February 2015 UILU-ENG-15-2203

SOFTWARE-DEFINED NETWORKING FOR SMART GRID RESILIENCE: OPPORTUNITIES AND CHALLENGES

Xinshu Dong, Hui Lin, Rui Tan, Ravishankar K. Iyer, and Zbigniew Kalbarczyk

Coordinated Science Laboratory
1308 West Main Street, Urbana, IL 61801
University of Illinois at Urbana-Champaign

REPORT DOCUMENTATION PAGE

Form Approved
OMB NO. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	February 2015	

4. TITLE AND SUBTITLE
Software-Defined Networking for Smart Grid Resilience: Opportunities and Challenges

5. FUNDING NUMBERS
OCI-1032889 (NSF)
DE-OE0000097 (DoE)

6. AUTHOR(S)
Xinshu Dong, Hui Lin, Rui Tan, Ravishankar K. Iyer, and Zbigniew Kalbarczyk

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Coordinated Science Laboratory, University of Illinois at Urbana-Champaign, 1308 West Main Street, Urbana, IL, 61801-2307

8. PERFORMING ORGANIZATION REPORT NUMBER
UILU-ENG-15-2203

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Agency for Science, Technology and Research (A*STAR), 1 Fusionopolis Way, #20-10 Connexis North Tower, Singapore 138632
National Science Foundation, 4201 Wilson Boulevard, Arlington, VA 22230
U.S. Department of Energy, 1000 Independence Ave. SW, Washington, DC 20585

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

Software-defined networking (SDN) is an emerging networking paradigm that provides unprecedented flexibility in dynamically reconfiguring an IP network. It enables various applications, such as network management, quality of service (QoS) optimization, and system resilience enhancement. Pilot studies have investigated the possibilities of applying SDN on smart grid communications, while the specific benefits and risks that SDN may bring to the resilience of smart grids against accidental failures and malicious attacks remain largely unexplored. Without a systematic understanding of these issues and convincing validations of proposed solutions, the power industry will be unlikely to embrace SDN, since resilience is always a key consideration for critical infrastructures like power grids. In this position paper, we aim to provide an initial understanding of these issues, by investigating (1) how SDN can enhance the resilience of typical smart grids to malicious attacks, (2) additional risks introduced by SDN and how to manage them, and (3) how to validate and evaluate SDN-based resilience solutions. Our goal is also to trigger more profound discussions on applying SDN to smart grids and inspire innovative SDN-based solutions for enhancing smart grid resilience.

14. SUBJECT TERMS
Software-defined networking; Smart grids; Resilience; Cybersecurity; Cyber-physical systems

15. NUMBER OF PAGES
11

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL

Software-Defined Networking for Smart Grid Resilience: Opportunities and Challenges*

Xinshu Dong[1], Hui Lin[2], Rui Tan[1], Ravishankar K. Iyer[2], Zbigniew Kalbarczyk[2]
[1] Advanced Digital Sciences Center, Illinois at Singapore
[2] Coordinated Science Laboratory, University of Illinois at Urbana-Champaign, IL, USA

Abstract

Software-defined networking (SDN) is an emerging networking paradigm that provides unprecedented flexibility in dynamically reconfiguring an IP network. It enables various applications such as network management, quality of service (QoS) optimization, and system resilience enhancement. Pilot studies have investigated the possibilities of applying SDN on smart grid communications, while the specific benefits and risks that SDN may bring to the *resilience* of smart grids against accidental failures and malicious attacks remain largely unexplored. Without a systematic understanding of these issues and convincing validations of proposed solutions, the power industry will be unlikely to embrace SDN, since resilience is always a key consideration for critical infrastructures like power grids. In this position paper, we aim to provide an initial understanding of these issues, by investigating (1) how SDN can enhance the resilience of typical smart grids to malicious attacks, (2) additional risks introduced by SDN and how to manage them, and (3) how to validate and evaluate SDN-based resilience solutions. Our goal is also to trigger more profound discussions on applying SDN to smart grids and inspire innovative SDN-based solutions for enhancing smart grid resilience.

1 Introduction

As a fundamental part of the smart grid infrastructure, a communication network connects massive grid devices over vast geographic areas to support the grid's supervisory control and data acquisition (SCADA) system. Current grid communication networks are based on the standard IP networking paradigm, where the network functionality (e.g., routing) is mostly fixed at the design phase. At run time, it is often tedious, cumbersome, and even impossible to reconfigure a network to react in time to accidental and malicious events that undermine grid efficiency and safety. Moreover, such a non-adaptive paradigm can become a performance and resilience bottleneck, because of the increasing adoption of modern smart grid technologies that request higher and dynamic network bandwidth and, meanwhile, may expose a larger attack surface because of the pervasive use of software. Examples include phasor measurement units (PMUs) and customer smart meters, which are bandwidth-demanding and found to be vulnerable [7, 25].

This position paper considers the application of software-defined networking (SDN) to smart grids for enhancing system resilience. SDN is a new networking paradigm whose key feature is the separation of the control plane and the data plane [10]. In SDN, network switches are simple forwarding devices, whose forwarding rules can be dynamically configured by a central controller. With the switches and the controller conforming to a control plane protocol (e.g., the OpenFlow protocol [19]), SDN empowers network operators to redefine the operations of a network at run time. In general network environments, SDN has been employed for real-time optimization of network quality of service (QoS) [13] as well as rapid response to detected failures and performance degradation caused by accidental failures [24] and malicious attacks [26].

Several studies [5, 9, 14, 20, 35] advocate adopting SDN to enrich functionality and improve QoS of smart grid communication networks by leveraging SDN's run-time configurability. While QoS is an important issue, system resilience, i.e., the ability of a system to recover and maintain critical services despite accidental failures and malicious attacks, is also a key consideration for critical infrastructures like power grids. In particular, the

*This technical report also appeared as a position paper in The 1st Cyber-Physical System Security Workshop (CPSS), April 14-17, 2015, Singapore.

resilience to attacks has received significantly heightened attention given recent security incidents in national critical infrastructures, such as Stuxnet [17] and Dragonfly [11]. Nonetheless, without a systematic understanding of the resilience benefits and risks that SDN can bring to smart grids, as well as the approaches to manage the risks, the power grid industry is unlikely to adopt SDN technologies. A key challenge in understanding these issues is the need to respect power-engineering-specific requirements and the complex cyber-physical coupling in the sensing-control-actuation closed loops in smart grids.

In this paper, we attempt to provide an initial understanding of the benefits and risks of SDN for smart grid resilience. Specifically, through illustrative examples, we discuss the following three questions:

(1) What are the opportunities for SDN to enhance smart grid resilience? In this context, a key advantage of SDN is its ability to dynamically configure the network (e.g., to create and delete routing paths) to prevent failures and attacks, mitigate their impact if they occur, and isolate them if possible. Although in principle this advantage applies to a broad class of accidental failures and malicious attacks, our focus in this paper is on attacks. Specifically, we discuss three use cases. First, we propose to use SDN to establish dynamic routes for grid control commands, only when the commands are to be transmitted from a control center to grid devices. This approach significantly shrinks the time window in which the attacker can inject malicious commands. Moreover, it also prohibits malicious rerouting and denial-of-service (DoS) attacks. Second, we propose to use SDN to reset switches or re-establish the routing of a grid control application upon the detection of compromised switches, to maintain grid control quality. Third, we propose to use SDN to hot-swap certain grid communication channels from grid-owned communication networks to the public Internet with sufficient encryption, in the presence of devastating attacks in the grid-owned networks. In summary, SDN can significantly raise the bar for attacks to be successful and provide fast network recovery for sustainable grid operations in the presence of attacks.

(2) What are the security risks that SDN brings to smart grids? System complexity often engenders both features and vulnerabilities. SDN brings two major risks. First, its control plane may contain vulnerabilities in its software. Second, its central controller is subject to single-point failures and DoS attacks [15, 28]. As SDN is an emerging technology, its security is still being investigated and improved in the general network context [8, 27]. However, it is also imperative to examine its security in smart grid environments with due consideration of the grid-specific requirements and the cyber-physical coupling. For instance, malicious rerouting of a sensor/control data flow using a long-latency path may be valid from a pure networking perspective, but may reduce the operational quality of grid control systems [4, 32, 33]. In this paper, we discuss three concrete security issues and possible countermeasures. First, a compromised SDN controller may issue malicious SDN control messages to undermine network performance and even destroy the network topology. We propose to examine each outgoing SDN control message by predicting its potential cyber and physical impact on the grid. Second, we propose to leverage several unique characteristics of grid communication traffic for early detection of DoS attempts. Third, we discuss a potential attack in which the attacker can deploy inside the communication network a "darknet" that hides its malicious activities (e.g., to send malicious commands to grid devices) from monitoring channels. Recent research results on rootkit detection [36, 23] may shed light on detection of such darknets in SDN. All the above security issues call for important future research to make SDN more viable for smart grids.

(3) How do we validate and evaluate the above proposals? Validation and evaluation of resilience solutions for complex cyber-physical systems like smart grids remain difficult problems. Integration of SDN will create additional challenges. In that regard, we describe our ongoing research in establishing a smart grid testbed that integrates Mininet (an SDN emulator), PowerWorld (a power system simulator), and a Bro-based semantic intrusion detection system (IDS) that analyzes the DNP3 traffic of a power grid SCADA system. The Mininet-PowerWorld co-simulator provides the cyber and physical "ground truth", while the IDS provides attack detection results for triggering SDN counteractions as well as a base framework to implement SDN control message verification. In summary, the testbed provides a handy and extensible environment that facilitates the exploration and validation of innovative ideas and solutions for smart grid resilience by SDN techniques.

Organization Section 2 briefly discusses related research, and Section 3 illustrates the architecture of SDN-enabled smart grids. Section 4 discusses examples of how SDN techniques can potentially improve grid resilience, while Section 5 explains some of the remaining challenges in applying SDN to improve smart grid resilience. In Section 6, we propose a testbed for prototyping and validating our ideas in, and we conclude in Section 7.

2 Related Work

As an SDN paradigm, OpenFlow was originally proposed as a pragmatic compromise that allows researchers to experiment with new network protocols at scale, without the need for switch vendors to expose internals of their products [19]. Subsequently, OpenFlow-based SDN has received significant research attention [6, 8, 15, 24] and has been applied to the building of various enterprise production networks, such as Google's data center network [13].

Using SDN to enhance network security and securing SDN itself have received increasing research interest for computer networks. Shin et al. [26] present FRESCO, a framework for composing security applications in OpenFlow networks with NOX as the SDN controller. Using FRESCO's scripting language, the implementations of sample security applications are less complex than the legacy implementations and those based directly on OpenFlow primitives. A position paper [16] points out the vulnerabilities brought by SDN to a system, such as the use of software and the possibility of single-point failure due to centralization of network control. Shin et al. [27] design a robust and secure SDN controller, which separates the controller kernel and SDN applications, manages application resources, and provides access control. Dhawan et al. [8] design an SDN application to prevent various attacks (e.g., ARP poisoning and DoS attacks) launched by malicious end hosts and compromised SDN switches. Avant-Guard [28] proposes a proxy-based solution to mitigate control and data plane saturation attacks, and more recently, Ambrosin et al. propose mitigation of buffer saturation attacks on such SDN switch proxies themselves [3].

SDN has also been proposed for network management and QoS in smart grids. Zhang et al. [35] discuss three use cases of SDN in smart grids, i.e., content-based data exchange, virtual networks for distributed energy resource (DER) aggregation, and smart building management. Goodney et al. [9] propose an efficient multicast SDN system that connects high-rate PMUs and data subscribers with different data rate requirements. Molina et al. [20] and Cahn et al. [5] propose to integrate SDN with IEC-61850-based substation automation systems. SDN can facilitate and improve the networking of many (up to a hundred) intelligent electric devices (IEDs) in a substation, by shortest path forwarding, multicast traffic reduction, load balancing, etc. Kim et al. [14] propose to use OpenFlow switches to form virtual local-area networks (VLANs) for multiple grid applications with different QoS requirements. For example, a PMU data collection tree desires smaller depth because of stringent real-time requirements, while a consumer meter data collection tree prefers smaller width due to the limited flow table memory in current off-the-shelf OpenFlow switches.

On the other hand, applying SDN to improve smart grid resilience has not received significant attention. Molina et al. [20] discuss an OpenFlow's fast failover mechanism upon the detection of node failures in the application of SDN to IEC-61850-based substations. In [31], Sydney et al. present a prototype that integrates a 4-bus power grid testbed with an OpenFlow network. They demonstrate the impact of a coincident occurrence of a communication link failure and a load shedding event caused by a generator failure. Despite these discussions and studies, the benefits and risks of SDN for smart grid resilience, to malicious attacks in particular, remains largely unexplored. Moreover, the associated validation and verification problems are also open and challenging, because of the cyber and physical complexities of smart grids.

3 Overview of SDN-enabled Grids

With run-time configurability, SDN can bring significant benefits to the smart grid landscape. We envisage a future in which, by adopting SDN, grid operators will gain greater power and flexibility in defeating or mitigating cyber-attacks. This section describes a simplified architecture of an SDN-enabled smart grid and highlights several threats that SDN can help mitigate.

Fig. 1 illustrates an SDN-enabled smart grid with three major components: a control center, a communication network, and a power grid (exemplified by the IEEE 14-bus test system).

The grid is mainly controlled by the Supervisory Control and Data Acquisition (SCADA) system involving computers, networks, control devices, and software. The control center runs the SCADA master commodity computers and servers to perform various grid control applications, e.g., grid status monitoring, under-frequency load shedding, frequency and voltage controls, and so forth. The SCADA master collects measurement data and transmits control commands from/to SCADA slaves in the grid via the grid communication network; the SCADA slaves, in turn, interact with various control devices. Recently, control devices in smart grids are increasingly being equipped with advanced computing capabilities, commercial off-the-shelf (COTS) operating systems and application software, and various communication interfaces. Such "smart" control devices, e.g.,

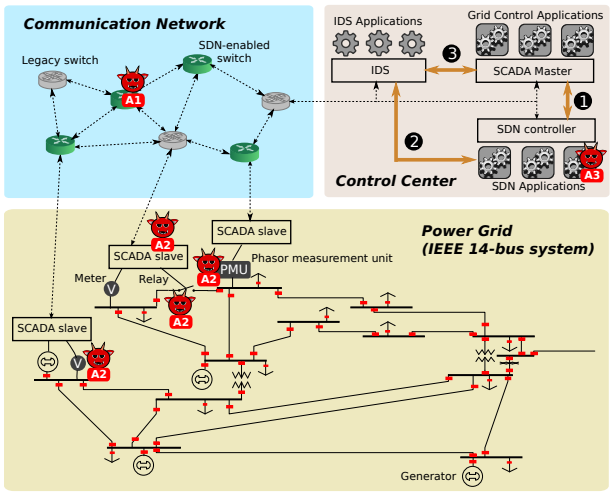

Figure 1: A simplified architecture of an SDN-enabled grid.

Intelligent Electronic Devices (IEDs) and Remote Terminal Units (RTUs), collect readings from sensors, e.g., traditional meters and PMUs, and issue commands to actuators, e.g., circuit breakers and tap changers.

With SDN technologies, the communication network shared by the SCADA master, SCADA slaves, and control devices, sensors, and actuators can be controlled by the SDN controller, with certain legacy network segments using legacy switches. The SDN controller runs various SDN applications to reconfigure the communication network at the right times to optimize QoS and implement resilience support.

In addition, the control center may run an IDS to analyze all incoming and outgoing packets to detect potential malicious activities. More specifically, the SCADA master, the SDN controller, and the IDS can communicate with each other for coordinated actions. We note that the proposed architecture does not mandate specific means of communication among the SCADA master, the SDN controller, and the IDS. The different communication channels are explained as follows (cf. Fig. 1): ❶ The SCADA master and the SDN controller can coordinate their actions to ensure correct and timely retrievals of sensor measurements and deliveries of control commands. ❷ The IDS can notify the SDN controller upon the detection of attacks, possibly with attack profiles (e.g., which data flow paths have been compromised), such that the SDN controller can reconfigure the network accordingly; meanwhile, the SDN controller can provide the IDS with the overall network status to help with attack detection. ❸ The IDS can notify the SCADA master upon the detection of the attacks, such that the SCADA master can tune control parameters to mitigate the impact of attacks; meanwhile, the SCADA master can provide the IDS with detailed run-time information to help detect attacks.

Although our discussions in this paper are independent of how the interactions ❶, ❷, and ❸ are substantiated in the control center, as a general security practice, we assume that they are directly connected via a separate LAN from the SDN-controlled network. Since our focus here is on SDN for grid resilience, our discussions in this paper mainly involve ❶ and ❷. For the interaction ❸, we refer readers to existing studies (e.g., [18]) for more details.

A smart grid faces various cybersecurity threats due to device and system vulnerabilities, careless vendor software upgrade, disgruntled employees, etc. To facilitate our discussion on the opportunities and challenges of SDN in improving grid resilience, we specifically categorize related threats to an SDN-enabled smart grid into the following classes (also illustrated in Figure 1). The categorization is mainly based on the components targeted by the attacks:

(A1) Compromised network switches;

(A2) Compromised grid devices, e.g., RTUs, relays, or SCADA slaves;

(A3) Compromised SDN controllers and/or SDN controller applications.[1]

The threats A1 and A2 are faced by any smart grid, while A3 is specific to SDN-enabled smart grids. Note that the threat A1 may become more credible in SDN-enabled smart grids, because of the software-based switch control and reduced switch heterogeneity [16]. In Section 4, we discuss how to leverage SDN to defeat or

[1]In the rest of this paper, we use the labels A1 to A3 to refer to the three classes of threats.

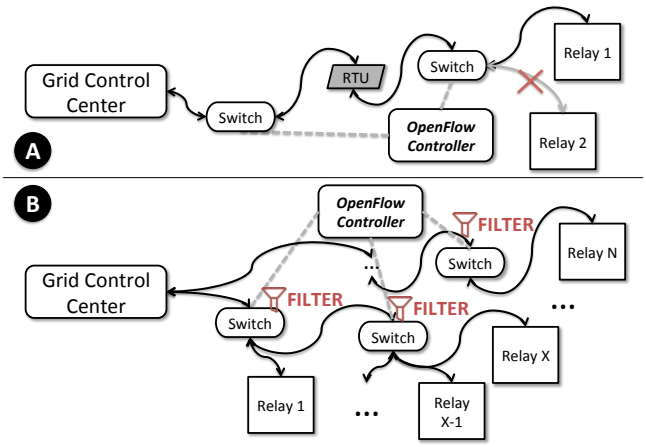

Figure 2: Illustration of SDN-enabled defense against attacks on control devices in a smart grid. (*A: Disabled path to prevent compromised RTUs from redirecting commands to unwanted relays. B: Filtering packets to mitigate DDoS attacks.*)

mitigate A1 and A2. In Section 5, we discuss the challenges brought by A1 and A3, as well as the approaches to manage them to make SDN more viable for enhancing smart grid resilience.

4 Grid Resilience Enhancement Opportunities with SDN

This section discusses three use cases to demonstrate how SDN can be leveraged to improve smart grid resilience to attacks.

4.1 Efficient Detection of Attacks on Critical Control Devices

Smart control devices, e.g., IEDs and RTUs, are playing a major role in smart grid operations. At the same time, such advanced computing and networking devices can expose a larger attack surface to attackers, who can penetrate the control network via various means, e.g., an imperfect "air gap" from the Internet, USB devices, and vendor software updates. Traditional security mechanisms (e.g., firewalls) are inadequate, as seen in recent security incidents [11, 17], because they often reside on network boundaries and cannot protect the system once they are bypassed.

SDN techniques enable unprecedented capabilities for preventing such attacks by dynamically reconfiguring the network to filter out unwanted and potentially malicious traffic due to the threats A1 and A2. For example, as illustrated in Fig. 1, the SCADA master and the SDN controller can coordinate to automatically establish a route to transmit control commands only when necessary. That will significantly shorten the time window during which an attacker can inject malicious control commands from a compromised grid control application or a compromised network switch. Moreover, as illustrated in Fig. 2A, even if an attacker compromises a critical RTU that forwards control commands to relays, he/she will not be able to maliciously reroute the commands to a different relay to cause damage to the grid.

As another example, an attacker can spoof packets that request sensors or relays to send measurements to a certain RTU or a data aggregator. That could, in turn, trigger flooded traffic from many sensors or relays to the victim RTU or data aggregator. As illustrated in Fig. 2B, with SDN, the control center can dynamically configure the switch, so that dynamic monitoring can be implemented to filter out suspiciously excessive traffic towards a certain destination. That can significantly alleviate the load of the victim RTU under such attacks, and maintain the overall availability of the grid communication network. In summary, we envision that SDN can provide handy support in constructing more flexible, precise, and efficient prevention and countermeasures against threats to critical devices in smart grid SCADA systems.

4.2 Resilient Virtual Network Layer for Grid Control Applications

Compromised network switches (A1) may launch a class of attacks that cannot be easily detected and confirmed. A representative example is malicious packet delay, which can lead to synchronization issues, performance degradation of grid controls [4, 33], and even destabilization [32]. It is often hard to recognize the presence of delay attacks, especially when the attacker strategically and perhaps mildly delays sensor measurement and/or control command packets to undermine the operation optimality. That is in contrast to integrity attacks, which can be detected by cryptographic mechanisms and out-of-band verification. Other examples of such hard-to-confirm attacks include selective packet drop and replay. Nevertheless, detection and confirmation of this class of attacks often involve cumbersome manual investigation and take an undesirably long time. Thus, it is desirable to ensure sustainable grid operation performance in the presence of such hard-to-confirm attacks.

SDN provides a mechanism for building a virtual network layer on top of physical communication links [14]. This additional layer can help mitigate the impact of the hard-to-confirm attacks. A virtual network is often defined to connect devices and convey packets that belong to a certain grid control application. By leveraging the control plane functionality, an SDN virtual network can enable finer-grained network status monitoring. For instance, an SDN virtual network can implement adaptive calculation of QoS metrics, e.g., link-wise delivery latency and packet loss rate, according to the dynamic evolution of the underlying physical network. Based on the monitoring result, the SDN controller can rapidly reset or even re-establish a virtual network for a grid control application to isolate suspicious switches. This is analogous to the "golden rule of thumb" of restarting a computer to quickly get rid of suspicious or transient issues. Without SDN, such network reset and re-establishment can be neither fast nor non-disruptive.

Fine-grained network status awareness and global control enable the SDN controller to strategically reset or re-establish a virtual network. The controller can schedule which switches to reset in phases to minimize disruption to the network traffic. It can also redirect the affected flows to alternative routes, while avoiding suspicious switches. Moreover, the global view of the network status will enable the SDN controller to re-establish a virtual network without adversely impacting the QoS of other virtual networks that have shared portion of physical communication links.

4.3 Hot-Swapping between Private & Public Communication Networks

One key aspect of grid resilience is the grid's need to survive major failures caused by catastrophic hazards and large-scale attacks (A1 and A2). Examples include distributed DoS (DDoS) attacks that compromise various switches, relays, and RTUs, which can lead to severe congestion of certain portion of the grid communication network. So far, the power grid has been primarily employing dedicated cables or leased communication links and networks [12, p.425][29]. While providing better isolation in general, such dedicated or leased links may be less resilient to intensive attacks, as they have limited bandwidth and routes. Some grid operators have started to embrace alternative means of communication (e.g., the Internet and wireless networks), for better (although shared) bandwidth and adoption of recent cybersecurity advances, e.g., modern cryptography [34]. However, many are still quite cautious of transmitting sensitive readings and grid control commands via the Internet, as it is supposedly more susceptible to cyber threats.

SDN can provide a unique approach to leveraging both leased lines and the public Internet to provide a highly robust survivability solution for grid operation communications, while minimizing the potential risk of exposure to cyber attacks. For instance, grid operators may rely on the leased lines for routine communications. However, under devastating circumstances, e.g., a significant portion of the grid communication links has been paralyzed, we can leverage SDN technologies to dynamically establish a faster route via the Internet as an emergency response. During the process, the SDN controller can dispatch flows to the remaining functional leased lines and the Internet according to their security requirements. For enhanced security, the SDN controller can also instruct respective control devices to enable encryption for packets being forwarded to routes via Internet. Such an approach enables fast response to extreme situations where ordinary priorities (e.g., "safer" leased lines versus fast recovery of grid operations) have changed.

5 Challenges in Using SDN for Grid Resilience

While enabling flexible reconfigurability, the separation of the control and data planes in SDN may bring in additional challenges in defending against attacks that target the powerful and centralized control plane. In

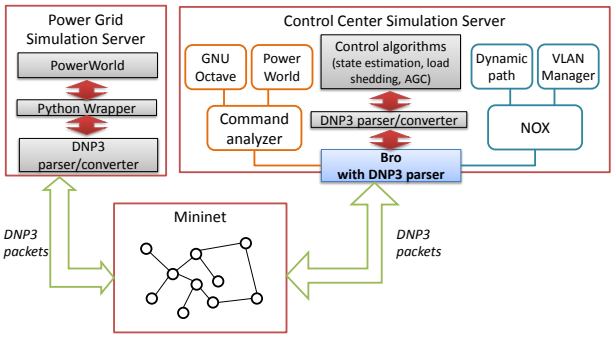

Figure 3: A cyber-physical co-simulation testbed.

particular, attackers may specifically target the control plane of SDN-enabled grid communication networks for *sabotage* and *hiding*. Further research on such potential issues is of great importance and urgency, to eliminate or alleviate the technical hurdles for field trials and deployments of SDN in smart grids.

Topology destruction by malicious control: Because of the centralization of network control, an SDN is susceptible to a compromised SDN controller and/or the SDN applications on top of it (A3). Compromised SDN controller and applications may maliciously change the configurations of the communication network, with the goal of undermining the performance of grid control applications or even destroying the whole network. As high availability is a critical requirement for smart grids, such a potential vulnerability needs to be carefully managed. Existing studies have applied model checking to examine SDN control messages in the general networking context [2, 6]. However, unique challenges arise in the specific context of smart grids, because of the need to consider the implications of SDN control messages for the physical and grid control systems. For instance, malicious rerouting of a sensor/control data flow using a long-latency path may still be valid from a pure networking perspective. However, it may significantly undermine the quality of grid controls [4, 32, 33]. To address this challenge, we propose to use IDS to examine the cyber and physical implications of each outgoing SDN control message, e.g., by real-time simulation [18] and machine-learning-based analysis [21].

DoS attacks accelerated by centralized control: The disproportionate network bandwidth and processing capability between the control and data planes may significantly elevate the magnitude as well as speed of DoS attacks. Existing studies (e.g., [8]) have shown that such DoS attacks may be launched by compromised SDN switches (A1) and malicious end hosts (A2), which flood the SDN controller with spoofed packets requesting a new flow rule. In spite of existing studies [8] that monitor SDN messages and detect successful DoS attacks by monitoring data plane traffic, detecting and counteracting DoS attempts at the control plane is still a challenging problem. Fortunately, several characteristics of smart grids will be helpful to development of robust techniques for detecting DoS attempts, e.g., rather regular SCADA traffic, static publisher-subscriber multicast data flows for PMU [9], and IEC 61850 Generic Object Oriented Substation Events (GOOSE) [20].

Darknet created by SDN "rootkits": By strategically manipulating the forwarding rules in different switches, an attacker who compromises part of the control plane of an SDN system can surreptitiously create a "darknet" within it (A1). Such a darknet can be used to control the communications to key field devices in the smart grid, such as RTUs and relays, while being invisible to the rest of the network. We find such a darknet analogous to rootkits in computer operating systems that are hidden in the kernel and completely evade user-space monitoring mechanisms; we call them *SDN rootkits*. Such SDN rootkits would paralyze the monitoring and control functions of the smart grid, like what happened in the Stuxnet attack but with a much easier attack procedure. Passive monitoring approaches will not be sufficient to detect SDN rootkits. We envisage development of countermeasures through strategic deployment of out-of-band detectors in the grid communication network and through leveraging of the latest progress on rootkit detection [36, 23].

6 An SDN-Enabled Smart Grid Testbed

We propose a testbed to provide an empirical platform for fast prototyping and quick validation of the advantages and challenges of the SDN-grid integration discussed in Sections 4 and 5. Such a testbed must involve

realistic cyber (SDN) and physical (grid dynamics and operations) aspects for simulating the cyber-physical nature of the SDN-enabled smart grid. Although recent studies have developed various co-simulation testbeds based on power system simulators and network simulators (e.g., `ns-2`) [22, 30], none of them have explored the implications and effects of a dynamically controllable communication network on a grid.

Therefore, in the proposed testbed, we leverage Mininet, a popular OpenFlow-based SDN emulator, to emulate SDN-based smart grid communications; we leverage PowerWorld, a high-fidelity power generation and transmission system simulator, to simulate the physical aspects of power systems. Our testbed will enable a co-simulation platform that integrates and coordinates both networking and power system simulations from Mininet and PowerWorld, allowing for experiments on the opportunities and challenges of enabling greater grid resilience with SDN techniques. For instance, it will be able to provide a worst-case estimate of how long it will take to reset or re-establish a virtual network (Section 4.2), and how affordable such a delay would be for power systems. As another example, with such a testbed, we can quickly test with different configurations of private/public network hot-swapping, and evaluate the extent to which they can improve the promptness of control commands, and thus the power system quality (Section 4.3).

Fig. 3 illustrates the architecture of the proposed
co-simulation testbed, which consists of a Power Grid Simulation Server (PGSS), a Control Center Simulation Server (CCSS), and a Mininet. The PGSS leverages PowerWorld to simulate the physical processes of generators, a transmission system, and loads, which provide the "ground truth" of the physical aspect of a power grid. We have used a Python wrapper of the PowerWorld COM API to implement real-time manipulation and access to the internal state (e.g., status of generators, load, meters, circuit breakers) of a PowerWorld simulation session. The CCSS can implement several grid monitoring and control applications, SDN control applications based on NOX, and IDS applications based on Bro [1], as described in [18]. Examples of grid monitoring and control applications include state estimation, under-frequency load shedding, and automatic generation control (AGC). The Bro-based IDS detects malicious outgoing grid and SDN control commands by predicting their execution consequences through rapid steady-state analysis using MATPOWER in GNU Octave, or through transient simulations using PowerWorld. The communications between the CCSS and any simulated field device in the PGSS go through Mininet, within which a node is associated with a field device in the PGSS. To increase the realism of co-simulations, all simulated field devices and the CCSS communicate in DNP3, a protocol widely adopted by power grids.

In summary, the testbed will support simulations of complete closed-loop grid controls driven by the cyber and physical "ground truth" from Mininet and PowerWorld. It will provide an environment to validate and evaluate innovative ideas and solutions of using SDN to improve grid resilience.

7 Conclusion

This paper discusses the opportunities that SDN may bring to smart grids for improving resilience, and the corresponding challenges that still remain. With three illustrative use cases, the paper demonstrates the potential of SDN in strengthening the resilience of smart grids, even under catastrophic circumstances. On the other hand, there are several critical challenges that need to be further studied and addressed before SDN can be securely deployed in smart grids. We hope that our discussion and our initial design of an experimental testbed can trigger more profound research to make SDN more viable for resilient smart grids.

Acknowledgments

We thank William Temple for proofreading this paper and providing useful comments. We also thank Jenny Applequist for her careful editing of the paper. This material is based upon work supported in part by Singapore's Agency for Science, Technology and Research (A*STAR) under a research grant for the Human-centered Cyber-physical Systems Programme at the Advanced Digital Sciences Center, the National Science Foundation (NSF) under Grant No. OCI-1032889, and the Department of Energy (DOE) under Award Number DE-OE0000097. Any opinions, findings, and conclusions or recommendataions expressed in this material are those of the authors and do not necessarily reflect the views of A*STAR, NSF, or DOE.

References

[1] The Bro network security monitor. `https://www.bro.org/`.

[2] E. Al-Shaer and S. Al-Haj. FlowChecker: Configuration analysis and verification of federated openflow infrastructures. In *Proceedings of the 3rd ACM Workshop on Assurable and Usable Security Configuration (SafeConfig)*, 2010.

[3] M. Ambrosin, M. Conti, F. D. Gaspari, and R. Poovendran. Lineswitch: Efficiently managing switch flow in software-defined networking while effectively tackling dos attacks. In *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security (AsiaCCS)*, 2015.

[4] S. Bhowmik, K. Tomsovic, and A. Bose. Communication models for third party load frequency control. *IEEE Transactions on Power Systems*, 19(1):543–548, 2004.

[5] A. Cahn, J. Hoyos, M. Hulse, and E. Keller. Software-defined energy communication networks: From substation automation to future smart grids. In *Proceedings of 4th IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2013.

[6] M. Canini, D. Venzano, P. Peresini, D. Kostic, and J. Rexford. A NICE way to test openflow applications. In *Proceedings of the 9th USENIX Symposium on Networked Systems Design and Implementation (NSDI)*, 2012.

[7] M. Davis. Recoverable advanced metering infrastructure. In *Blackhat*, 2009.

[8] M. Dhawan, R. Poddar, K. Mahajan, and V. Mann. SPHINX: Detecting security attacks in software-defined networks. In *Proceedings of the 2015 Network and Distributed System Security (NDSS) Symposium*, 2015.

[9] A. Goodney, S. Kumar, A. Ravi, and Y. H. Cho. Efficient PMU networking with software defined networks. In *Proceedings of 4th IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2013.

[10] A. Greenberg, G. Hjalmtysson, D. A. Maltz, A. Myers, J. Rexford, G. Xie, H. Yan, J. Zhan, and H. Zhang. A clean slate 4D approach to network control and management. *SIGCOMM Comput. Commun. Rev.*, 35(5), 2005.

[11] A. Hesseldahl. Hackers infiltrated power grids. `http://on.recode.net/1FpKP7Y`.

[12] E. Hossain, Z. Han, and H. V. Poor, editors. *Smart Grid Communications and Networking*. Cambridge Univ. Press, 2012.

[13] S. Jain, A. Kumar, S. Mandal, J. Ong, L. Poutievski, A. Singh, S. Venkata, J. Wanderer, J. Zhou, M. Zhu, J. Zolla, U. Holzle, S. Stuart, and A. Vahdat. B4: Experience with a globally-deployed software defined wan. In *Proceedings of the Annual Conference of the ACM Special Interest Group on Data Communication (SIGCOMM)*, 2013.

[14] Y.-J. Kim, K. He, M. Thottan, and J. G. Deshpande. Virtualized and self-configurable utility communications enabled by software-defined networks. In *Proceedings of 5th IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2014.

[15] R. Kloti, V. Kotronis, and P. Smith. OpenFlow: A security analysis. In *Proceedings of the IEEE International Conference on Network Protocols (ICNP)*, 2013.

[16] D. Kreutz, F. Ramos, and P. Verissimo. Towards secure and dependable software-defined networks. In *Proceedings of ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking (HotSDN)*, 2013.

[17] R. Langner. Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security & Privacy*, 9(3):49–51, 2011.

[18] H. Lin, A. Slagell, Z. Kalbarczyk, P. W. Sauer, and R. K. Iyer. Semantic security analysis of scada networks to detect malicious control commands in power grids. In *Proceedings of the Smart Energy Grid Security (SEGS) Workshop*, 2013.

[19] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner. OpenFlow: enabling innovation in campus networks. *SIGCOMM Computer Communication Review*, 38(2):69–74, 2008.

[20] E. Molina, E. Jacob, J. Matias, N. Moreira, and A. Astarloa. Using software defined networking to manage and control IEC 61850-based systems. *Computers & Electrical Engineering*, 2014.

[21] H. H. Nguyen, R. Tan, and D. K. Y. Yau. Safety-assured collaborative load management in smart grids. In *Proceedings of the 5th ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS)*, 2014.

[22] D. M. Nicol, C. M. Davis, and T. Overbye. A testbed for power system security evaluation. *International Journal of Information and Computer Security*, 3(2):114–131, 2009.

[23] C. Pham, Z. Estrada, P. Cao, Z. Kalbarczyk, and R. K. Iyer. Reliability and security monitoring of virtual machines using hardware architectural invariants. In *Proceedings of the 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2014.

[24] M. Reitblatt, M. Canini, A. Guha, and N. Foster. FatTire: declarative fault tolerance for software-defined networks. In *Proceedings of ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking (HotSDN)*, 2013.

[25] D. P. Shepard, T. E. Humphreys, and A. A. Fansler. Evaluation of the vulnerability of phasor measurement units to gps spoofing attacks. *International Journal of Critical Infrastructure Protection*, 5(3):146–153, 2012.

[26] S. Shin, P. A. Porras, V. Yegneswaran, M. W. Fong, G. Gu, and M. Tyson. FRESCO: Modular composable security services for software-defined networks. In *Proceedings of the 2013 Network and Distributed System Security (NDSS) Symposium*, 2013.

[27] S. Shin, Y. Song, T. Lee, S. Lee, J. Chung, P. Porras, V. Yegneswaran, J. Noh, and B. B. Kang. Rosemary: A robust, secure, and high-performance network operating system. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2014.

[28] S. Shin, V. Yegneswaran, P. Porras, and G. Gu. AVANT-GUARD: Scalable and vigilant switch flow management in software-defined networks. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2013.

[29] H. L. Smith. A brief history of electric utility automation systems. *Electric Energy T&D Magazine*, 14:39–44, April 2010.

[30] T. Strasser, M. Stifter, F. Andren, and P. Palensky. Co-simulation training platform for smart grids. *IEEE Transactions on Power Systems*, 29(4):1989–1997, 2014.

[31] A. Sydney, D. S. Ochs, C. Scoglio, D. Gruenbacher, and R. Miller. Using GENI for experimental evaluation of software defined networking in smart grids. *Computer Networks*, 63:5–16, 2014.

[32] R. Tan, V. Badrinath Krishna, D. K. Yau, and Z. Kalbarczyk. Impact of integrity attacks on real-time pricing in smart grids. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2013.

[33] K. Tomsovic, D. E. Bakken, V. Venkatasubramanian, and A. Bose. Designing the next generation of real-time control, communication, and computations for large power systems. *Proceedings of the IEEE*, 93(5):965–979, 2005.

[34] F. Wu, K. Moslehi, and A. Bose. Power system control centers: Past, present, and future. *Proceedings of the IEEE*, 93(11):1890–1908, Nov 2005.

[35] J. Zhang, B.-C. Seet, T.-T. Lie, and C. H. Foh. Opportunities for software-defined networking in smart grid. In *Proceedings of the International Conference on Information, Communications and Signal Processing (ICICS)*, 2013.

[36] L. Zhang, S. Shetty, P. Liu, and J. Jing. Rootkitdet: Practical end-to-end defense against kernel rootkits in a cloud environment. In *Proceedings of the European Symposium on Research in Computer Security (ESORICS)*, pages 475–493, 2014.