Modeling a Cyber Resilient Smart Grid using Software Defined Networks

Hellen Maziku
Tennessee State University
Nashville, TN
hmaziku@my.tnstate.edu

David M. Nicol
formation Trust Institute
Univ. of Illinois at Urbana-Champaign
dmnicol@illinois.edu

CCS Concepts

•**Security and privacy → Distributed systems security; Denial-of-service attacks;**

Keywords

Cyber Resilience; Smart Grid; SDN; Security Metrics; OpenFlow

1. INTRODUCTION

The increasing dependence on energy across all domains from datacenters to households suggests that power systems must operate 24/7 with high reliability and high availability. Real time emergency response capability in power systems is mandatory and message data has an upper-bound of 4 ms latency tolerance. Traditionally, all communication between devices inside and outside of power substations has been implemented using copper wires and legacy communication protocols [2]. More recently as illustrated in Fig. 1, a modern smart grid has been introduced which enables two-way flow of energy from power to plug to be automated, monitored and controlled [3]. Intelligent Electronic Devices (IEDs) are used to monitor the state of the electricity infrastructure.

Integrating IP-based communications in the smart grid while increases compatibility between different vendors' components, it also increases the likelihood of successful IP-based network attacks, such as IP spoofing and DoS attacks.

The present challenge is enabling the smart grid communication network become cyber resilient. A cyber resilient smart grid should be able to reduce the impact of cyber incidents and provide the ability to operate in the face of persistent attack. By 2020, DOE's vision is to see that resilient energy delivery systems are designed, installed, operated, and maintained [1]. It is therefore imperative to explore cyber resilient models for the smart grid.

2. RELATED WORK

DOI: 10.1145/1235

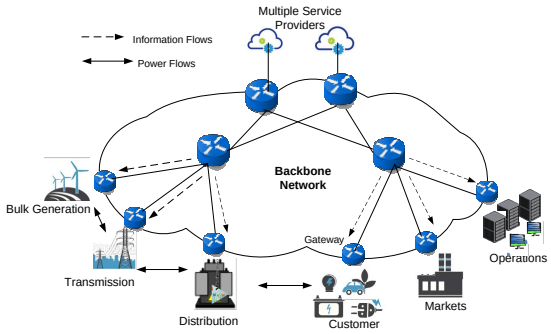

Figure 1: Data paths in the backbone and Local Area Networks of the Smart Grid.

Premaratne, et al. devise a metric formulae to quantify the security of an IED and the IEC61850 network with primary focus on the goals of the attacker [4]. Premaratne, et al. discover that all attacks to IEDs have countermeasures except DoS attacks which can be launched from a remote location across a WAN. This is because, despite having a firewall which can block unwanted hosts, there is the possibility of an attacker using a legitimate host allowed by the firewall to launch the attack. Software Defined Networks (SDN) allows decoupling of the control and data plane, enabling logically centralised network controllers to manage whole networks. In SDN, network traffic is identified, monitored, controlled and managed on a flow level. We therefore use SDN principles to model a cyber resilient smart grid, specifically under DoS attacks.

3. TECHNICAL APPROACH

Our cyber resilient model depends on the security score of IEDs in the smart grid network. We improve the security score model in [4] to include criticality of each IED. Criticality of an IED translates to the impact of attacks to the smart grid network incase this IED were to be compromised. Present day IEDs integrate most of protection, control, monitoring, metering and communication functionalities in to a single device. Their criticality emerges from where they are positioned with in the smart grid. The score for a particular threat based upon its susceptibility (s_i) and countermeasure factor (c_i) would be $t_i = s_i(1 - c_i)$. If a threat has one or more countermeasures, its countermeasure factor (c_i) is set to one. If no countermeasures exist, c_i is set to zero. If the attack can be executed: remotely

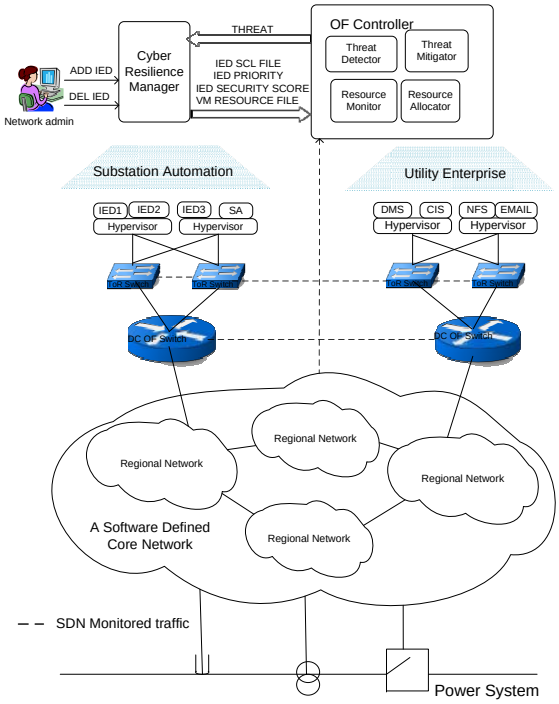

Figure 2: A Cyber resilient Software Defined Smart Grid.

from a WAN $s_i = 1$, within a LAN $s_i = 0.2$ and if physical manipulation is needed, $s_i = 0.1$. The score for the jth IED with m_j threats would hence be:

$$E_j = \sum_{j=1}^{m_j} t_i * S_R \tag{1}$$

Where S_R is security requirement of an IED. Case impact of IED compromise: Limited (Low) $S_R = 0.5$, Serious (Medium) $S_R = 1.0$, Catastrophic (High) $S_R = 1.51$. Overall security score of the network with n IEDs can be calculated from:

$$R = 10 - min\left(10, \sum_{j=1}^{n} E_j\right) \tag{2}$$

Figure 2 emulates a software defined smart grid with virtualized IEDs. We use this architecture to implement and evaluate our cyber resilience model in the presence of an attack. Substation and enterprise data centers are connected through a network of OpenFlow switches. An OpenFlow controller constantly monitors network utilization. When an attack is detected, the controller calculates the security score of the network according to (1) and (2). The controller then takes into account the current security posture, cyber resilience requirements, network topology and available resources to make an informed decision of which SDN mitigation method to use.

4. PRELIMINARY IMPLEMENTATION

Consider a windmill collector substation with 2 Current Differential and Overcurrent IEDs (Group1), 1 Distribution Substation Transformer Monitoring IED (Group2) and 3 Distribution Feeder protection and control IEDs (Group3), 6 OpenFlow switches, 3 end hosts and 3 Servers. Group1 IEDs are positioned in the generation and transmission domain (medium critical) . Group2 IEDs are positioned in the substation domain (most critical) and Group3 IEDs are positioned in the distribution domain (least critical). Table 1 gives the security score of Group2 IEDs. The overall security score of the substation in case of DoS attacks is 0. This indicates that just a few serious DoS attacks on IEDs in the windmill substation network would leave the network vulnerable and non-compliant. Use the SDN framework to remedy this and provide a resilient system. Currently, we use mininet to simulate the OpenFlow switches and Triangle Microworks IEC 61850 test suite to simulate IEDs.

Table 1: Security score for group2 IEDs. S_R = High/critical = 1.51.

DoS Attack	s_i	c_i	t_i
Energy based DoS. LAN	0.2	1	0
Bulky messages. LAN	0.2	0	0.2
Low rate link floods. LAN/WAN	0.2, 1	0, 0	1.2
Protocol based DoS. LAN/WAN	0.2, 1	0, 0	1.2
Software based DoS. LAN/WAN	0.2, 1	0, 0	1.2
$E_j = \sum_{j=1}^{m_j} t_i * S_R$			5.74

5. CONCLUSION

In this poster, we give the motivation for cyber resilient models for the smart grid. We classify the criticality of IEDs and develop a model for quantifying the security score of smart grid networks. Our preliminary implementation demonstrates the impact of DoS attacks on the smart network. We outline an SDN framework that ensures cyber resilience in the presence of attacks. After this initial modeling, we intend to focus on implementing controller modules including; resource monitor, threat mitigator and resource allocator.

6. ACKNOWLEDGMENTS

This material is based upon work supported by the Maryland Procurement Office under Contract No. H98230-14-C-0141.

7. REFERENCES

[1] R. K. Abercrombie, F. T. Sheldon, K. R. Hauser, M. W. Lantz, and A. Mili. Risk assessment methodology based on the nistir 7628 guidelines. In *System Sciences (HICSS), 2013 46th Hawaii International Conference on*, pages 1802–1811. IEEE, 2013.

[2] A. Cahn, J. Hoyos, M. Hulse, and E. Keller. Software-defined energy communication networks: From substation automation to future smart grids. In *Smart Grid Communications (SmartGridComm), 2013 IEEE International Conference on*, pages 558–563. IEEE, 2013.

[3] I. A. Geoff Mulligan. Ip enabled smart objects and the smart grid. http://www.sensorsmag.com/sensors-mag/a-new-revolution-part-2-ip-enabled-smart-objects. [Online].

[4] U. Premaratne, J. Samarabandu, T. Sidhu, R. Beresh, and J.-C. Tan. Security analysis and auditing of iec61850-based automated substations. *Power Delivery, IEEE Transactions on*, 25(4):2346–2355, 2010.