

Network Virtualization System for Smart Grid Data Acquisition System

Seonyong Jeong*, Yongjae Lee[†], Seungwon Shin[†]

*Graduate School of Information Security, KAIST, Daejeon, South Korea

[†]School of Electrical Engineering, KAIST, Daejeon, South Korea
s.jeong@kaist.ac.kr, ylee.cs@kaist.ac.kr, claude@kaist.ac.kr

Abstract—The smart grid is an intelligent electrical grid system which can enable an interaction between consumer and producer by adapting information technology on power planting, electric power transmission, and power consumption. In this system, consumers and producers can exchange information about the use of electricity in real time. By using this advantage, the consumers can notice the time which has low charges and adjusting the power consumption. Also, the producer can operate electric power supply elastically by supplying the electricity adjusting to the power demand. To achieve this, the smart grid system consists of not only traditional electrical components such as power plant, substation, electrical meter, but also all devices which consume electrical power including TV, refrigerator, IoT devices. As the number of devices grows and the network becomes more complex, the number of packet types in the smart grid system has grown up. Also, the types of data traffic become more varied than before. For example, critical command traffics, use of electricity from the home remote terminal, a large number of sensing data from the IoT devices can be exchanged by the network. However, not all the packet type has the same properties and requirements. In traditional network infrastructure, the administrator should set up a new physical network infrastructure to offer the different network requirements for each type. In this study, we show some benefits of network slicing which can offer different properties corresponding to the type of packets and its importance.

Index Terms—Smart grid, Network Slicing, Network Virtualization

I. INTRODUCTION

The smart grid is an innovative system which can manage and control the modern electrical grid system. The system applies novel information and communication technology to the traditional electrical grid, so the consumers and producers of electricity can exchange data related to power consumption on the fly. This real time interaction enables efficient resource utilization such as optimizing power provisioning according to the power demand and flexible scheduling of energy consumption [1]. To make this two-way communication available, the smart grid should consist of not only traditional electrical facilities such as power plants, power substations, household meters, but also various kinds of Intelligent Electrical Devices (IEDs) including smart meters, smart plugs, and Internet of Things (IoT) devices.

As the number of devices in the smart grid system grows, the number of services in the smart grid system becomes greater than before. The smart grid system gathers the sensing data from the remote sensors, operates the electric devices consisting of the system, and handles the various kinds of fault

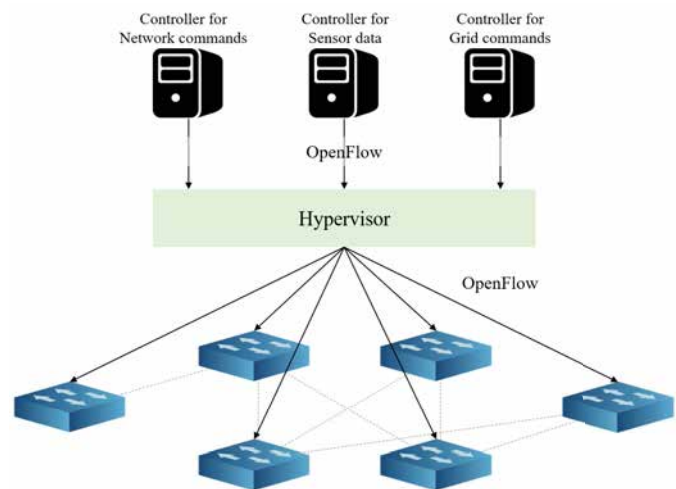


Fig. 1. Network virtualization for the smart grid

from the system. Each service has its own service properties and requirements such as priority, authority, and required bandwidth, and it is necessary to satisfy such requirements for the services in a flexible way.

In the legacy electrical grid system based on the traditional network infrastructure, the administrator should construct some separate networks to support differential properties for each service. However, in the smart grid system, it is virtually impossible to separate networks for each service because there are too many services for the administrator to manage, considering the different levels of QoS and security requirements of such services. Furthermore, it is hard to handle different types of traffic elastically with the traditional network infrastructure where routing equipments do not have functionalities that enable flexible traffic routing.

Recently, Software Defined Networking (SDN) has been proposed and shown its potential for resolving problems that have been raised in the conventional network environment. It is a new networking paradigm which pursues dynamic and flexible networking management, emphasizing the role of software in both the control plane and the data plane. SDN enables a network system administrator to control the network system elastically by defining and installing network management rules on the fly, which is hard to implement in the hardware-centric conventional networking system.

In this work, we explore the potential of SDN to resolve challenges that we face when we design and build a smart grid system, and propose a novel smart grid system built upon the SDN technologies. In Figure 1, we illustrate the proposed system for the smart grid system where the administrator can deploy a number of applications that are in charge of controlling various services such as sensor data collection, smart grid network management, and electricity production and consumption monitoring. By deploying separate applications to achieve their goal, the administrator only needs to focus on each application, and their individual networking requirements are mediated by the hypervisor. So, the proposed system provides the virtually separated networks without any additional network constituents by locating the hypervisor between the control plane (i.e., applications) and the data plane (i.e., switches).

II. RELATED WORK AND BACKGROUND

Several studies have shown that the network virtualization by Software Defined Networking (SDN) can slice the existing network and offer an isolated slice to separate services. Sherwood et al. introduced FlowVisor which can slice the physical network hardware resources virtually and isolate the sliced network [2]. Blenk et al. systemized existing SDN network hypervisors [3]. They surveyed not only general purpose hypervisors such as FlowVisor [2], Veritago [4], AdVisor [5], but also investigated network hypervisors with a special purpose, including CellVisor [6], RadioVisor [7] and MobileVisor [8]. However, there is little information available on applying the network virtualization specialized to the smart grid network. Dong et al. suggested some possibilities and challenges of SDN on the smart grid network [10]. They reported some strength of network virtualization on the smart grid, but they only discussed the finer-grained monitoring by leveraging it. In this study, we focus on the advantages of network virtualization and present the advantages of it. This study may lead to a better understanding of the benefits on the network virtualization to the smart grid network.

A. FlowVisor

FlowVisor is the first network hypervisor that leverages the flexibility of the SDN controller. This hypervisor is located between the tenant network controller and the physical data planes. It provides various network resource isolation functionalities such as bandwidth isolation and topology isolation by modifying control messages and checking the header of flowing packets based on the administrator's policy. In this section, we will present how FlowVisor works.

1) *Topology Isolation*: FlowVisor offers the topology isolation by utilizing a proxy between the physical devices and network slice controllers. The hypervisor edits the OpenFlow messages to report only network devices to the network controller which corresponds to the network slice [9]. By reporting the modified configuration network, the hypervisor can deceive the network controller into thinking there are only

selected network facilities. In addition, FlowVisor instance can be run on the other instance of the FlowVisor.

2) *Network Resource Isolation*: FlowVisor offers the Network Resource Isolation by using a number of distinct priority queues. By mapping the packets from a specific network slice to a prescribed Virtual Local Area Network Priority Code Point, they can offer the different priorities corresponds to the type of packets. However, this does not guarantee the fixed bandwidth. So in Enhanced FlowVisor, the hypervisor checks the link capacity and if the link capacity is not enough, they declined the request of virtual network allocation [14].

III. ADVANTAGES

Unlike the traditional grid system, a smart grid consists of traditional electrical facilities as well as smart devices which enable gathering and monitoring data and operating devices remotely. As the number of intelligent devices installed in the smart grid increases, and this prompts an increase in the amount of data and complexifying the network infrastructure [11]. By leveraging network hypervisor, an administrator can offer isolated network slice to each services without additional setting and can manage the complicated network easily. In this paper, we present some advantages of network virtualization in the smart grid system and how this technology can be utilized to simplify the complicated network.

A. Differential QoS

A network hypervisor can provide different level of Quality of Service (QoS) for each priority of service. There are various network services in the smart grid network and each of them has a different priority. For example, the importance of a caution packet of electric power leakage is not the same as that of an electricity usage packet. In case of sending a caution packet, the system must guarantee the successful transmission in any situation so that the engineer can recover the defective part soon. On the other hand, it is not a crucial problem to lose electricity usage packets. The usage packet also contains information about the cumulative electricity usage, so the system can recover the lost packet by checking the cumulative data.

Figure 2 presents a method of providing distinct service quality by applying overlay hypervisor to the smart grid network. The network hypervisor is located between the forwarding plane and controllers of each service and sets the forwarding rules to each switch by aggregating the OpenFlow messages from the controllers [9]. They can offer some virtually isolated network slice on the physical network without setting up the extra network facilities.

This advantage has a strength to handle the unexpected network packet increment. Brodsy et al. reported a denial-of-service (DoS) attack on wireless sensor network which can be included in the smart grid [12]. Even if a sudden network traffic flooding by a DoS attack occurs, the system should guarantee the transmission of caution packets although the usage packet is dropped. By leveraging the network virtualization technology, the hypervisor can assure the delivery of

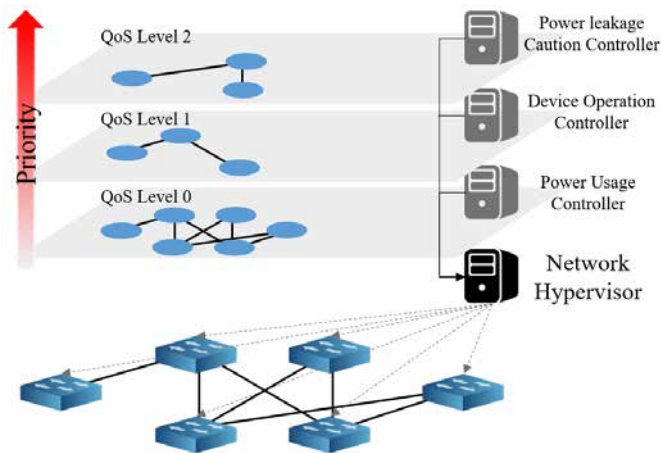


Fig. 2. Differential QoS by leveraging network hypervisor

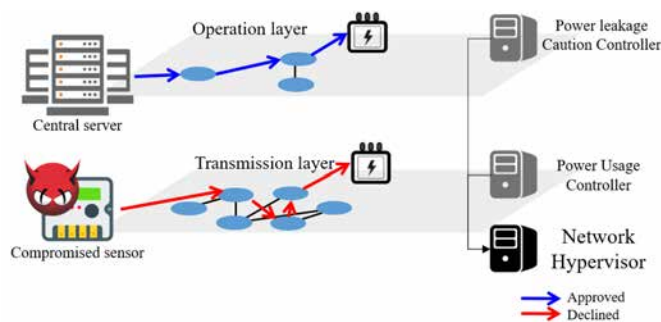


Fig. 3. Packet approval based on the network slice authority

high priority packets by dropping lower priority packets or rerouting the delivery path to not heavy loaded traffic routes. So, we can guarantee the differential QoS corresponds to the importance of data type.

B. Authority Management

Modern smart grid system includes various types of external system. For instance, the system has diverse types of sensors to gather a large amount of power data. Also, for the remote operation, a lot of actuators are installed in the smart grid system. These various interconnected devices enrich the smart grid system, but most of these external devices are not reliable.

Figure 3 shows two scenarios of packet approval and dropping based on the network slice's authority. In general, only authorized users such as a central server can send operational messages. However, an attacker can compromise a terminal unit and send some critical operational messages by disguising as an authorized user. Goodspeed et al. identified attack vectors for wireless devices used in advanced metering infrastructure [13]. They documented how an attacker extracts critical information including authentication from the devices. If the attacker takes the authentication and sends a shutdown message to a critical infrastructure such as transforming station.

To prevent this, the administrator can slice the network by using the network hypervisor and separate devices into

each layer following the devices' rules. In addition, he can also assign some authorities to each isolated network slice. For example, the operation layer only includes the authorized nodes such as a central server, and the transforming station only accepts the operation message from the operation layer. In contrast, a malicious node which is not authorized by the smart grid administrator cannot join the operation layer. So, the node can only send the operation message via the transmission layer, and the transforming station can deny the operation message. By slicing operable network slice and non-operable network slice, we can make only a control packet from operable slice be approved.

IV. CONCLUSION

As the smart grid network becomes more complicated, the importance of network management becomes greater than before. In this study, we showed some advantages of network virtualization applied to the smart grid network. However, there is a severe overhead on the existing network hypervisors for a general network. Our final goal is developing a network hypervisor optimized for the smart grid network. As future work, we will study the requirements for the effective smart grid network to optimize the hypervisor for the system.

ACKNOWLEDGEMENTS

This research was supported by Korea Electric Power Corporation. (Grant number:R18XA05)

REFERENCES

- [1] Y. Wu, V. K. N. Lau, D. H. K. Tsang, L. P. Qian and L. Meng, "Optimal Energy Scheduling for Residential Smart Grid With Centralized Renewable Energy Source," in *IEEE Systems Journal*, vol. 8, no. 2, pp. 562-576, June 2014. doi: 10.1109/JSYST.2013.2261001
- [2] Rob Sherwood, Glen Gibb, Kok-Kiong Yap, Guido Appenzeller, Martin Casado, Nick McKeown, Guru Parulkar (2009). FlowVisor: A Network Virtualization Layer.
- [3] A. Blenk, A. Basta, M. Reisslein and W. Kellerer, "Survey on Network Virtualization Hypervisors for Software Defined Networking," in *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 655-685, Firstquarter 2016. doi: 10.1109/COMST.2015.2489183
- [4] R. D. Corin, M. Gerola, R. Riggio, F. De Pellegrini, and E. Salvadori, "VERTIGO: Network virtualization and beyond," in *Proc. EWSDN*, 2012, pp. 24-29
- [5] E. Salvadori, R. D. Corin, A. Broglio, and M. Gerola, "Generalizing virtual network topologies in OpenFlow-based networks," in *Proc. IEEE GLOBECOM*, Dec. 2011, pp. 1-6.
- [6] L. Li, Z. Mao, and J. Rexford, "CellSDN: Software-defined cellular networks," Princeton Univ., Princeton, NJ, USA, *Comput. Sci. Tech. Rep.*, 2012
- [7] S. Katti and L. Li, "RadioVisor: A slicing plane for radio access networks," in *Proc. USENIX ONS*, 2014, pp. 237-238.
- [8] V. G. Nguyen and Y. H. Kim, "Slicing the next mobile packet core network," in *Proc. ISWCS*, 2014, pp. 901-904.
- [9] Nick McKeown, Tom Anderson, Hari Balakrishnan, Guru Parulkar, Larry Peterson, Jennifer Rexford, Scott Shenker, Jonathan Turner, "OpenFlow: Enabling Innovation in Campus Networks", CCR 2008
- [10] Xinshu Dong, Hui Lin, Rui Tan, Ravishankar K. Iyer, and Zbigniew Kalbarczyk. 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)*. ACM, New York, NY, USA, 61-68. DOI=http://dx.doi.org/10.1145/2732198.2732203
- [11] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A Survey on Smart Grid Communication Infrastructures: Motivations, Requirements and Challenges," *IEEE Communications Surveys Tutorials*, vol. 15, no. 1, pp. 5-20, 2013.

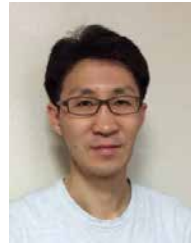
- [12] J. Brodsky, A. McConnell, "Jamming and Interference Induced Denial-of-Service Attacks on IEEE 802.15.4-Based Wireless Networks", Proceedings of the SCADA Security Scientific Symposium 2009 (S4), pp. 2-12-11, January 21-22, 2009.
- [13] T. Goodspeed, D. R. Highfill, B.A. Singletary, "Low-level Design Vulnerabilities in Wireless Control Systems Hardware", Proceedings of the SCADA Security Scientific Symposium 2009 (S4), pp. 3-13-26, January 21-22, 2009.
- [14] S. Min, S. Kim, J. Lee, and B. Kim, "Implementation of an Open-Flow network virtualization for multi-controller environment," in Proc. ICACTION, 2012, pp. 589-592



Seonyong Jeong received the B.S. degree in the School of Electronic Engineering from Kyungpook National University, Daegu, Republic of Korea in 2018. He is currently in his Master's degree in the Graduate School of Information Security at KAIST, Daejeon, Republic of Korea. His research interests include sensor network security, smart grid security.



Yongjae Lee received the Ph.D. degree in computer science from the School of Computing, KAIST in 2018. He received B.S. degree in computer science and engineering in 2008 from Chung-ang University and M.S. degree in 2010 from KAIST. He is currently a postdoctoral researcher at KAIST. His research interests include system and network security.



Seungwon Shin received the Ph.D. degree in computer engineering from the Electrical and Computer Engineering Department, Texas A&M University. He received his M.S degree and B.S degree in electrical and computer engineering from KAIST. He is currently an Associate Professor in the School of Electrical Engineering at KAIST. He has conducted several SDN security projects to make SDN environments more secure (e.g., FRESCO, FortNOX, and Avant-Guard) and their outputs have been published at top-tier networking/security conferences, such as

ACM CCS, NDSS, and SIGCOMM-HotSDN.