# Anomaly Detection in Smart Grids based on Software Defined Networks

Oliver Jung, Paul Smith, Julian Magin and Lenhard Reuter
*Center for Digital Safety and Security, Austrian Institute of Technology, Vienna, Austria*

Keywords: Smart Grid, Software Defined Networks, Network Security, Anomaly Detection, Information Theory.

Abstract: Software-defined networking (SDN) is a networking architecture that increasingly receives attention from power grid operators. The basic principle is the separation of the packet forwarding data plane and the central controller implemented in software that provides a programmable network control plane. SDN can provide various functions that facilitate the operation of smart grid communication networks, as it can support network management, quality of service (QoS) enforcement, network security, and network slicing. Due to periodical updates of the central controller, a real-time view of the network is available that allows for detecting attacks like e.g. denial-of-service (DoS) attack or network scanning. These kinds of attacks can be detected by applying anomaly detection mechanisms on the gathered information. In this position paper, we highlight the benefits SDN can bring to smart grids, address the implications of SDN on network security, and finally describe how information collected by a popular OpenFlow SDN controller can be used to detect attacks in smart grid communication networks.

## 1 INTRODUCTION

The power grid is currently subject to significant changes. It has to cope with an growing number of decentralized generation, an increasing number of electric vehicles, new business models like virtual power plants and local energy communities (MENDES et al., 2018) and the demand for energy- and cost-efficient system operation. Some of these challenges can only be coped with by introducing information and communication technology into all parts of the power grid to build the smart grid. The smart grid communication network thus has to support all different kinds of applications coming with specific requirements for e.g. quality of service (QoS) and Security.

To handle all these requirements grid operators originally introduced Multi Protocol Label Switching (MPLS) into their communication networks. However, due to the essential benefits provided that software-defined networking (SDN) for communication in smart grids they are currently considering to replace MPLS by SDN or to build an SDN overlay on top of MPLS.

SDN can provide features like network segmentation, fast failover, network monitoring required for smart grid communication infrastructures. The centralized SDN controller has a complete overview of the communication network status and thus monitoring can be be significantly simplified. This is not only important for identifying problems in smart grid network equipment, such as switches and routers, but also for security reasons. Gathered network traffic information are well suited for applying anomaly detection to identify different kinds of network misbehaviour. Operators are thus enabled to detect malfunctioning or misconfigured power grid devices, such as intelligent electronic devices (IED) or remote terminal units (RTU) and to detect malicious attacks.

The central SDN controller collects traffic flow information from all switches connected and thus has complete visibility of the network. It has been shown that anomaly detection can be successfully applied to traffic flows in order to identify different kinds of attack that can severely degrade smart grid availability.

This position paper addresses the benefits that software defined networking can offer to smart grid communication networks, in particular focusing on improved attack identification capabilities, by applying network-based anomaly detection to SDN flow information.

This paper is organized as follows. Section 2 will introduce related work. Section 3 deals with communication networks for smart grids while Section 4 addresses basic SDN functionalities, related security issues and the pros and cons for introducing SDN in



Jung, O., Smith, P., Magin, J. and Reuter, L.
Anomaly Detection in Smart Grids based on Software Defined Networks.
DOI: 10.5220/0007752501570164
In *Proceedings of the 8th International Conference on Smart Cities and Green ICT Systems (SMARTGREENS 2019)*, pages 157-164
ISBN: 978-989-758-373-5

smart grids. Section 5 describes how anomaly detection can actually be done in SDN and how our approach will be validated. Finally, Section 6 concludes our paper.

Table 1: List of acronyms.

| | |
|---|---|
| DDOS | Distributed denial-of-service |
| DOS | Denial-of-service |
| DS | Differentiated service |
| HAN | Home Area Network |
| ICMP | Internet Control Message Protocol |
| IED | Intelligent Electronic Device |
| MPLS | Multiprotocol Label Switching |
| NAN | Neighborhood Area Network |
| ONOS | Open Network Operating System |
| PCA | Principal Component Analysis |
| QoS | Quality of Service |
| RTU | Remote Terminal Unit |
| SCADA | Supervisory Control and Data Acquisition |
| SDECN | Software-defined Energy Communication Network |
| SDN | Software-defined Networking |
| VLAN | Virtual Local Area Network |
| WAN | Wide Area Network |

## 2 RELATED WORK

Software-defined networking (SDN) for smart grid communication has not only attracted attention from the research community but recently also from practitioners. One of the first analyses of this issue can be found in (Zhang et al., 2013). They highlight the SDN capabilities that make it ideally suited for the smart grid: a) ease of configuration and management, b) cross domain content-based networking, and c) virtualisation and isolation. They present three use cases to underline their position.

In (Cahn et al., 2013) the authors describe how communication within an electric substation can be improved. One of the challenges of conventional substation networks is the complex configuration of multicast groups for more than a hundred IEDs. The suggested software-defined energy communication network (SDECN) architecture can eliminate many substation network management issues by providing auto-configuration capabilities.

The authors of (Aydeger et al., 2016) explored how an SDN-enabled smart grid infrastructure can improve substations resilience with self-recovery by considering wireless communication links as failover solution. The approach was evaluated using a virtual Mininet-based test bed with the ns-3 network simulator.

It generally has been acknowledged that there are quite some security related issues around SDN. On one hand side, SDN can provide functionalities for improving network security by improved network visibility and ease of re-configuration. On the other hand, the controller constitutes a single point of failure that increases the attack surface due to complexity. The pros and cons around SDN security have been summarized by (Dacier et al., 2017).

An approach for improving smart grid resilience through SDN is presented in (Dong et al., 2015). The solution establishes communication links only when grid control commands are sent from the control centre to the grid devices. By doing so, the attacker has only limited time to inject bogus control commands.

Using traffic flow information for network monitoring is a recognized key benefit of SDN. However, anomaly detection in SDN has gained only limited attention. In (Braga et al., 2010) the authors suggest to use an artificial neural network method for DDoS attack detection based on SDN traffic flow features. Authors of (Mehdi et al., 2011) apply different anomaly detection mechanisms in an SDN. They evaluate the probability of successful connection attempts and use maximum entropy estimation of traffic features. However, the latter approach requires the examination of every packet and thus dismisses the benefits of SDN to some extent.

A comparison of OpenFlow and sFlow concerning flow retrieval for anomaly detection is provided by (Giotis et al., 2014). They claim that the number of flow table entries may grow in a way that it can impact the switching performance, in particular, in the case of DoS attacks. Thus, sFlow with sampling for data collection is used for detection purposes while OpenFlow is responsible for attack mitigation by dropping attack traffic.

Traffic features are mostly analysed separately in order to detect anomalies. To allow for anomaly detection across multiple traffic features or flows, authors in (Lakhina et al., 2005) apply the multiway subspace method after an initial entropy-based analysis.

In this paper, we propose to apply entropy-based anomaly detection to flow data that is collected by an OpenFlow controller in a smart grid. We expect to gain even better results as smart grid traffic is assumed to be uniformly distributed given that most data packets from sensor measurements are sent periodically and control commands are rather scarce under normal conditions.

## 3 SMART GRID COMMUNICATION

Smart Grids are a set of technologies that are used for remote control, monitoring, automation and digitalization of electrical power systems, including electricity distribution, demand and supply.

The electrical distribution grid is expected to accommodate more smart loads (e.g. controllable loads) and distributed energy generation devices, such as PV inverters, in the near future. Connecting more devices requires the communication network to be easily scalable, manageable and secure.

In general the aim of smart grid implementations is to optimize failure handling, grid control, costs, supply and demand, and increase the share of electricity from renewable energy sources. In order to meet these objectives, the communication infrastructure has to support extensive network monitoring to detect failures before they severely impact grid control, and maintain a high level of security and dependability.

Thus, utilities introduce Multi Protocol Label Switching (MPLS) in their communication backbones. The main reasons for this are the provisioning of virtual private networks and the traffic engineering capabilities. However, MPLS is not very flexible when it comes to new network services (Sydney et al., 2013).

In contrast, the programmable controller in software defined networks allows for the easy deployment of new network services, even during runtime. In SDN, different classes of smart grid network traffic can be isolated, e.g. to guarantee QoS. The software-based network control applications allow for arbitrary changes of switching devices. They add an additional layer of control over network traffic as it allows to prioritize or permit/block certain packet flows. SDN may thus outperform MPLS as a backbone communication technology.

The emergence of digital communication networks has also added to the evolution of Supervisory Control and Data Acquisition (SCADA) systems that are essential for power system network operation. Currently, a number of open international standards exist in the SCADA systems of utilities, such as the IEC 60870–5 and IEC 61850 series. While IEC 61850 is predominantly applied to intra-substation communication, IEC 60870–5-104 is used for telecontrol between control centres and substations (Yang et al., 2013).

The smart grid is expected to support a number of different functionalities that come with their specific performance requirements for the communication infrastructure. This infrastructure has to connect a vast number of geographically spread devices, such as Remote Terminal Units (RTUs) in substations, controllers of distributed energy resources, as well as bulk generation. In general, three categories of communication networks can be distinguished: Home Area Networks (HANs), Neighborhood Area Networks (NANs) and Wide Area Networks (WANs) (Kuzlu et al., 2014).

Wide area networks connect distributed NANs and HANs in different geographic locations. Real-time measurements from devices are transported from the substations to control centres through the wide area networks. Control messages are sent by the control centre to the substations using the WAN. For wide-area situational awareness, utilities require a lot of time-stamped and real-time measurement data from sensors in the power grid for monitoring, control, and protection (Wang et al., 2011). Thus, the WAN in the smart grid system should provide reliably high bandwidth and low latency.

Neighborhood Area Networks connect sensors on the distribution feeders and transformers, and IEDs carrying out control commands, distributed energy resources in the distribution grid, or smart meters at customer premises (Wang et al., 2011). These devices build the main source of information for the control centres to estimate the state of the distribution grid, and they are controlled by the control centre. The main requirement for applications in the customer premises, such as smart metering, is scalability. These applications are usually not sensitive to low bandwidth or high latency. In contrast applications in the field like e.g. SCADA for grid control require low latency and high reliability. Operators should thus be able to provide separated QoS classes to the different categories of applications using e.g. network slicing or virtualization, as provided by SDN.

Home area networks connect devices in the customer premises to support applications such as demand response or advanced metering. The HAN is usually not under the control of the utility. Communication with devices in the HAN is done via a home gateway or with the smart meter directly. The number of devices connected to the HAN is limited and there are no strict communication requirements compared to WAN and NAN.

## 4 SOFTWARE DEFINED NETWORKS

SDN is a network architecture where configuration and intelligence are provided by an SDN controller.

The separated data plane is a mere packet forwarding layer, implementing rules that are defined by a controller. The SDN controller enables programmability of network configuration using protocols like OpenFlow (Open Networking Foundation, 2012) to control flow tables that are maintained by switches and routers in the network. By relocating control functionalities to a software-based controller, SDN can provide a high degree of flexibility for implementing new networking solutions for Smart Grids.

Network switches and routers usually have packet routing and control algorithms included in the device firmware. However, the firmware is often not accessible with the consequence that the switch's functionality cannot be changed easily. In contrast, a software-based controller with numerous existing open-source implementations, such as OpenDaylight (Medved et al., 2014) or ONOS (Berde et al., 2014), can be changed and new functionality added.

Figure 1 shows the basic SDN concept and architecture. The southbound interface defines the instruction set of the forwarding devices or switches. Although there are other proprietary protocols, OpenFlow (Open Networking Foundation, 2012) is the most popular communication protocol to configure forwarding devices from the control plane. It is supported by numerous commercial-of-the-shelf switches.

The northbound interface is the API for network applications, denoted as *App* in Figure 1. Actual network control and operation is implemented in the network applications. They provide essential network services such as switching, routing, firewalls, load balancing or intrusion prevention. They interact with the data plane without having the need of dealing with each individual switch.

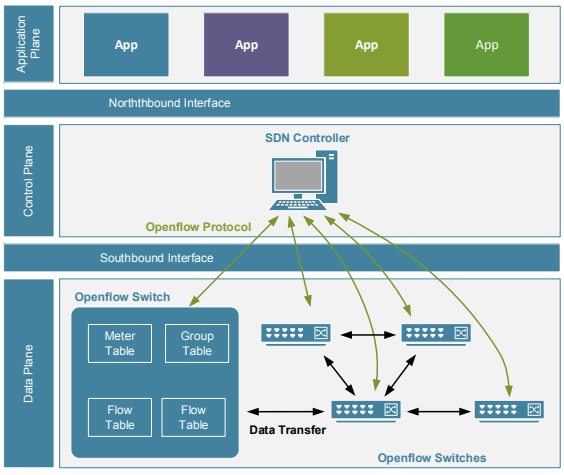


Figure 1: OpenFlow SDN conceptual architecture.

The OpenFlow switch maintains different tables. The most important ones are the flow tables. They define how packets are processed by the switch. The table consists of three parts: (i) match fields such as ingress port, destination and source IP address, or ICMP type for matching received packets; (ii) instructions that are executed for matched packets, like forwarding or dropping packets; (iii) and statistics regarding the matched packets. When a new packet is received, which has no matching entry in the flow table, it is forwarded to the controller for further processing. The controller processes the packet and prepares the flow entry that is implemented by the switch.

Group tables are a way to support more complex tasks that are not possible using flow table instructions. Using groups, complex actions or sets of actions can be executed. Each group can contain separate lists of actions, called OpenFlow buckets.

The meter tables contain per flow meter entries with the purpose of implementing QoS operations. They are used to monitor and control the rate of associated flows and can apply drop actions or change the differentiated services (DS) field of the IP packet.

## 4.1 SDN in Smart Grids

The main benefit of SDN in smart grids is the capability to dynamically configure network devices by manipulating data traffic flows, in order to improve QoS or system resilience by preventing and mitigating failures and attacks (Dong et al., 2015). In general, the key advantages of applying SDN in smart grids include (Rehmani et al., 2018):

- Isolation of traffic classes and applications: As described in Section 3, smart grid communication networks are divided into different categories, supporting applications with different demands concerning bandwidth, latency and reliability. SDN can establish virtual networks in order isolate applications (Kim et al., 2014).
- QoS enforcement: SDN introduces QoS mechanisms for giving higher priority to time critical measurements from different devices and control messages, e.g. from the control centre to the substation by link reservation (Dorsch et al., 2014)
- Resilience: Resilience of smart grid communication networks can be increased by fast re-routing and switchover from failing links. Mechanisms provided by SDN introduce lower latency in case of failover compared to classical routing mechanisms, as SDN mechanisms respond faster to network events (Dorsch et al., 2014).

- Network Visibility: The central SDN controller periodically requests status information from the connected SDN switches. Thus, it has full visibility of all flows in the network and is aware of the number of received packets and bytes, available bandwidth and links. Acquired flow statistics which provides a real-time view of the network state is accessible via open APIs and thus a convenient source of information for traffic monitoring applications (Ali et al., 2015).
- Security: Link isolation is a requirement for smart grid communication networks. IEC 62351-10 (International Electrotechnical Commission, 2012) defines security architecture guidelines for power systems and requires the implementation of separated security domains. Similarly, NIST IR 7628 (National Institute of Standards and Technology, 2014) asks for communications partitioning. Link isolation can moreover be used to enforce access control policies and to implement one-way communication where messages can only be sent from a trusted to an untrusted domain and not vice versa.

  Moreover, SDN traffic routing features can be used to block or redirect malicious traffic originating from DoS attacks or a network scan.

SDN can thus bring numerous advantages to smart grid communication networks. Utilities are currently evaluating in field trials the use of SDN in there process networks. In the following section, some of security aspects of SDN deployments are highlighted.

## 4.2 SDN and Network Security

The SDN paradigm can bring opportunities to enhance security of smart grid communication networks, offering new approaches for preventing, detecting and mitigating attacks. However, SDN also increases the attack surface and existing standards do not address issues of authentication and authorization.

The introduction of several network applications can significantly increases the system complexity (Dacier et al., 2017), making it harder to identify a specific application that is responsible for changing flow entries in a particular way. The SDN APIs can be used in order to implement elaborate security applications. Acquiring network statistics, isolating networks, leveraging active attack response is significantly simplified.

The drawback of the central controller is that acts as a single point of failure, which potentially reduces system resilience and is an attractive target for attackers. Attackers who are able to compromise the controller can gain full control over the network. Additionally, the controller is susceptible to denial-of-service-attacks using vast numbers of unknown flows and thus overloading the controller.

On the other hand, the centralized real-time situational awareness of the controller allows for detecting DoS attacks more reliably and to mitigate attacks by network re-configuration, meaning that packets that are identified as being part of an attack can be dropped or redirected to a security appliance (Scott-Hayward et al., 2016).

How data collection for security purposes can be gathered is described in the following section, using the OpenFlow SDN controller as an example.

## 4.3 Data Collection in OpenFlow

In order to gain situational awareness in the network, the SDN controller performs regular requests of flow statistics from the OpenFlow-capable SDN switches. In each request all flow table entries and included counter values are queried and downloaded to the controller. The popular ONOS controller requests by default every 5 seconds information about active flows using the `OFPMP_FLOW` message with the `OFPTT_ALL` option. SDN controllers commonly provide a REST API that allows easy access to flow entries in general and to flow statistics in particular. An anomaly detection application can make use of this API to interact with the controller.

The flow table counters are updated for each packet that corresponds to the match fields of the flow table. Match fields can include e.g. ingress port or packet headers fields. Moreover, the flow table holds an action field that defines how the matched packet should be processed, e.g. forwarding to a specified switch port, drop packet (empty instruction set), or modify a virtual LAN (VLAN) tag. Thus, the OpenFlow flow statistics is closely related to packet forwarding performed by the SDN switch. As a consequence, the switches acquire full flow information compared to conventional packet forwarding devices that aggregate packets into flows and export flow data using protocols like sFlow, NetFlow, and IPFIX where often packet sampling is applied in order to reduce effort for packet processing e.g. on backbone routers. As the central SDN controller is responsible for managing all the connected SDN switches, it can acquire a complete overview of the smart grid communication network knowing the flows of all switches.

Anomaly detection mechanisms can make use of the counters that are included in the flow table. The OpenFlow Switch Specification (Open Networking Foundation, 2012) defines optional as well as manda-

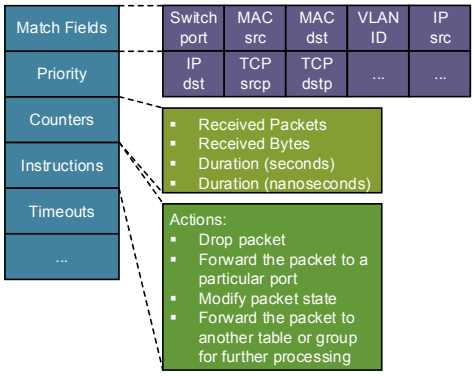


Figure 2: OpenFlow flow table.

tory per flow packet and byte counters. A duration counter maintains track of the time a flow entry exists in the flow table. The structure of the flow table is shown in Figure 2.

The per flow counters monitor the number of packets since the flow entry was installed in the flow table. For anomaly detection purposes, usually network traffic of a certain time interval is considered, e.g. a 5 seconds interval. Thus, the anomaly detection mechanism has to retain counter information until the end of the following interval.

# 5 ANOMALY DETECTION

Flow data is widely used source of information for detecting various types of security related incidents. This includes malicious events such as distributed denial-of-service (DDoS) attacks and network scans. Compared to packet-based analyses, anomaly detection solely on flow data usually results in more false positives and negatives because of the lower resolution of flow data.

Intrusion detection systems can be classified as signature-based and anomaly-based detection systems. The former is only able to detect known attacks by monitoring network traffic for known byte patters or traffic sequences. This leads to low false positives, incidents that are erroneously categorized as attacks, but unknown attacks can not be detected. Anomaly-based intrusion detection systems are able to detect these kind of attacks by identifying deviations from normal behaviour .

Most network traffic anomalies have in common that they change the distribution of IP packet header fields like source and destination addresses and ports. In the anomaly detection context these fields characterising the traffic behaviour are the traffic features. Obviously in case of the DoS, e.g. flooding attack it can be expected that the number of packets destined to the victim will rise and thus change the traffic feature distribution. Also a port scan will manifest in the feature distribution where a single host scans various destination IP addresses and ports from a single IP address and port.

There are numerous approaches for flow based anomaly detection (Sperotto et al., 2010). We will focus on entropy based anomaly detection in the following as an entropy based metric can effectively measure changes in the distribution of traffic features over time.

## 5.1 Entropy based Anomaly Detection

Entropy based anomaly detection approaches relying on network feature distributions have been proven successful for detecting different classes of attacks like DoS and ports scans. They have been applied in smart grid as well as in SDN environments (Giotis et al., 2014; Lakhina et al., 2005).

We propose to use Shannon Entropy to detect anomalies in the distribution of traffic feature such as source IP address, destination IP address, TCP source port and TCP destination port. Entropy can be used as a measure of the regularity of traffic features (Lee and Xiang, 2001). High entropy means a scattered feature distribution while low entropy values represent a converged distribution.

A DoS attack, where vast numbers of packets are destined to one destination IP address and destination port will significantly reduce entropy and can thus be detected as a drop in entropy. A network scan where whole network is scanned for existing IP addresses and open ports will manifest in a rise in entropy.

Depending on the number of existing flows, calculating entropy values for each feature can generate extensive data sets. Hence, in order to reduce the dimensionality of the data gathered Principal Component Analysis (PCA) is used in a second step to reduce data dimensions. That is a procedure form multivariate statistics and consists of a linear regression model. PCA can be considered as a pre-processing step for the classification phase. The aim is to set appropriate counter measurements to prevent intrusions and therefore provide more resilient network services (Lakhina et al., 2005).

## 5.2 Testbed Validation

Figure 3 shows the testbed that will be used to verify that entropy based anomaly detection can be successfully applied to SDN flow information in a smart grid communication network. We will integrate the anomaly detection application in a power grid ICT in-

frastructure which consists of a substation ring with SDN switches. Grid status information will be retrieved from the substation RTU using Modbus TCP. The SDN anomaly detection application is using flow information requested from the switches by the ONOS controller using the controller's REST API. Flow statistics has to be requested by the controller using OpenFlow `OFPTT_ALL` request. In order to prevent flow entries to expire before they have been collected by the controller the flow timeout has to be adjusted to the request rate.

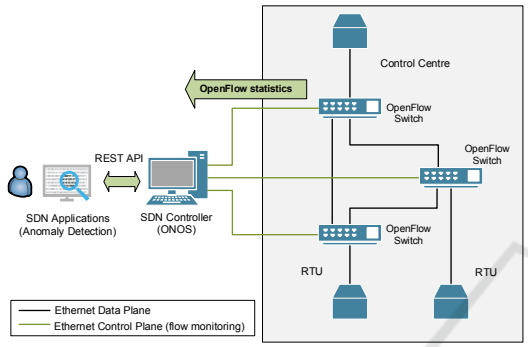


Figure 3: Anomaly Detection testbed.

For generating smart grid traffic we will use Raspberry Pis with OpenMuc. OpenMuc is a framework for implementing smart grid monitoring and control applications and supports the most important smart grid communication protocols (e.g. IEC 61850, IEC 60870-5-104, or Modbus). We will launch different kinds of attacks such as DoS, network scans, port scans against the smart grid nodes, and will mimic attacker activities through irregular activities like unplanned firmware updates and unusual connection attempts. The metrics for evaluating efficiency of the detection mechanism will be the ratio of false positives and false negatives.

In addition we will use traffic traces from real power grid that do not contain any attacks. We will inject attack traces into these traces in order evaluate the performance of the anomaly detection approach.

## 6 SUMMARY AND CONCLUSIONS

This paper has shown that SDN can bring numerous benefits to smart grid communication infrastructures. One of them is enhanced network visibility (situation awareness), in which traffic flows and associated statistics from switches are available at a centralized SDN controller. Due to the SDN conceptual architecture this features is inherently provided by SDN.

The SDN controller's APIs enable access to this information and can be used to support the implementation of a wide-variety applications that are useful for smart grid networks, including anomaly detection systems.

An anomaly detection mechanism that has been successfully applied to traffic flows is entropy-based anomaly detection. This form of detection system can identify attacks, such as DoS attacks or port scans, which can have a severe impact on smart grids or could be part of network reconnaissance for preparing an attack. As part of our ongoing research, we will implement and validate our approach to entropy-based detection on an SDN testbed, which consists of an ONOS SDN controller and Edgecore OpenFlow switches. To generate representative smart grid network traffic, a Raspberry Pi cluster has been developed that can, for example, be configured to represent RTUs. Finally, we will verify our assumptions using network traces from a real power grid.

As network re-configuration in SDN can be done easily we will investigate ways to mitigate attacks by e.g. dropping all packets that are part of the DoS attack or limiting the number of packets to a rate where they have no impact on the smart grid.

## ACKNOWLEDGEMENTS

The presented work is conducted in the research project VirtueGrid, which is funded by the Austrian Climate and Energy Fund (KLIEN, ref. 858873) within the program e!MISSION (eCall 9096736).

## REFERENCES

Ali, S. T., Sivaraman, V., Radford, A., and Jha, S. (2015). A Survey of Securing Networks Using Software Defined Networking. *IEEE Transactions on Reliability*, 64(3):1086–1097.

Aydeger, A., Akkaya, K., Cintuglu, M. H., Uluagac, A. S., and Mohammed, O. (2016). Software defined networking for resilient communications in Smart Grid active distribution networks. pages 1–6. IEEE.

Berde, P., Snow, W., Parulkar, G., Gerola, M., Hart, J., Higuchi, Y., Kobayashi, M., Koide, T., Lantz, B., O'Connor, B., and Radoslavov, P. (2014). ONOS: towards an open, distributed SDN OS. In *Proceedings of the third workshop on Hot topics in software defined networking - HotSDN '14*, pages 1–6, Chicago, Illinois, USA. ACM Press.

Braga, R., Mota, E., and Passito, A. (2010). Lightweight DDoS flooding attack detection using NOX/OpenFlow. In *IEEE Local Computer*

*Network Conference*, pages 408–415, Denver, CO, USA. IEEE.

Cahn, A., Hoyos, J., Hulse, M., and Keller, E. (2013). Software-defined energy communication networks: From substation automation to future smart grids. pages 558–563. IEEE.

Dacier, M. C., Konig, H., Cwalinski, R., Kargl, F., and Dietrich, S. (2017). Security Challenges and Opportunities of Software-Defined Networking. *IEEE Security & Privacy*, 15(2):96–100.

Dong, X., Lin, H., Tan, R., Iyer, R. K., and Kalbarczyk, Z. (2015). Software-Defined Networking for Smart Grid Resilience: Opportunities and Challenges. In *Proceedings of the 1st ACM Workshop on Cyber-Physical System Security - CPSS '15*, pages 61–68, Singapore, Republic of Singapore. ACM Press.

Dorsch, N., Kurtz, F., Georg, H., Hagerling, C., and Wietfeld, C. (2014). Software-defined networking for Smart Grid communications: Applications, challenges and advantages. pages 422–427. IEEE.

Giotis, K., Argyropoulos, C., Androulidakis, G., Kalogeras, D., and Maglaris, V. (2014). Combining OpenFlow and sFlow for an effective and scalable anomaly detection and mitigation mechanism on SDN environments. *Computer Networks*, 62:122–136.

International Electrotechnical Commission (2012). IEC TR 62351-10: Power systems management and associated information exchange - Data and communications security - Part 10: Security architecture guidelines.

Kim, Y.-J., He, K., Thottan, M., and Deshpande, J. G. (2014). Virtualized and self-configurable utility communications enabled by software-defined networks. In *2014 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pages 416–421, Venice, Italy. IEEE.

Kuzlu, M., Pipattanasomporn, M., and Rahman, S. (2014). Communication network requirements for major smart grid applications in HAN, NAN and WAN. *Computer Networks*, 67:74–88.

Lakhina, A., Crovella, M., and Diot, C. (2005). Mining anomalies using traffic feature distributions. In *Proceedings of the 2005 conference on Applications, technologies, architectures, and protocols for computer communications - SIGCOMM '05*, page 217, Philadelphia, Pennsylvania, USA. ACM Press.

Lee, W. and Xiang, D. (2001). Information-theoretic measures for anomaly detection. In *Proceedings of the 2001 IEEE Symposium on Security and Privacy*, SP '01, pages 130–, Washington, DC, USA. IEEE Computer Society.

Medved, J., Varga, R., Tkacik, A., and Gray, K. (2014). OpenDaylight: Towards a Model-Driven SDN Controller architecture. In *Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014*, pages 1–6.

Mehdi, S. A., Khalid, J., and Khayam, S. A. (2011). Revisiting Traffic Anomaly Detection Using Software Defined Networking. In Sommer, R., Balzarotti, D., and Maier, G., editors, *Recent Advances in Intrusion Detection*, volume 6961, pages 161–180. Springer Berlin Heidelberg, Berlin, Heidelberg.

MENDES, G., NYLUND, J., and ANNALA, S. (2018). Local energy markets: Opportunities, benefits, and barriers. Ljubljana.

National Institute of Standards and Technology (2014). Guidelines for Smart Grid Cybersecurity. Technical Report NIST Internal or Interagency Report (NISTIR) 7628 Rev. 1, National Institute of Standards and Technology.

Open Networking Foundation (2012). OpenFlow Switch Specification 1.3.0.

Rehmani, M. H., Davy, A., Jennings, B., and Assi, C. (2018). Software Defined Networks based Smart Grid Communication: A Comprehensive Survey. *arXiv:1801.04613 [cs]*. arXiv: 1801.04613.

Scott-Hayward, S., Natarajan, S., and Sezer, S. (2016). A Survey of Security in Software Defined Networks. *IEEE Communications Surveys & Tutorials*, 18(1):623–654.

Sperotto, A., Schaffrath, G., Sadre, R., Morariu, C., Pras, A., and Stiller, B. (2010). An Overview of IP Flow-Based Intrusion Detection. *IEEE Communications Surveys & Tutorials*, 12(3):343–356.

Sydney, A., Nutaro, J., Scoglio, C., Gruenbacher, D., and Schulz, N. (2013). Simulative Comparison of Multiprotocol Label Switching and OpenFlow Network Technologies for Transmission Operations. *IEEE Transactions on Smart Grid*, 4(2):763–770.

Wang, W., Xu, Y., and Khanna, M. (2011). A survey on the communication architectures in smart grid. *Computer Networks*, 55(15):3604–3629.

Yang, Y., McLaughlin, K., Littler, T., Sezer, S., Pranggono, B., and Wang, H. F. (2013). Intrusion Detection System for IEC 60870-5-104 based SCADA networks. In *2013 IEEE Power & Energy Society General Meeting*, pages 1–5, Vancouver, BC. IEEE.

Zhang, J., Seet, B.-C., Lie, T.-T., and Foh, C. H. (2013). Opportunities for Software-Defined Networking in Smart Grid. In *2013 9th International Conference on Information, Communications Signal Processing*, pages 1–5.