timing or side-channel analysis. Similarly, an increased delay for the establishment of a new flow rule in response to an incoming packet can inform a potential attacker about the behavior of the OpenFlow controller within the SDN-enabled smart grid. This

unintended information disclosure from data plane devices, applications, flows, controllers should also be considered as part of any confidentiality service.

Traditionally, confidentiality can be provided by adopting either symmetric and asymmetric key-based encryption schemes [16]. In symmetric encryption, one key is utilized among the PMUs, PLCs, smart meters, IEDs, applications, flows, network controllers. Examples of symmetric encryption that can be utilized for the smart grid include AES, RC4. On the other hand, in asymmetric encryption, a pair of two keys (aka public and private) are utilized among the communicating components of the smart grid. RSA and ECC are the two most important examples of asymmetric encryption that could be deployed. Moreover, the maturing state-of-the art encryption mechanisms based on fully-homomorphic-encryption could be utilized for specifically preserving the privacy of the flows.

Authentication: Authentication involves guaranteeing the genuineness of the communication among the devices in the data plane, controllers, and the applications. An authentication mechanism verifies if the exchanged information stems from the legitimate participants of the SDN-enabled smart grid because a malicious entity (e.g., a compromised IED) may be able to inject counterfeit content or resend the same content into the SDN-enabled smart grid. More specifically, an adversarial smart grid application may attempt to insert new flow rules that may circumvent flow rules imposed by other applications [14]. Adversaries may also insert new rules to damage the system by influencing the state estimation, which is crucial to evaluate the demand.

Authentication can fundamentally be provided based on three factors [16]: (1) *Knowledge factor*: the proof of the knowledge of some secret (e.g., passwords) is provided to the authenticator. Symmetric, asymmetric key-based encryption schemes and hashing algorithms can all be utilized as part of the authentication mechanism with the knowledge factor. (2) *Possession factor*: authenticator verifies the claimant using the credentials provided by a specialized hardware. Electronic cards, smart cards, smart tokens physically owned by the claimant can be utilized and integrated with the SDN-enabled smart grid devices and applications. (3) *Identity factor*: the authenticator utilizes features uniquely identifying in the verification of the claimant. Both static or dynamic patterns that can identify the devices and applications can be utilized. For instance, behavioral information from the SDN-enabled smart grid devices and applications such as communication patterns, timing patterns, delays can all be utilized [9] as part of this authentication method. Within the SDN-enabled smart grid, all of these authentication techniques can be individually or a combination of one or more of the techniques could be adopted. If more than one factor is utilized, the authentication is called multi-factor authentication.

Integrity: Integrity refers to the capability to detect detect if the exchanged content between the communicating devices of the smart grid have been altered or not. Furthermore, the integrity service involves ensuring that the exchanged content is not deleted, replication of old data, counterfeit, or stale because the nature of the messages in the smart grid are very time-sensitive. Within the SDN-enabled smart grid, modification of the flow rules or insertion of new Openflow rules [8] by adversaries can cause severe damage to the healthy operations of the smart grid.

Integrity is usually provided by appending the cryptographic digest of the message content to the message itself [16]. When the PMUs, PLCs, smart meters, IEDs, applications, network controllers receive the message, they can check to see if the digest of the content matches the digest they computes on their end. If the digests match each other, then the message is deemed legitimate and not to have changed from its original content. Content digests in integrity are usually created with the usage of hashing algorithms. There are several hashing algorithms such (e.g., MD5, SHA-2) in use today, which do not require the presence of keys unless they are specifically designed to work with keys like keyed-hashing (e.g., HMAC, CMAC). Alternatively, integrity can be provided as part of a digital authentication mechanism utilizing symmetric and asymmetric encryption techniques. For instance, the last block of the encrypted data in AES can be appended to the message that would be sent as the integrity code. In a similar fashion, a private key in the asymmetric encryption techniques (e.g., RSA, ECC) can be used to provide the integrity code appended to the message.

Access Control: With access control, unauthorized use of a resource in the SDN-enabled smart grid is prevented. Access control addresses which participant of the smart grid reaches which content or service. For instance, IEDs should not be allowed to have the privileges of PMUs. Proper security measures must prevent any unauthorized SDN controller access. An unauthenticated application might try to access to resources for which it does not have exclusive privileges. Or, an authenticated application, IEDs, PMUs, PLCs, and Smart Meters may abuse its privileges.

Access control is usually achieved through four different methods [16]: (1) *discretionary access control (DAC)*; (2) *mandatory access control (MAC)*; (3) *role-based access control (RBAC)*; and (4) *attribute-based access control (ABAC)*. In DAC, access control decisions are made based on the exclusive rights that are set for the flows, applications, IEDs, PMUs, PLCs, and Smart Meters. An entity in DAC can enable another entity for accessing resources. In MAC, access control function considers the criticality of the resources and the rights of the flows, applications, IEDs, PMUs, PLCs, and Smart Meters on the resources. In MAC, an entity can not enable another entity for accessing the resources. In RBAC, access control decisions are based on the roles created within the the SDN-enabled smart grid. A role can include more than one entity e.g., the flows, IEDs. Moreover, a role defines the capabilities what the entities can do or not do within a certain role. Finally, in ABAC, the access control decisions are based on the features of the flows, applications, IEDs, PMUs, PLCs, and Smart Meters, resources to be accessed, and environmental conditions.

Availability: Due to the threats to SDN-enabled smart grid,

some portion of the grid or some of the functionalities or services provided by the grid could be damaged and unavailable to the participants of the grid. For instance, some PLCs could be compromised and they could cease functioning. A Denial-of-Service (DoS) type attack [13] can overflow the communication link of the SDN controller-switch [14]. SDN flow switch tables can be flooded by fake entries. In a similar fashion, a centralized SDN controller can be a single point of failure. Moreover, recent technological advances enabled the integration of the wireless technologies (e.g.,) into the smart grid infrastructure. In such cases, adversaries may jam the wireless medium, effectively hampering all the communications. Thus, availability service ensures that the necessary functionalities or the services provided by the SDN-enabled smart grid are always carried out, even in the case of attacks.

Usually, the smart grid includes redundant components in their infrastructure. This is to ensure the continuous operation during failures. In a similar fashion, the SDN-enabled smart grid can be designed with such redundancy to achieve the availability service.

Accountability: With accountability (aka non-repudiation [15]), the SDN-enabled smart grid ensures that a device or a software component (e.g., applications, IEDs, PMUs, PLCs, and Smart Meters) can not refute the reception of a message from the other device or application or the sent of a message to the other device or application in the communication.

Accountability can be provided as a service bundled inside authentication and integrity. For instance, a digital signature scheme (DSS) [15], which is based on utilizing encryption methods would address accountability. Additionally, proper auditing mechanisms and logs should be utilized to provide accountability in the SDN-enabled smart grid.

VI. Conclusion

In this work, we introduced how the emerging SDN paradigm could be considered as a viable technology for the Smart Grid communication architecture, which is currently under massive modernization effort by the utility providers. We discussed how flexibility and ease of control, management, security, and maintenance provided by the SDN technology could make a compelling case for applying SDN in three unique smart grid deployments that will mimic a wireless local network: Specifically, we focused on SCADA systems, AMI, and Microgrid Systems and discussed how an increasing number of smart grid devices that are being deployed to connect all the components of the Smart Grid together could benefit from the SDN. Furthermore, we articulated potential security threats that could arise in an SDN-enabled smart grid and provided some potential solutions to alleviate the threats.

Applying the maturing SDN technology into the smart grid infrastructure presents ample unique research challenges in security and networking to engineers and scientists and to the best of our knowledge this is the first work exploring those challenges. We would like to emphasize that the ideas mentioned here will be perfectly applicable to other wireless local networks. For instance, the experience in an SDN-based NANs can be adapted in a community wireless mesh network. In the same manner, vehicular ad hoc networks can also benefit from DER deployments in microgrids.

References

[1] Ian F. Akyildiz, Ahyoung Lee, Pu Wang, Min Luo, and Wu Chou. A roadmap for traffic engineering in sdn-openflow networks. *Comput. Netw.*, 71:1–30, October 2014.

[2] Kenneth C Budka, Jayant G Deshpande, Tewfik L Doumi, Mark Madden, and Tim Mew. Communication network architecture and design principles for smart grids. *Bell Labs Technical Journal*, 15(2):205–227, 2010.

[3] R. Hill N. Bessis C. Baker, A. Anjum and S. L. Kiani. Improving cloud datacenter scalability, agility and performance using openflow. 2012.

[4] P. F. Rosa F. de O. Silva, J. H. de S. Pereira and S. T. Kofuji. Enabling future internet architecture research and experimentation by using software defined networking. 2012.

[5] Qi Hao Fei Hu and Ke Bao. A survey on software-defined network and openflow: From concept to implementation. 2014.

[6] Harald Gjermundrod, David E Bakken, Carl H Hauser, and Anjan Bose. Gridstat: A flexible qos-managed data dissemination framework for the power grid. *Power Delivery, IEEE Transactions on*, 24(1):136–143, 2009.

[7] A. Goodney, S. Kumar, A. Ravi, and Y.H. Cho. Efficient pmu networking with software defined networks. In *Smart Grid Communications (SmartGridComm), 2013 IEEE International Conference on*, pages 378–383, Oct 2013.

[8] R. Kloti, V. Kotronis, and P. Smith. Openflow: A security analysis. In *Network Protocols (ICNP), 2013 21st IEEE International Conference on*, pages 1–6, Oct 2013.

[9] Wenyi Liu, A.S. Uluagac, and R. Beyah. Maca: A privacy-preserving multi-factor cloud authentication system utilizing big data. In *Computer Communications Workshops (INFOCOM WKSHPS), 2014 IEEE Conference on*, pages 518–523, April 2014.

[10] Brian Miller. Concept for next generation phasor measurement: A low-cost, self-contained, and wireless design. Master's thesis, University of Tennessee, 2010.

[11] V. Nascimento, M. Moraes, R. Gomes, B. Pinheiro, A. Abelem, V.C.M. Borges, K.V. Cardoso, and E. Cerqueira. Filling the gap between software defined networking and wireless mesh networks. In *Network and Service Management (CNSM), 2014 10th International Conference on*, pages 451–454, Nov 2014.

[12] Nico Saputro, Kemal Akkaya, and Suleyman Uludag. A survey of routing protocols for smart grid communications. *Computer Networks*, 56(11):2742 – 2771, 2012.

[13] L. Schehlmann, S. Abt, and H. Baier. Blessing or curse? revisiting security aspects of software-defined networking. In *Network and Service Management (CNSM), 2014 10th International Conference on*, pages 382–387, Nov 2014.

[14] S. Scott-Hayward, G. O'Callaghan, and S. Sezer. Sdn security: A survey. In *Future Networks and Services, 2013 IEEE SDN for*, pages 1–7, Nov 2013.

[15] William Stallings. *Cryptography and Network Security: Principles and Practices (3rd edition)*. Prentice Hall, 2003.

[16] William Stallings and Lawrie Brown. *Computer Security: Principles and Practice (3rd edition)*. Prentice Hall, 2015.

[17] Ucsd microgrid.

[18] K. Kannan V. Mann, A. Vishnoi and S. Kalyanaraman. Crossroads: Seamless vm mobility across data centers through software defined networking. 2012.

[19] ITU-T Recommendation X.800. Security architecture for open systems interconnection for ccitt applications. 1991.

[20] Jianchao Zhang, Boon-Chong Seet, Tek-Tjing Lie, and Chuan Heng Foh. Opportunities for software-defined networking in smart grid. In *Information, Communications and Signal Processing (ICICS) 2013 9th International Conference on*, pages 1–5, Dec 2013.