Chapter 4
Securing SDN-Enabled Smart Power Grids:
SDN-Enabled Smart Grid Security

Uttam Ghosh
Tennessee State University, USA

Pushpita Chatterjee
Old Dominion University, USA

Sachin Shetty
Old Dominion University, USA

ABSTRACT

Software-defined networking (SDN) provides flexibility in controlling, managing, and dynamically reconfiguring the distributed heterogeneous smart grid networks. Considerably less attention has been received to provide security in SDN-enabled smart grids. Centralized SDN controller protects smart grid networks against outside attacks only. Furthermore, centralized SDN controller suffers from a single point of compromise and failure which is detrimental to security and reliability. This chapter presents a framework with multiple SDN controllers and security controllers that provides a secure and robust smart grid architecture. The proposed framework deploys a local IDS to provide security in a substation. Whereas a global IDS is deployed to provide security in control center and overall smart grid network, it further verifies the consequences of control-commands issued by SDN controller and SCADA master. Performance comparison and simulation result show that the proposed framework is efficient as compared to existing security frameworks for SDN-enabled smart grids.

DOI: 10.4018/978-1-5225-5510-0.ch004

INTRODUCTION

Smart grid is a large-scale heterogeneous complex networking between a several number of sensors, actuators, smart meters, supervisory control and data acquisition (SCADA) systems, and also end-user devices and appliances located on residential and commercial premises in order to facilitate the generation, transmission and distribution of power. The communication infrastructure must be scalable, reliable, secure and efficient to sustain the transmission of a massive amount of real-time data generated by the deployed sensors in smart grid. Software defined networking (SDN) can be integrated in smart grid to achieve such communication infrastructure. It allows to manage and verify the correctness of network operations at run time. The globalized view of the SDN controller allows fault (due to accidental failures and malicious attacks) detection, isolation of affected components, and remediates of abnormal operation in the SDN-enabled smart grid networks more efficiently as compared to legacy based networks.

The proliferation of the smart grid technologies brings the promise of an era of easy and optimal use of power delivery systems as well as intelligence and efficiency. Recently, a number of research papers have been proposed in the literature (A.Goodney, Kumar, Ravi, & Cho, 2013) (Aydeger, Akkaya, & Uluagac, 2015) (Dorsch, Kurtz, Georg, Hagerling, & Wietfeld, 2014) (Ghosh, Dong, Tan, Kalbarczyk, Yau, & Iyer, 2016) (K. Akkaya, 2015; J. Zhao, 2016) (D. Gyllstrom, 2014) to introduce the concept of SDN in smart grid networks. Most of these proposals mainly focus on (i) the advantages and potential risks of using SDN in smart grid and (ii) investigation how SDN can fulfill communication requirements of smart grid communication networks regarding properties like quality of service (QoS), latency and link failover time (recovery time from a link failure). However, considerably less attention has been given to provide security in SDN-enabled smart grid networks (Cahn, Hoyos, Hulse, & Keller, 2013) (Dong, Lin, Tan, Iyer, & Kalbarczyk) (Dorsch, Kurtz, Georg, Hagerling, & Wietfeld, 2014). Most of the researchers assume that SCADA master, SDN controller and their applications are non-compromised. They further consider that SDN can offer security in smart grid by providing consistent access control, applying efficient and effective security policies, and managing and controlling the network centrally. Their main focus on protecting the smart grid networks against various forms of outsider attacks and providing security assurance within the cyber (or SDN) domain only. They significantly overlook the insider attacks that may harm the smart grid system as a whole (Zhang, Wang, Sun, II, & Alam, 2011). It further suffers from possible reliability and security issues due to use of a centralized SDN controller.

This Chapter propose a security framework with multiple SDN controllers and intrusion detection systems (IDS) to provide a secure and robust smart grid architecture. A light- weight identity based cryptography (Akkaya, 2015) has been used to protect the smart grid network from outside attacks. A local IDS is deployed in a substation to collect the measurement data periodically and to monitor the control-commands that are executed on SCADA slaves. Whereas a global IDS runs at control center and collects the measurement data from the substations and estimates the state of the smart grid system by utilizing the theory of differential evolution (Akkaya, Uluagac, & Aydeger, 2015). It further verifies the consequences of control-commands issued by either SDN controller or SCADA master. The global IDS generates an alarm and notifies to the intrusion elimination system (IES) if it detects unsteady state of smart grids.