Software Defined Networking enabled Resilience for IEC 61850-based Substation Communication Systems

Hellen Maziku
College of Engineering
Tennessee State University, Nashville, TN, USA
Email: hmaziku@my.tnstate.edu

Sachin Shetty
Virginia, Modeling, Analysis and Simulation Center
Old Dominion University, Norfolk, VA, USA
Email: sshetty@odu.edu

***Abstract*—The resilience of smart grid hinges on its ability to deliver service in a timely and reliable manner even in the presence of persistent attacks. While digital communications in the smart grid present benefits such as higher data transfer rates, they also increase the attack surfaces, permitting IP-based network attacks, such as DoS attacks. To mitigate these emerging attacks and ensure power system requirements are met, there is a need to incorporate resilient capabilities in smart grid. Security risk assessment is a critical component to ensure smart grid cyber resilience. However, there are few security risk assessment approaches for ensuring resilience in smart grid. In this paper, we develop a security score model within a Software Defined Network (SDN) framework for IEC 61850-based substation communication network. The SDN framework incorporates the security risk score model and SDN principles are leveraged to achieve cyber resilience. We illustrate how SDN relieves our smart grid network of congestion and improves timing performance of IEC 61850 type messages, making them time compliant. The security score model also incorporates the criticality of device in the IEC 61850 network. We implement the security score model in Software Defined Network, which provides the ability to reconfigure the IEC 61850 network in real time. We evaluate the model in an experimental GENI testbed characterized by wide-area network dynamics and realistic traffic scenarios to address IEC 61850 network attacks.**

***Index Terms*—Cyber Resilience; Smart Grid; SDN; Security Metrics; OpenFlow; IED**

I. Introduction

The smart grid, being one of the most critical infrastructures, must be available 24/7. To achieve the goal of availability, the smart grid must deliver service in a timely and reliable manner even in the face of persistent attacks. Digital communications in the smart grid present unlimited benefits such as higher data transfer rates, peer to peer communications amongst protection devices, and the ability to have multiple masters with Modbus TCP. Evolution to digital communications has also facilitated emergence of IEC 61850 standard, which has now been adopted as the core communication standard for the smart grid. IEC 61850 standard provides a unified network platform for interconnecting all devices, leading to interoperability and power utility automation.

While digital communications in the smart grid present all these benefits, they also increase the attack surface, permitting IP-based network attacks, such as IP spoofing and DoS attacks. In December 2015, cyber attackers successfully attacked Ukraine's power distribution infrastructure, taking down 27 substations and cutting out power to 225,000 customers for more than three hours [5]. The Ukraine power attack demonstrated interesting evidence on how digital communication pathways increase attack surfaces in the energy sector [2].

The availability of smart grid, which can be defined as timely and reliable access, suffers in an event of any attack such as Denial of Service (DOS) attack. The IEC 61850 standard also known as the standard for Communication Networks and Systems for Power Utility Automation defines 7 message types based on stringent timing requirements. Type 1 messages which are the most time sensitive messages are mapped directly on to the data link layer for prompt delivery. For example, the transfer time limit for a trip message is defined to be 1 ms. To mitigate emerging attacks on smart grid and ensure the tight power system requirements are met, there is a need for cyber resilient smart grid. 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 attacks.

Security risk assessment is one of the critical components for ensuring cyber resilient smart grid and has not received much attention in the literature. To the best of our knowledge, there is currently no standardized security risk assessment approach for the smart grid. Premaratne, et al. devise and simulate a metric formula to model risks and quantify the security of an IEC61850 network from the perspective of the attacker [11]. However, this security score model does not incorporate the criticality of each device in the smart grid network. Criticality of a smart grid device translates to the impact of an attack to the overall smart grid network in case this device were to be compromised. In this paper, we quantitatively assess security risks in smart grids in the perspectives of both the defender and the attacker. We improve the security score model of an IEC61850 network in [11] to reflect the criticality of each device and its impact on the overall smart grid network.

A cyber resilient smart grid should also be dynamic, adaptive and have the ability to re-configure a network in presence of attacks. Unfortunately, the current smart grid infrastructure is static and non-adaptive which makes it nearly impossible or consumes a lot of time to reconfigure a network to react to present day sophisticated attacks. [1]. Software Defined Networking (SDN), provides the ability to reconfigure a network in real time. SDN allows decoupling of the control and data plane, enabling logically centralized network controllers to manage whole networks. In SDN, network traffic is identified, monitored, controlled and managed on a flow level. SDN enables real-time flow management which can be modified based on the network response and on demand changes of the users or the network applications requirements [8], [4]. SDN is the answer to cyber resilience, which is smart grid's most challenging problem to date.

In this paper, we propose an SDN framework which incorporates security risk model, mitigation policies [9] and end to end QoS to address link flood attacks in a IEC 61850-based substation communication network. We develop the security risk model to ensure resilience for a SDN enabled windmill collector substation. The security risk model is deployed in a OpenFlow controller, which continuously monitors the network resources and helps choose the best SDN mitigation policy to adopt in presence of link flood attacks. The open flow controller also enforces end-to-end QOS policy on all network nodes to ensure that mitigation policies do not impact the requirements of competing flows. The OpenFlow controller is implemented in a GENI testbed which emulates a IEC61850-based substation communication network. We show that the knowledge of the security score of the smart grid network helps in choosing an effective mitigation policy in presence of attacks. We also show SDN principles such as enforcing QoS policies, such as, bandwidth reservation relieve the network of link flood attacks and help IEC 61850 applications meet their time transfer limits.

II. SDN-based Security Risk Assessment in Smart Grid

A. Security risk assessment in the smart grid

A cyber resilient system requires an extensive risk assessment model. A resilient smart grid framework should be able to quantify the security of the communication network in the presence and in the absence of attacks. To complement our SDN cyber resilient framework, we propose a security risk model that power utility companies can use to quantify the security of their networks beforehand. We extend and improve the security score model in [11] to include criticality of each Intelligent Electronic Device (IED). Given a particular threat i with susceptibility to occur s_i and countermeasure factor c_i, Premaratne, et al. [11] propose the score of the threat to be:

$$t_i = s_i(1 - c_i) \tag{1}$$

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 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 becomes:

$$E_j = \sum_{j=1}^{m_j} t_i \tag{2}$$

We improve the threat score for the IED by taking into account the criticality of the IED, also known as the security requirement S_R of the IED. The modified score for the jth IED with m_j threats and security requirement S_R becomes:

$$E_{jm} = E_j * S_R \tag{3}$$

If the impact of the IED compromise on the overall smart grid is limited (Low), $S_R = 0.5$, If the impact is serious (Medium), $S_R = 1.0$, and if the impact is catastrophic (High), $S_R = 1.51$.

The security quantification model scores in [11] range between 0 and 10 similar to the Common Vulnerability Scoring System (CVSS) standard. We therefore use the CVSS Security Requirement metric for Availability (AR) to reflect the impact an IED would have on the overall smart grid if it were to be compromised.

Overall security score of the network with n IEDs can be calculated from:

$$R = 10 - min\left(10, \sum_{j=1}^{n} E_{jm}\right) \tag{4}$$

III. Technical Approach

Fig. 1 illustrates a SDN based smart grid with virtualized IEDs. Our resilient architecture utilizes computing and networking resources on the GENI testbed [3]. 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. The network of OpenFlow switches forms the core network. The OpenFlow controller has four distinct modules; the resource monitor nodule, resource allocator module, threat detector module and finally the threat mitigator module. The resource monitor and resource allocator modules work hand in hand to constantly monitor network traffic and watch over resources and how these resources are being utilized. When the threat mitigator is alerted by the threat detector about a potential attack, the mitigator module reads the security score of the network as well as resilience requirements as inputs from the cyber resilience manager. The mitigator module also receives user defined requirements in place of an attack e.g. specific destination to reroute compromised traffic, policy changes from network admins, etc. Depending on the network's security score, company's resilience metrics, current resource utilization and network topology, the mitigator module makes an informed decision on which SDN mitigation scheme to deploy.

In this paper, we model the security quantification score of a windmill collector substation network [7]. We implement

SDN resource monitor and threat detector modules that constantly watch over network resources in the windmill collector substation network and detect presence of link flood attacks. We also implement threat mitigator and resource allocator modules that re-allocate resources during an attack and choose which SDN mitigation technique to deploy.

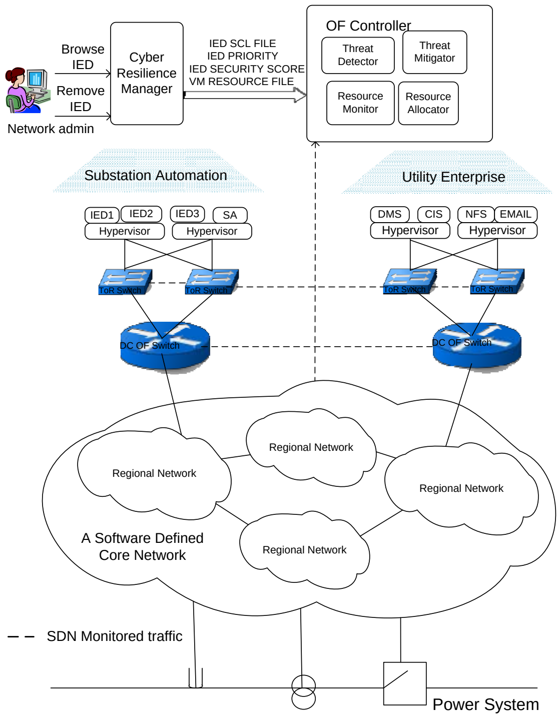

Fig. 1. A Cyber resilient Software Defined Smart Grid

IV. Implementation and Evaluation of SDN based windmill collector substation

In this section, we present the details for the implementation and evaluation of a cyber resilient SDN based windmill collector substation in the emulated data center. Our SDN framework can be extended to any smart grid network.

A. Security Quantification for the Windmill Collector Substation

The Global Environment For Network Innovations (GENI) [3] is a federated virtual laboratory that provides access to multiple different testbeds to GENI experimenters, enabling networking and distributed systems research. We leverage the GENI resources to implement the emulated data center. The windmill collector substation network topology consists of six IEDs forming 2 bays. Each bay switch is OpenFlow enabled.The two bays connect to a SCADA control center through a router and to the station computer through an OpenFlow enabled station switch. The bays also connect to a Human Machine Interface (HMI) through the same station switch.

Using our security score model in (4), we quantify the security of group 1, group 2 and group 3 IEDs in the presence of Link flood attacks (DoS attacks).Table II gives the security score of group 1 IEDs. The security scores for group group 2 and group 3 IEDs are obtained in similar manner. Overall security score of the network becomes:

TABLE I
Security score for group 1 IEDs. S_R = Medium = 1.0

DoS Attack	s_i	c_i	t_i
Energy based DoS. LAN	0.2	1	0
Bulky messages. WAN	1	0	1
Low rate link floods. WAN	1	0	1
Software based DoS. LAN	0.2	1(IDS)	0
Group 1 has 2 IEDs. $E_j = \sum_{j=1}^{m_j} t_i$			4
$E_{jm} = E_j * S_R$			4

$$R = 10 - min(10, (4 + 5.74 + 7.2)) = 0 \tag{5}$$

Assume a compliance threshold, 9. For example, the network can be considered secure if and only if the score for R exceeds 9. A single link flood threat launched over the WAN brings the security score to 9, making the network vulnerable and non-compliant. This indicates that a few serious attacks on IEDs in the windmill substation network leave the network vulnerable and non-compliant. We propose and use the SDN framework to remedy these risks and provide a resilient system.

B. Emulated windmill collector Data Center in GENI

Fig. 2 depicts the topology of the data center network which utilizes GENI resources. We use the topology to create a slice and reserve GENI resources for our data center at Missouri InstaGENI. There are 3 OVS switches in the data center. There are also 6 hosts that run libIEC61850 API to mimic IEC61850 ACSI and serve as virtual IED servers [6]. The 6 IEDs access each other and the station computer through the data plane (layer 2). The station computer serves as the client for the IEC 61850 applications. The station computer: fetches reports from IED1, browses IED 5 for logical nodes and also sends control commands to IED 6. There are ping flows between the station computer and IED 2. There are iperf flows between the station computer and IED 3. The POX controller is hosted on a node in Boston within the GENI testbed. [10]. The Controller listens and accepts TCP connections at a specific IP address and port number.

C. Resource Manager and Threat Detector

We write modules in our POX controller that periodically monitor network resources in our data center. The modules periodically obtain port and flow statistics from all switches in the network. Through these modules, the controller discovers the heaviest flows and busiest links. The heaviest flow is the iperf flow from the station computer to IED 3. The busiest link is the link between bay 1 switch and station switch. Fetching reports from IED 1 takes 20 ms and Fig. 3 reveals incoming traffic from IED1 being throttled. Fig. 4 shows that it takes an average time of 697 ms to browse logical nodes and discover the data models in IED 5. As seen in Fig. 5 sending control

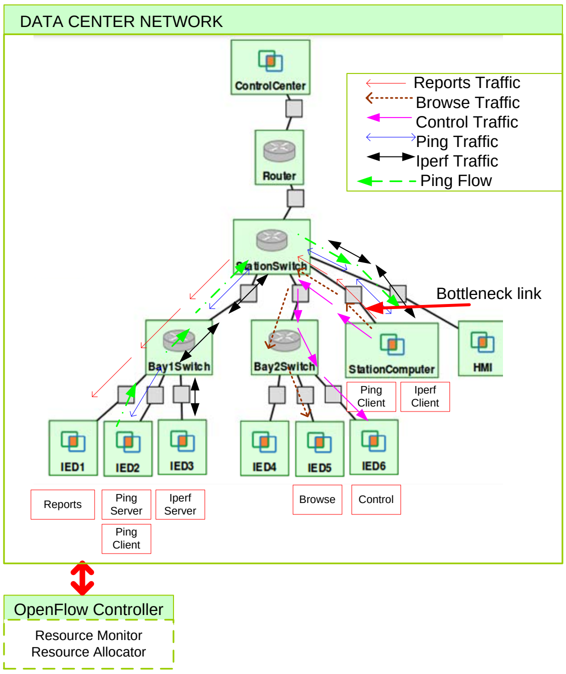

Fig. 2. Network flows in the SDN enabled Windmill Collector Substation

commands to IED 6 takes an average time of 3805.27 ms. Ping flows from IED 2 to the station computer represent non IEC 61850 applications. Fig. 6 shows that link flood attacks throttle ping flows, taking an average time of 30.47 ms.

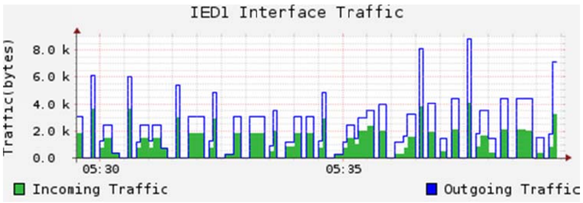

Fig. 3. Effect of link flood attacks on report fetching

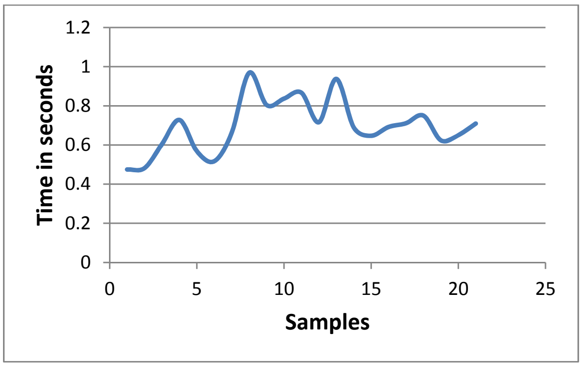

Fig. 4. Effect of link flood attacks on model discovery

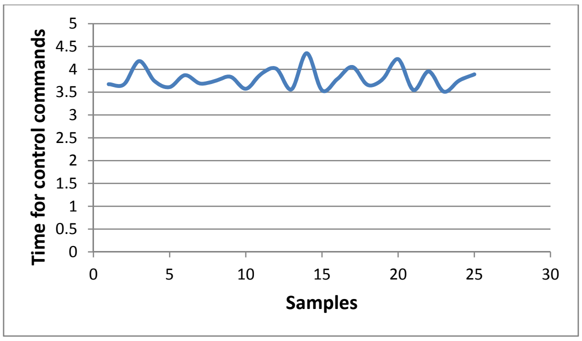

Fig. 5. Effect of link flood attacks on Control Operations

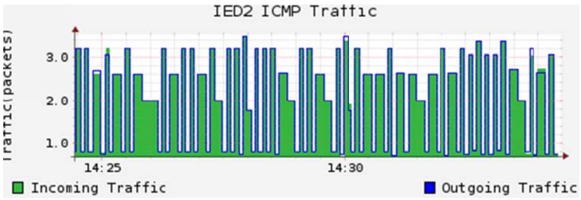

Fig. 6. Effect of link flood attacks on non IEC 61850 applications

D. Resource Allocator and Threat Mitigator

SDN offers numerous mitigation techniques in presence of attacks. The security score of the windmill collector data center indicates the network to be most vulnerable and non compliant. We therefore implement an SDN decision to drop iperf flows which is the heaviest application in the data center. The SDN decision to drop heaviest flows improves fetching reports by 50% and relieves the application from being throttled as illustrated by Fig. 7 . The decision to drop iperf flows improves the model discovery timing performance from an average time of 697 ms to 454 ms. As illustrated in Fig. 8 , dropping iperf flows hugely improves ping flows from an average time of 30.47 ms to 1.67 ms, which is a 95% improvement. Sending control commands to operate and cancel from the station computer to IED 6 improves from an average time of 3805 ms to 2992 ms. An average time of 2992 ms still fails to meet timing requirement for control commands, which is 1-1000 ms.

We therefore implement another SDN decision to enforce QoS on all switches along the control command flow path. The controller uses OVS capabilities to create 2 queues (a default and a dedicated queue) on each port of every OpenFlow switch in the network to enable egress traffic shaping. A queue is used to store traffic until the switch is free to process it. The egress rate is the rate in which packets are sent out from the OpenFlow switch. An egress rate limit is performed on a per-queue per-port basis. We set the bandwidth of the dedicated queue to 4 Mbps and use the SDN action OFPAT ENQUEUE in OpenFlow 1.0 to install an OpenFlow rule to Enqueue all ping traffic to the dedicated queue. Enforcing QoS on ping flows, although takes down the average ping time from 1.67 ms to 10.88 ms, it improves the control operation application from 2992 ms to 444.72 ms. An average time of 444.72 ms meets timing requirement for control commands, which is 1-1000 ms. The SDN decision to enforce QoS on ping flows relieves fetching reports from being throttled as illustrated by Fig. 9 .

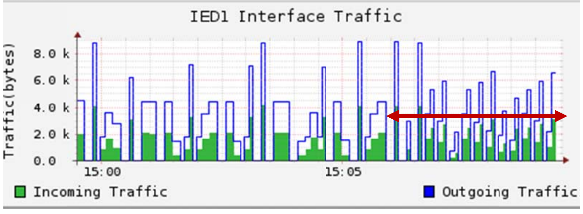

Fig. 7. How dropping of iperf flows impacts fetching reports

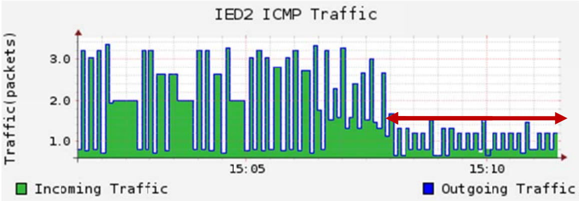

Fig. 8. How dropping of iperf flows impacts Ping flows

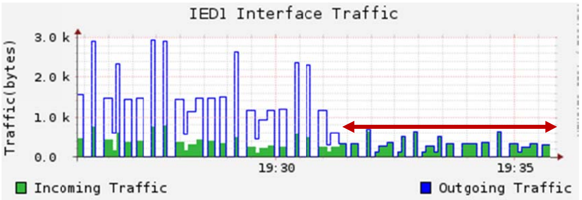

Fig. 9. Enforcing QoS on ping flows impacts fetching reports

TABLE II
SDN DECISION MATRIX FOR DIFFERENT IEC 61850 APPLICATIONS.

	Reports (ms)	Browse IED (ms)	Control Commands (ms)	Other apps (Ping in ms)
No SDN	20	697	3805	30.47
Drop	10	454	2992	1.67
Rate Limit	10	408	444.72	10.88

Table II gives the summary of an SDN decision matrix for different IEC 61850 applications. Table II provides an example of how a power utility company can use both a risk score model and SDN to make an informed decision, hence obtain cyber resilience.

V. Conclusion and Future work

In this paper, we develop and evaluate a technique to quantitatively assess security risks in smart grids. We propose a security score model that factors in the criticality of each device is in the IEC 61850 network. We developed a OpenFlow controller that incorporates the security score model and SDN principles to address link flood attacks in order to provide a resilient smart grid. We empirically evaluate SDN mitigation policies in presence of link flooding attacks on IEC 61850 networks. The OpenFlow controller is capable of identifying heaviest flows and busiest links at real time and detects link floods. The OpenFlow controller also relieves the windmill collector substation of congestion and improves timing performance of IEC 61850 type messages, making them time compliant. The end-to-end QOS policies in the OpenFlow controller also improves performance of other non IEC 61850 applications in the smart grid network. In our future work, we will incorporate additional SDN mitigation policies, introduce new attacks, and evaluate the technique on different network topologies.

Acknowledgment

This material is based upon work supported by the Department of Energy under award number DE-OE0000780 and DHS Award 2014-ST-062-000059. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

References

[1] Xinshu Dong, Hui Lin, Rui Tan, Ravishankar K Iyer, and Zbigniew Kalbarczyk. Software-defined networking for smart grid resilience: Opportunities and challenges. 2015.

[2] EISAC and SANS. Analysis of the cyber attack on the ukrainian power grid: Defense use case. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf. [Online].

[3] GENI. Exploring networks of the future. http://www.geni.net/. [Online].

[4] Dimitrios Gkounis. *Cross-domain DoS link-flooding attack detection and mitigation using SDN prin-ciples*. PhD thesis, MS thesis. Institute of Technology Zurich, 2014.

[5] Robert Lemos. Hackers infiltrated ukrainian power grid months before cyber-attack. http://www.eweek.com/security/hackers-infiltrated-ukrainian-power-grid-months-before-cyber-attack.html. [Online].

[6] libIEC61850. Open source library for iec61850. http://libiec61850.com/libiec61850/. [Online].

[7] M. Warren M. Nelson. Power engineers windmill collector substation project. ece 480. senior design. https://seniordesign.engr.uidaho.edu/2008_2009/power/Final_report.pdf, December 2009. [Online].

[8] Nick McKeown. Software-defined networking. *INFOCOM keynote talk*, 17(2):30–32, 2009.

[9] Nick McKeown, Tom Anderson, Hari Balakrishnan, Guru Parulkar, Larry Peterson, Jennifer Rexford, Scott Shenker, and Jonathan Turner. Openflow: enabling innovation in campus networks. *ACM SIGCOMM Computer Communication Review*, 38(2):69–74, 2008.

[10] POX. Pox controller framework. https://openflow.stanford.edu/display/ONL/POX+Wiki. [Online].

[11] Upeka Premaratne, Jagath Samarabandu, Tarlochan Sidhu, Robert Beresh, and Jian-Cheng Tan. Security analysis and auditing of iec61850-based automated substations. *Power Delivery, IEEE Transactions on*, 25(4):2346–2355, 2010.