SDN-Enabled Cyber-Physical Security in Networked Microgrids

Yan Li, *Member, IEEE*, Yanyuan Qin, *Student Member, IEEE*, Peng Zhang, *Senior Member, IEEE*, and Amir Herzberg

***Abstract*—A software-defined active synchronous detection (SDASD) is presented to protect networked microgrids (NMs) from cyberattacks on SDN network and power bot attacks on inverter controllers of distributed energy resources (DERs). A *HostStatus_Checker* is designed and embedded in an SDN controller to authenticate the entity of hosts for data communication of NMs. Based on the secured communication layer, active synchronous detection method is introduced to efficiently detect power bot attacks on DER controllers in NMs without impeding system normal operations. Extensive tests show that SDASD can detect and mitigate malicious attacks online and serve as a powerful safeguard for monitoring and protecting future NMs.**

***Index Terms*—Cyberattack, software-define networking, host location hijacking, active synchronous detection, cyber-physical security, networked microgrids, distributed energy resources.**

I. Introduction

NETWORKED microgrids (NMs), namely a cluster of interconnected microgrids with interactive power support and coordinated energy management [1]–[3], has been envisioned as the keystone of the future smart and connected communities. Communication infrastructure and inverter controllers in distributed energy resources (DERs) are two essential constituents in operating a stable and secure NM system. Nowadays, Software-Defined Networking (SDN) [4], [5] has been increasingly employed to enable ultra-fast microgrid control, support scalable NMs, and respond to NM contingencies [6]. Although the global monitoring and real-time configuration of SDN significantly enhance the resiliency and reliability of NMs [7], it makes the system vulnerable to cyberattacks due to its holistic network visibility and flexible network programmability [8], [9]. Those attacks are typical cases of the *first generation of cyberattacks* on the power grids as they exploit information technology (IT) networks such as SDN to compromise NM operations. Recently there is an emergence of a *second generation of cyberattacks* on the power grids, i.e., the use of *power bots* which are corrupted power-consuming or DER devices controlled by remote attackers. Consequently, cybersecurity concerns have become a major hurdle to the wide adoption of NMs.

In recent years, awareness of attacks against SDN has grown in the computer science community. VeriFlow introduces a layer between control plane and data plane to detect the network anomalies [10]. Based on the model checker techniques, FlowChecker is a tool to identify intra-switch misconfiguration in one single encoded FlowTable [11]. AvantGuard introduces connection migration and actuating triggers to deter data-to-control-plane saturation attacks [12]. FRESCO provides OpenFlow-enabled detection and mitigation modules [13]. ANCHOR attempts to enforce global policies for security in SDN [14]. DELTA provides a security assessment framework which can perform SDN attacks in diverse test environments [15]. Despite the above advances, the inherent vulnerability inside OpenFlow controllers remains an open challenge. Because the hosts for data communication in SDN network are the key to secure resilient operations of microgrids and NMs [8], [9], cyberattacks on these hosts are the foremost challenges yet to be addressed. Power bot attacks on the DER inverter controllers exacerbate the cybersecurity risks in NMs because NM operations fully depend on the reliable functioning of the DER inverters. Nevertheless, existing fault-tolerant control and robust control are designed to detect and accommodate traditional faults and thus can neither identify nor mitigate power bot attacks [16].

To bridge the gap, a Software-Defined Active Synchronous Detection (SDASD) method is proposed to effectively defend against both the first generation of cyberattacks such as cyberattacks on SDN network and the second generation of cyberattacks such as power bot attack on inverters. First, a dynamic defense strategy is devised and implemented in the SDN communication infrastructure to protect NMs against cyberattacks on SDN network. Meanwhile, by using a probe signal transmitted via a secured SDN network, active synchronous detection will be developed to detect power bot attacks on inverter controllers of DERs. The novelties of SDASD are threefold:

1) It offers extremely lightweight real-time detection of cyberattacks on cyber-physical NMs, meaning it would not compromise the performance of SDN network or DER controllers. Thus, secure ultra-fast controls can be

Manuscript received July 9, 2018; revised November 2, 2018; accepted December 17, 2018. Date of publication December 24, 2018; date of current version June 20, 2019. This work was supported in part by the National Science Foundation under Grants CNS-1647209, ECCS-1611095, and ECCS-1831811, in part by the Office of the Provost, University of Connecticut, in part by the Eversource Energy Center, and in part by the UTC Fellowship. Paper no. TSTE-00679-2018. *(Corresponding author: Peng Zhang.)*

Y. Li and P. Zhang are with the Department of Electrical and Computer Engineering, University of Connecticut, Storrs, CT 06269 USA (e-mail: yan.7.li@uconn.edu; peng.zhang@uconn.edu).

Y. Qin and A. Herzberg are with the Department of Computer Science and Engineering, University of Connecticut, Storrs, CT 06269 USA (e-mail: yanyuan.qin@uconn.edu; amir.herzberg@uconn.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSTE.2018.2889451

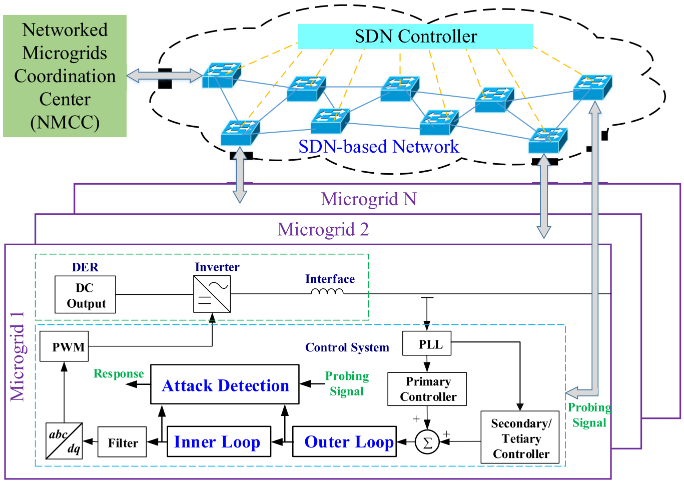


Fig. 1. SDASD architecture.

guaranteed to significantly improve the stable operation of NMs.

2) It enables active detection of power bot attacks quickly and precisely by injecting programmable probe signals into NMs. Therefore, once an NM system is under attack, security issues can be quickly pinpointed and restorations can be efficiently implemented.
3) It enables a secure plug-and-play function of microgrids via OpenFlow protocol. It means in the future, NMs can be configured and dispatched more effectively.

The remainder of this paper is organized as follows: Section II describes the overall architecture of SDASD. Section III establishes the defense strategies against cyberattacks on SDN network and Section IV presents the active synchronous detection method against power bot attacks on the DER controller. In Section V, tests on networked microgrids verify the feasibility and effectiveness of the presented SDASD. Conclusions are drawn in Section VI.

II. Architecture of SDASD

SDASD is a generic framework that includes two layers: (1) Network security layer for protecting the data plane communication channel of SDN network, and (2) power bot defense layer for actively detecting attacks on DER controllers in physical NMs based on the probe signals transmitted via the secured SDN network. Fig. 1 shows the architecture of SDASD.

In Fig. 1, the function of *Networked Microgrids Coordination Center (NMCC)* is to coordinate the operations of NMs and generate probe signals used for the power bot defense layer. *SDN Controller* is based on protocols, such as OpenFlow [17], and enables intelligent networking in the communication network. In *Microgrid*, the DC output of each *DER* is converted by an *Inverter* to AC output, and then integrated into the physical NMs through an *Interface* circuit [18], [19]. The *Control System* is to adjust the power output from a DER unit. Specifically, the Phase Lock Loop (*PLL*) is adopted to identify the phase of input signals, usually the three-phase voltages [20]. This phase is then used either in *Primary Controller* or *Secondary/Tertiary Controller* to generate a droop-control signal or secondary/tertiary control signal for the double-loop controller [21], i.e., *Outer Loop* and *Inner Loop*. *Attack Detection* usually uses a detection function to identify attacks. One typical example of the double-loop controller and attack detection is given in Section IV. *Filter* is used to eliminate any possible noise introduced by the probe signal. Finally, the signals generated by the double-loop controller are transformed from the *dq* frame to the *abc* frame, and the *PWM* technique [22] is then used to generate signals to control the switches, such as IGBTs, in the *Inverter*.

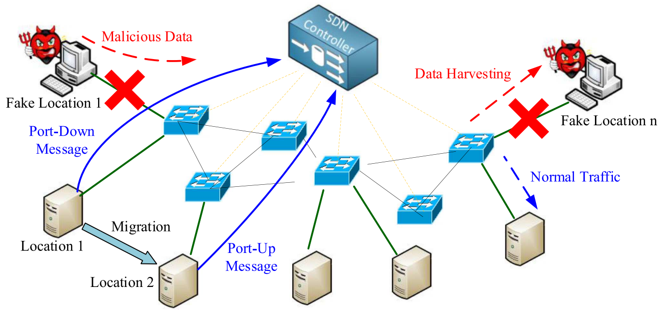


Fig. 2. Cyberattack defending strategies.

Strategies of detection and defense of cyberattack and power bot attacks on the aforementioned cyber-physical NMs are introduced in the following sections.

III. Defense Against Cyberattacks on SDN

This paper focuses on defending the hijacking attacks of hosts (for data communication) of networked microgrids coordination center (NMCC) and microgrids, because poisoning data via hosts could easily and significantly deteriorate the normal operation of a NM system. The essential idea of defending such cyberattacks on SDN data plane is to set up a ***HostStatus_Checker*** flag in Host Tracking Service (HTS) [23], [24] in SDN controller to check the precondition and postcondition of hosts so as to authenticate their entity.

A. Host Tracking Service Update in SDN Controller

In NMs or other cloud computing scenarios, host or controller might migrate frequently due to physical topology changes of microgrids. Since the host profile is maintained and used in the SDN controller to track the location of one specific host within network, the HTS provides an effective way to track network mobility. Specifically, HTS monitors the ***HostStatus_Checker*** flag in the ***Packet-In*** messages, and once is aware that a particular host migrates to a new location, HTS updates host profile table where each item includes host MAC address, switch port number, and switch Datapath ID (DPID) [8].

B. Defending Strategies

The defending strategies are shown in Fig. 2, including the following perspectives:

- Precondition: Before a host of NMCC or microgrid migrates to another location, a ***Port-Down*** message will be sent to the SDN controller to pre-update the ***HostStatus_Checker***. At this moment, the host is supposed to be unreachable in the previous location.

- Postcondition: After the host successfully migrates to the new location, a ***Port-Up*** message will be sent to the SDN controller from the new location to complete the update of ***HostStatus_Checker*** and host profile table. At this moment, the host is supposed to be available in the new location.
- Defense against cyberattacks:
  a) Malicious Data Injection: If data packets are received with the same host information (MAC/IP address) but from different locations (import information) without sending a ***Port-Down*** message to the SDN controller beforehand, it means the location migration did not happen actually. This event will be identified as a host location hijacking cyberattack, and the following actions will be taken: (1) alarms will be raised; and (2) the corresponding malicious traffic from the new location will be blocked to guarantee normal operation of NMs.
  b) NMs Critical Data Sniffer: If data packets are received from a new host only sending ***Port-Up*** message to SDN controller beforehand but without ***Port-Down*** message, this host will be identified as a compromised host, and the following steps will be taken: (1) SDN controller will immediately shut down its corresponding port; and (2) normal traffic will not be sent to the compromised host.

IV. Active Synchronous Detection in DER Controllers of Networked Microgrids

In this paper, active synchronous detection [16] is extended to detect power bot attacks in NMs and is implemented through SDN network. The essential idea of active synchronous detection includes the following three steps: (1) NMCC generates small probe signals; (2) those signals are transmitted via the secured SDN network to targets (e.g. DER controllers); and (3) the target responses are transmitted back to NMCC and compared against pre-determined detection rules to identify whether and where power bot attacks occur.

A. Probe Signals for Active Synchronous Detection

To ensure the real-time detection and non-impediment of the targets' normal operations, the probe signals being continuous, periodic, and with small magnitudes in frequency domain are preferable. Mathematically, those features can be described as:

$$s(t) = s(t + n\mathrm{T}), \tag{1}$$

$$\|s(f)\| \leq \varepsilon, \tag{2}$$

$$\int_{t}^{t+\mathrm{T}} s(t)dt = 0, \tag{3}$$

where T is the period of the continuous signal $s(t)$, $\|\cdot\|$ is the l_2 norm of the harmonic at the frequency f, ε is a small threshold. (1)–(3) offer the following features:

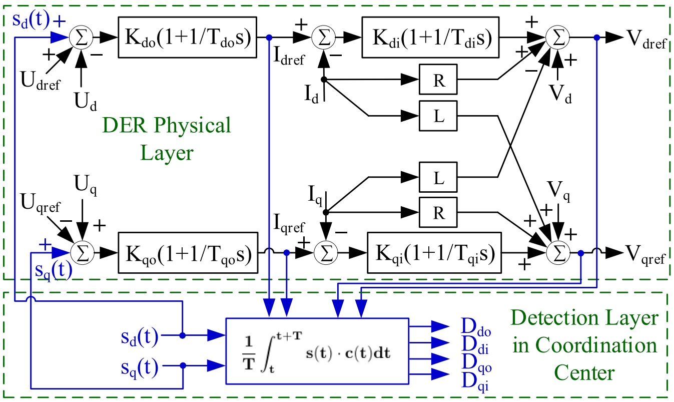


Fig. 3. Active synchronous detection on double loop controller.

- The impact of the probe signal on the target within one period is zero, which means the probe signal does not change the overall performance of DER controllers.
- The probe signal is programmable and can be modified flexibly at the NMCC, if necessary, to further increase the cost of the adversary.

B. Active Synchronous Detection in DER Controllers

The most malicious power bot attacks on NMs could be those on the inverter controllers of DERs because such attacks can immediately compromise or collapse NMs. As the *dq* double loop controller is widely used in DER inverters [18] (see Fig. 1), active synchronous detection of power bot attacks on this type of controllers is developed to exemplify how the detection rules are built.

The cyber-secured double loop structure is illustrated in Fig. 3, where probe signals, e.g., $s_d(t)$ and $s_q(t)$, are generated in NMCC and then delivered through the secured SDN network to critical DERs in each microgrid. These probe signals can be adjusted whenever necessary. The attack detection function can be chosen as a shifting window average as follows:

$$D = \frac{1}{\mathrm{T}} \int_{t}^{t+\mathrm{T}} s(t) \cdot c(t)dt, \tag{4}$$

where $s(t)$ refers to probe signals $s_d(t)$ or $s_q(t)$; $c(t)$ corresponds to control signals I_{dref}, I_{qref}, V_{dref}, or V_{qref}; D represents the attack detector signals including the outer loop signals (D_{do} and D_{qo}) and the inner loop signals (D_{di} and D_{qi}). These detector signals are calculated in NMCC and discussed below.

C. Detection Rules

Detection rules are derived and built in the NMCC to identify the type and location of a power bot attack. Two typical power bot attacks on DER controllers are considered:

1) Topologies of controllers are attacked and modified;
2) Parameters in DER controllers are overwritten by attacker.

To detect the attacks, two sinusoidal signals in (5) and (6) are generated at the NMCC and routed to the

TABLE I
VALUES OF DETECTOR SIGNALS UNDER POWER BOT ATTACKS

Controller Under Attack	Type of Attacks	D_{do}	D_{qo}	D_{di}	D_{qi}
Outer Loop	1)	0	0	0	0
	2)	$\alpha_d^2 K'_{do}/2$	$\alpha_q^2 K'_{qo}/2$	$\alpha_d^2 K'_{do} K_{di} (T'_{do} T_{di} \omega_d^2 - 1)/2T'_{do} T_{di} \omega_d^2$	$\alpha_q^2 K'_{qo} K_{qi} (T'_{qo} T_{qi} \omega_q^2 - 1 -)/2T'_{qo} T_{qi} \omega_q^2$
Inner Loop	1)	$\alpha_d^2 K_{do}/2$	$\alpha_q^2 K_{qo}/2$	0	0
	2)	$\alpha_d^2 K_{do}/2$	$\alpha_q^2 K_{qo}/2$	$\alpha_d^2 K_{do} K'_{di} (T_{do} T'_{di} \omega_d^2 - 1)/2T_{do} T'_{di} \omega_d^2$	$\alpha_q^2 K_{qo} K'_{qi} (T_{qo} T'_{qi} \omega_q^2 - 1 -)/2T_{qo} T'_{qi} \omega_q^2$
Outer Loop & Inner Loop	1)	0	0	0	0
	2)	$\alpha_d^2 K'_{do}/2$	$\alpha_q^2 K'_{qo}/2$	$\alpha_d^2 K'_{do} K'_{di} (T'_{do} T'_{di} \omega_d^2 - 1)/2T'_{do} T'_{di} \omega_d^2$	$\alpha_q^2 K'_{qo} K'_{qi} (T'_{qo} T'_{qi} \omega_q^2 - 1 -)/2T'_{qo} T'_{qi} \omega_q^2$

DER controller.

$$s_d(t) = \alpha_d \sin(\omega_d t), \tag{5}$$

$$s_q(t) = \alpha_q \sin(\omega_q t). \tag{6}$$

Then the attack detection function D_{do} and D_{qo} can be calculated as follows:

$$D_{do} = \frac{1}{\mathrm{T}} \int_t^{t+\mathrm{T}} s_d(t) I_{d\mathrm{ref}} dt = \frac{\alpha_d^2 K_{do}}{2}, \tag{7}$$

$$D_{qo} = \frac{1}{\mathrm{T}} \int_t^{t+\mathrm{T}} s_d(t) I_{q\mathrm{ref}} dt = \frac{\alpha_q^2 K_{qo}}{2}. \tag{8}$$

Correspondingly, the attack detection function D_{di} and D_{qi} can be calculated as follows:

$$D_{di} = \frac{1}{\mathrm{T}} \int_t^{t+\mathrm{T}} s_d(t) V_{d\mathrm{ref}} dt = \frac{\alpha_d^2 K_{do} K_{di}}{2} \left(1 - \frac{1}{T_{do} T_{di} \omega_d^2}\right), \tag{9}$$

$$D_{qi} = \frac{1}{\mathrm{T}} \int_t^{t+\mathrm{T}} s_q(t) V_{q\mathrm{ref}} dt = \frac{\alpha_q^2 K_{qo} K_{qi}}{2} \left(1 - \frac{1}{T_{qo} T_{qi} \omega_q^2}\right). \tag{10}$$

In brief, (7) and (8) show the outer loop responses of the detection function given in (4) in the *d*-axis and *q*-axis, respectively; and similarly, (9) and (10) show the inner loop responses in the *d*-axis and *q*-axis, respectively. More details of the above derivation can be found in Appendix I.

So, by using (7) and (8), attacks on the outer loop of DER controller can be identified; attacks on the inner loop can be detected via (9) and (10). More specially, if a DER controller is intact, the steady-state values of the detector signals should be identical to the values given in (7)–(10). Otherwise, if the DER controller is under attack, the detector signals will deviate from these values. Table I summarizes the abnormal values under the aforementioned attacks. By checking these abnormal values, the type and location of a specific power bot attack can be identified.

V. TEST AND VALIDATION OF SDASD

A typical NM system shown in Fig. 4 is used to test and validate the effectiveness of SDASD in defending against cyber-physical attacks on NMs. This test system includes six microgrids and operates in islanded mode, which means Circuit Breaker 0 is open. More details of the test system can be found in Appendix II. Fig. 5 shows the SDN topology used for the NM system, including one SDN OpenFlow controller Ryu [25] and five switches. The NM system is modeled in Matlab/Simulink. Simulation time step is 50 μs, and a sample rate of 10 for communication data is selected. SDN network is running in a Mininet environment. In Mininet, we set the bandwidth for each link as 1 Gbps, following a common practice used in Ethernet network. User Datagram Protocol (UDP) [26] is adopted to transmit data packets between microgrids and NMCC through Mininet [27].

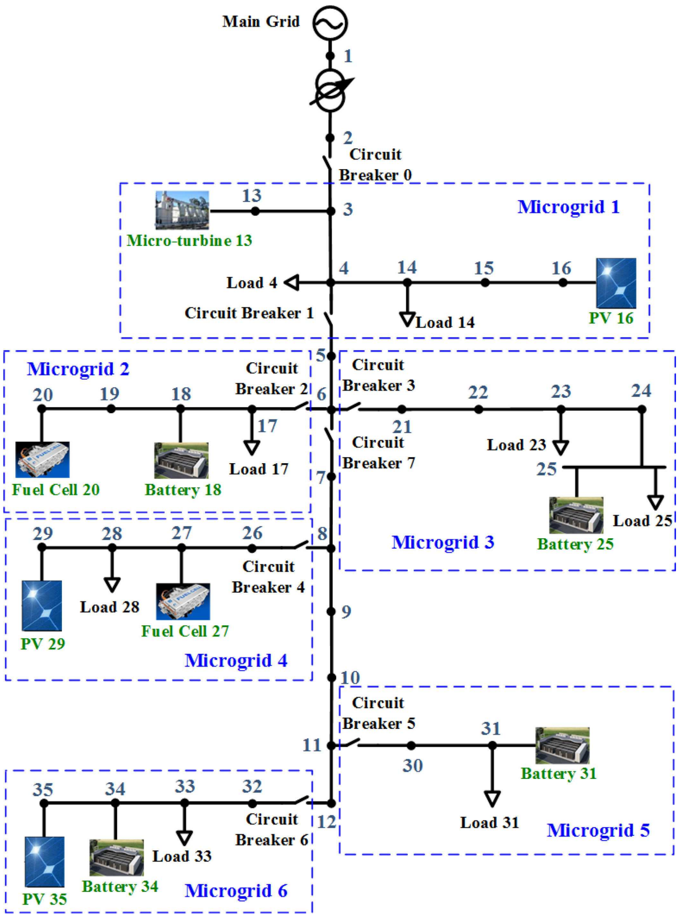


Fig. 4. A typical networked microgrids.

A. Verification of SDASD on Defending Against Cyberattacks

NMCC is initially running in Center 1 whose IP address is 10.0.0.7. Center 2 with IP address 10.0.0.8 is a new migrated destination. To verify the efficacy of SDASD in defending against cyberattacks, three different cases are given as follows:

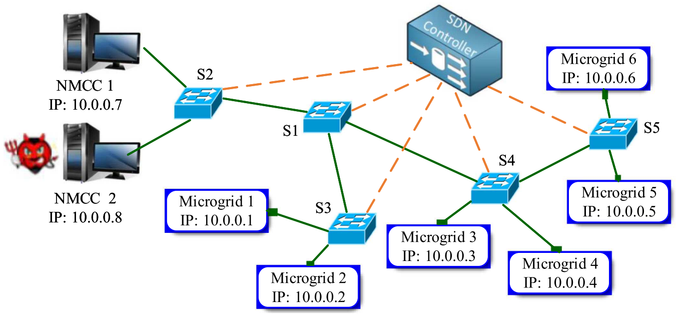


Fig. 5. SDN topology for the NM system.

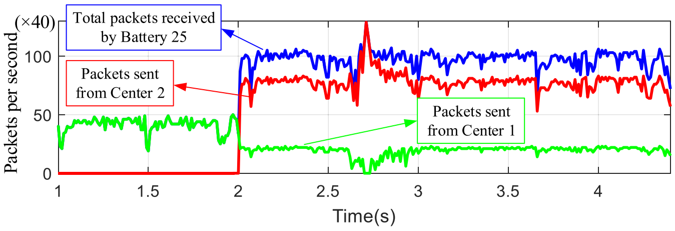
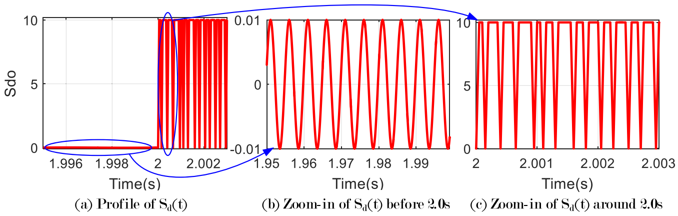


Fig. 6. Case 1: Traffic monitoring (packet received by Battery 25).



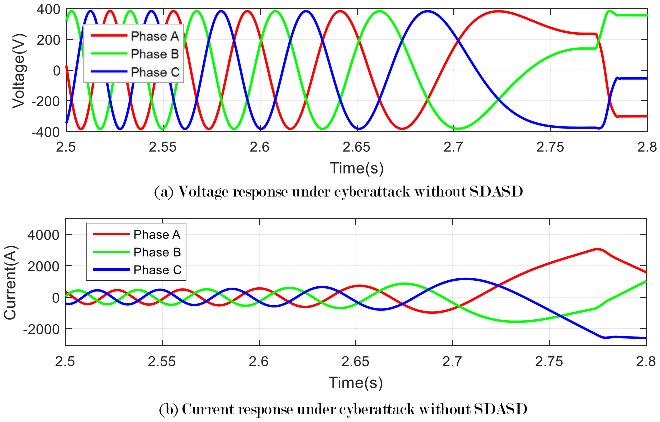
(a) Profile of $S_d(t)$ (b) Zoom-in of $S_d(t)$ before 2.0s (c) Zoom-in of $S_d(t)$ around 2.0s

Fig. 7. Case 1: Probe signal $s_d(t)$ of Battery 25 under cyberattacks.

1) Case1: Cyberattacks Without SDASD: Center 2 is hacked and keeps injecting fake packets in the name of Center 1 with same MAC/IP address. Here we use Scapy [28] to periodically generate those fake packets. Specifically, to manipulate the NM system, at $t = 2.0$ s attacker injects malicious packets with the payload of 10 into the probe signal $s_d(t)$ of Battery 25. It is originally a sinusoidal wave with amplitude $\alpha_d = 0.01$ and frequency $\omega_d = 1256$ rad/s.

When abnormal value of D_{do} is detected, Circuit Breaker 3 is opened at $t = 2.05$ s. Fig. 6 shows the data traffic, where before $t = 2.0$ s, packets are only sent from Center 1, and after $t = 2.0$ s, malicious traffic are added from Center 2. Fig. 7 shows the probe signal received by Battery 25. It can be seen that without SDASD, the malicious traffic significantly affects the normal traffic and more malicious data are received by Battery 25. Fig. 8 shows the voltage and current responses in Microgrid 3, which indicates cyberattacks severely impact NM normal operations and eventually lead to a system collapse.

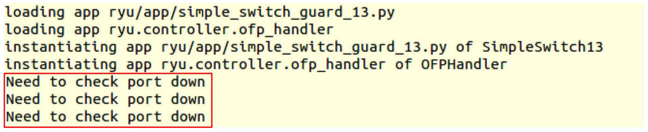
2) Case 2: Cyberattacks Elimination With SDASD: The same cyberattack is launched and in this case SDASD will detect the anomaly in Center 2 and protect the SDN network to guarantee data security. With SDASD, traffic from malicious host will be forwarded to the SDN controller through ***Packet-In*** message and, since there is no ***Port-Down*** message, no flow rules will be added; finally these data packets will be directly discarded. Fig. 9 shows alarm is raised in SDN network. Fig. 10 shows the normal operation of NMs with SDASD.



(a) Voltage response under cyberattack without SDASD

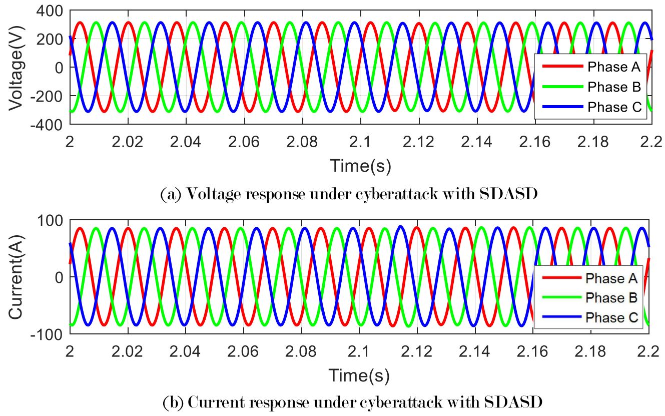
(b) Current response under cyberattack without SDASD

Fig. 8. Case1: Voltage and current responses at bus 25.



```
loading app ryu/app/simple_switch_guard_13.py
loading app ryu.controller.ofp_handler
instantiating app ryu/app/simple_switch_guard_13.py of SimpleSwitch13
instantiating app ryu.controller.ofp_handler of OFPHandler
Need to check port down
Need to check port down
Need to check port down
```

Fig. 9. Case 2: Alarm is raised in an SDN network.



(a) Voltage response under cyberattack with SDASD

(b) Current response under cyberattack with SDASD

Fig. 10. Case 2: Voltage and current responses at bus 25.

From Figs. 7∼10, it can be seen that:

- Without SDASD, malicious packets can be easily injected into SDN network via compromised host, because from SDN controller's viewpoint, data packets are sent out from the same location even though part of the data are actually from the malicious Center 2 as shown in Fig. 6. Therefore, without SDASD, SDN network is vulnerable to host location hijacking cyberattacks. Such attacks will further cause catastrophic collapse in NMs as shown in Fig. 8.
- With SDASD, the NM system is prevented from malicious hijacking attacks. SDASD is able to guarantee reliable operations of NMs under network attacks and avoid possible economic losses of customers.

3) Case 3: Normal NMCC Migration Under SDASD: In this test, we demonstrate a scenario of normal NMCC migration.

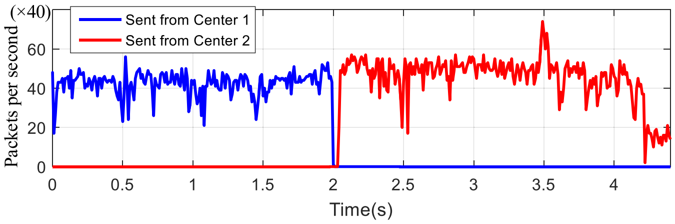


Fig. 11. Case 3: Divert traffic during normal migration process with SDASD.

In this case, NMCC moves from Center 1 to Center 2 at $t = 2.0$ s. ***Port-Down*** message is sent to the SDN controller to pre-update the host profile table, and traffic from Center 1 will stop immediately. When Center 2 is effective, a ***Port-Up*** message is forwarded to the SDN controller, and finish the host profile table update. Correspondingly, the SDN controller will update the flow rules in the switch by installing new rule and removing old rule. Finally, the probe signals will be sent from Center 2 to Battery 25. In this process, the NM system is able to maintain normal operation similar to Fig. 10. Fig. 11 shows the divert traffic during the migration process. From Fig. 11, it can be seen that:

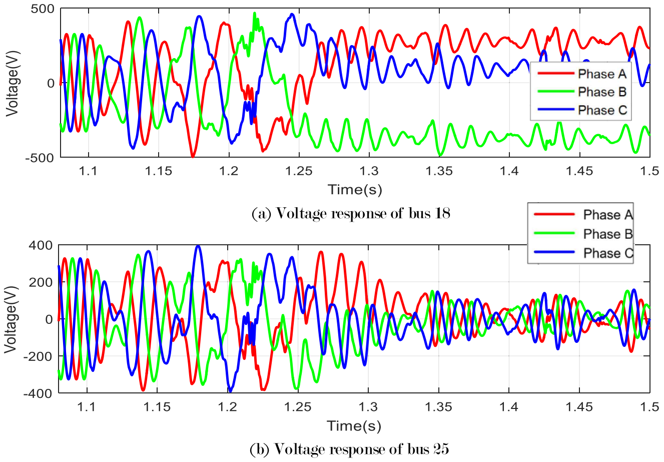
- Before $t = 2.0$ s, the probe signals are sent from Center 1; while after $t = 2.0$ s, they are sent from Center 2 instead. This means NMCC successfully migrates to a new location.
- SDASD is able to guarantee highly reliable host location migration, which is very important for resilient NMs operations due to the frequent topology changes in NMs caused by microgrid islanding and re-connecting.

B. Validation of Active Synchronous Detection of Power Bot Attacks on DER Controllers

As SDASD is capable of guaranteeing the cybersecurity of the SDN network, it is reasonable to assume the probe signals and detection signals are transferred via a secured SDN network. To fully justify the effectiveness of active synchronous detection on power bots, four different cases are given as follows:

1) Case 4: Type I Attack Validation: A type I attack is launched on the inverter inner loop of Battery 18 in Microgrid 2 at $t = 1.10$ s. Two sub-cases are introduced to compare the performance of the test system without or with SDASD. When SDASD is activated, $\alpha_d = \alpha_q = 0.01$ and $\omega_d = \omega_q = 1256$ rad/s. Fig. 12 shows the three-phase voltage responses at buses 18 and 25 before SDASD is applied. Fig. 13 and Fig. 14 illustrate the three-phase voltage and current responses under SDASD protection. Fig. 15 demonstrates the changes of D_{do} in Battery 18. Specifically, the power bot attack is detected via SDASD at $t = 1.108$ s when D_{do} reaches zero, and Circuit Breaker 2 is opened immediately to disconnect Microgrid 2 to isolate the attack.

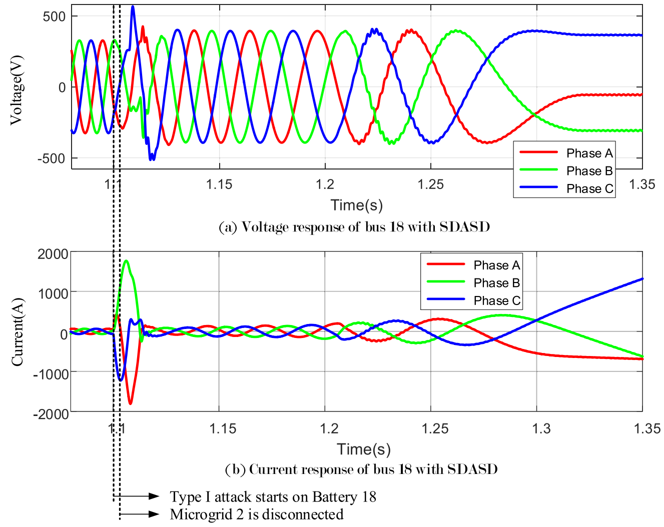
2) Case 5: Type II Attack Validation: A type II attack occurs on the inverter inner loop of Fuel Cell 27 in Microgrid 4 at $t = 1.20$ s, where K_{di} is modified from 0.25 to 10.0. Fig. 16 shows the three-phase voltage responses at buses 27 and 31 when SDASD is disabled. Fig. 17 and Fig. 18 illustrate the



(a) Voltage response of bus 18

(b) Voltage response of bus 25

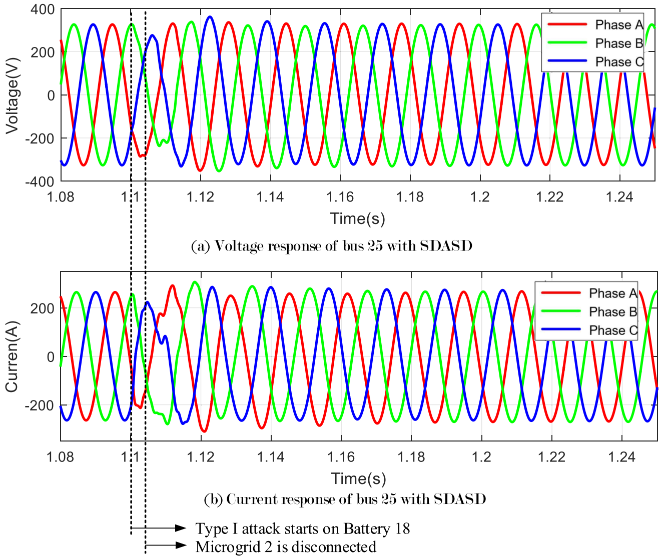
Fig. 12. Case 4: Voltage response of buses 18 and 25 without SDASD.



(a) Voltage response of bus 18 with SDASD

(b) Current response of bus 18 with SDASD

Fig. 13. Case 4: Voltage and current response of bus 18 with SDASD.



(a) Voltage response of bus 25 with SDASD

(b) Current response of bus 25 with SDASD

Fig. 14. Case 4: Voltage and current response of bus 25 with SDASD.

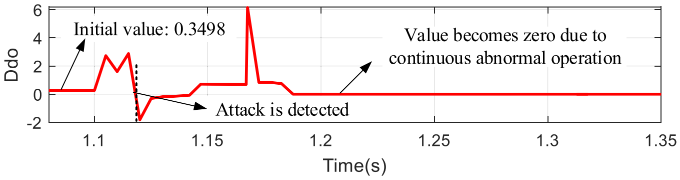
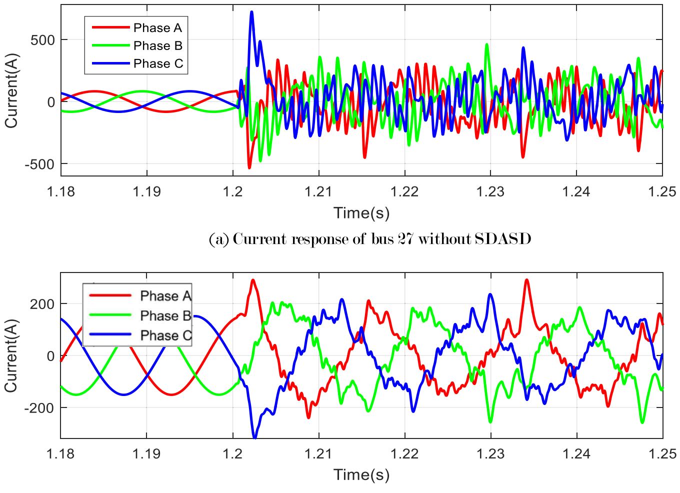


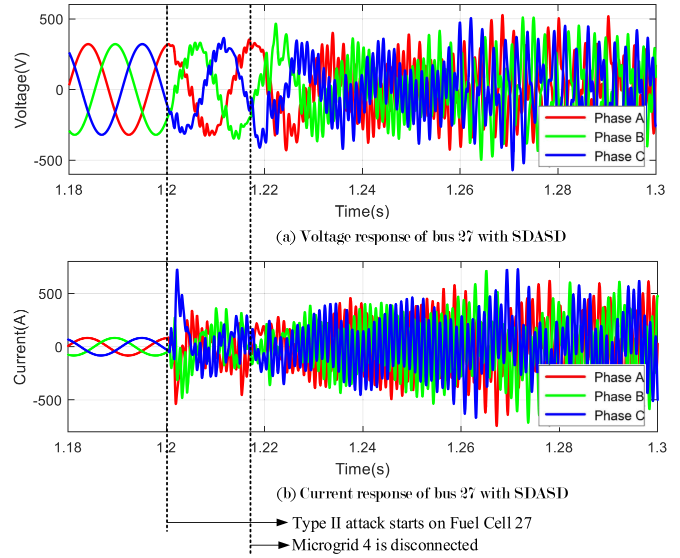
Fig. 15. Case 4: Detection results of D_{do} in Battery 18.



(a) Current response of bus 27 without SDASD

(b) Current response of bus 31 without SDASD

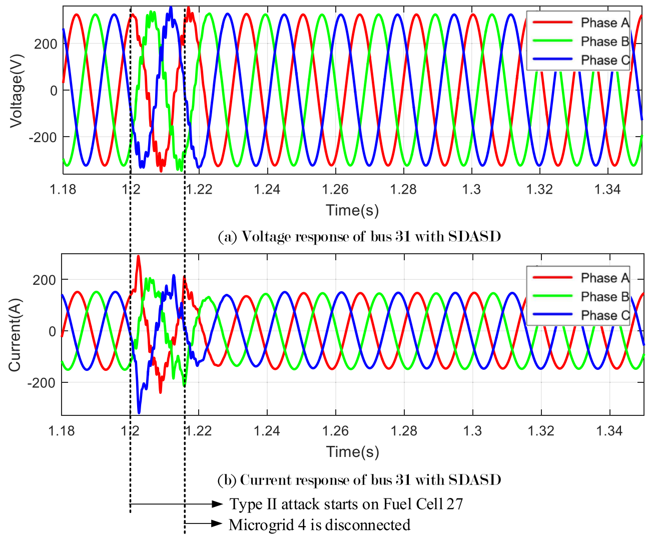
Fig. 16. Case 5: Current response of buses 27 and 31 without SDASD.



(a) Voltage response of bus 27 with SDASD

(b) Current response of bus 27 with SDASD

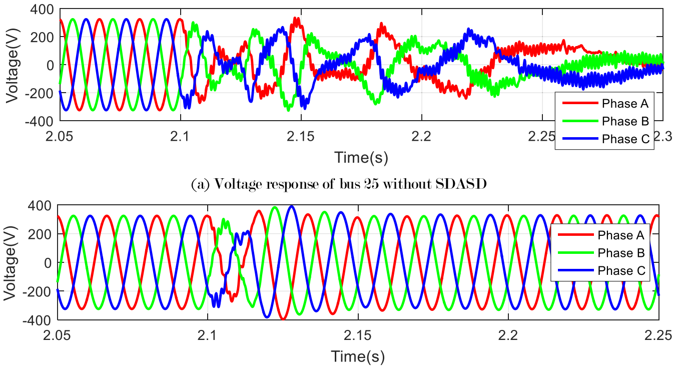
Fig. 17. Case 5: Voltage and current response of the bus 27 with SDASD.



(a) Voltage response of bus 31 with SDASD

(b) Current response of bus 31 with SDASD

Fig. 18. Case 5: Voltage and current response of the bus 31 with SDASD.



(a) Voltage response of bus 25 without SDASD

(b) Voltage response of bus 25 with SDASD

Fig. 19. Case 6: Voltage response of the bus 25 under simultaneous attacks.

three-phase voltage and current responses after SDASD is applied. Specifically, SDASD detects the attack at $t = 1.217$ s and Circuit Breaker 4 is opened immediately to disconnect Microgrid 4 to isolate the attack. Figs. 12∼18 show that:

- Without SDASD, the impact of attack rapidly spread across the interconnected NMs and significantly deteriorate its performance (see Fig. 16).
- With SDASD, the power bot attack is detected and isolated to mitigate its impact on the overall NM system as shown in Fig. 14 and Fig. 18, which validates the effectiveness of SDASD in detecting power bot attacks.
- The actual value of D_{do} before the system attacked is 0.3498 (see Fig. 15) which is proximate to the calculated value 0.35 obtained from (7). It verifies the correctness of the detection rules.
- The value of D_{do} changes to zero in Fig. 15 after Microgrid 2 is disconnected from the NMs system. Seemingly it conflicts with the value shown in Table I after Microgrid 2 is disconnected from the networked system. The reason is that Battery 18 operates abnormally due to attack, whereas Table I only summarizes the steady-state of detection results. In practice, alarm should always be raised once the detection results change significantly, especially when it becomes zero as shown in Table I.

3) Case 6: Simultaneous Attacks at Different Points: A type I attack occurs on the inner loop of Battery 31 at $t = 2.10$ s; simultaneously, a type II attack occurs on the inner loop of PV 35, where K_{di} is modified from 0.25 to 20.0. Fig. 19 illustrates the three-phase voltage responses without and with SDASD. From Fig. 19, it can be seen that SDASD can quickly detect attacks and isolate the compromised system, which validates

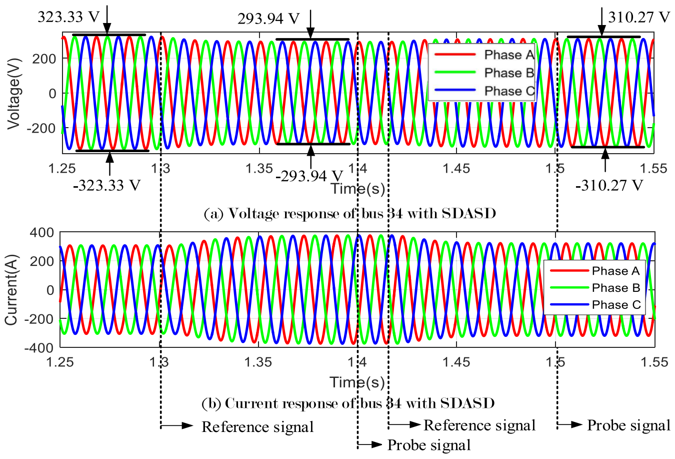


Fig. 20. Case 7: Voltage and current response of the bus 34 with SDASD.

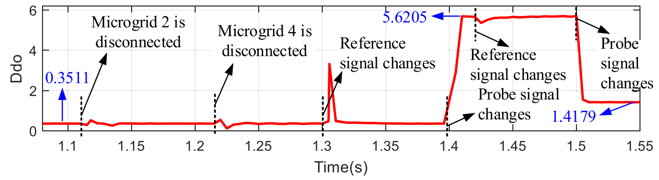


Fig. 21. Case 7: Detection results of D_{do} in Battery 34.

the feasibility of SDASD on protecting NMs from simultaneous attacks at different points.

4) Case 7: Validation of SDASD's Reliability and Robustness: SDASD is expected to be both reliable and robust, which means (1) it does not malfunction under various normal operation conditions; (2) it guarantees correct detection with arbitrarily switched probe signals; and (3) it does not impede NM operations. To demonstrate its reliability and robustness, microgrid operation control signals (e.g. U_{dref} in Fig. 3) and probe signals $s(t)$ are adjusted online through NMCC. Specifically, the voltage magnitude reference signal of Battery 34 in Microgrid 6 is adjusted from 0.99 p.u. to 0.90 p.u. (i.e., from 323.33 V to 293.94 V) at $t = 1.30$ s, and further adjusted to 0.95 p.u. (i.e., 310.27 V) at $t = 1.42$ s. The amplitude of the probe signal $s_d(t)$ is adjusted from 0.01 to 0.04 at $t = 1.40$ s, and further adjusted to 0.02 at $t = 1.50$ s. Fig. 20 shows the three-phase voltage and current responses with SDASD, and Fig. 21 illustrates the changes of D_{do} in Battery 34. From Figs. 20∼21, it can be observed that:

- DERs can be effectively dispatched corresponding to the changes of control signals. Such changes have no effect on the detection results, as illustrated in the test results during [1.30 s, 1.40 s]. Therefore, SDASD can accurately distinguish normal control operations from cyberattacks. It verifies SDASD is a reliable solution for protecting NMs.
- As seen from Fig. 21, when the amplitude of the probe signal quadruples from 0.01 to 0.04 at $t = 1.40$ s, the detection result will change from 0.3511 to 5.6205 which is 16 times of 0.3511. And when the amplitude of the probe signal halves from 0.04 to 0.02 at $t = 1.50$ s, the detection result will change from 5.6205 to 1.4179 which is 25% of 5.6205. The detection results thus are coincident with the detection rules derived in Table I.
- When the probe signal is adjusted online, the NMs system maintains its normal operations as shown at $t = 1.40$ s and $t = 1.50$ s in Fig. 20. It indicates SDASD is dependable and has zero footprint on a secured system.

Overall, SDASD is a 'non-infrastructure' solution because it neither modifies the NM physical infrastructure nor causes any disturbances on the NM states.

VI. Conclusion

A Software-Defined Active Synchronous Detection (SDASD) method is contributed in this paper to detect and mitigate both cyberattacks on SDN network and power bot attacks on NMs. By devising a ***HostStatus_Checker***, the host tracking service is well designed in SDN controller to defend against host location hijacking attacks on the SDN cyber layer. Active synchronous detection technology is further developed to detect and localize power bot attacks on the physical NMs. Case studies on a typical NM system have confirmed the efficacy and reliability of SDASD in protecting NMs from cyber-physical attacks.

Appendix I
Derivations of (7) and (9)

According to (4), when $s(t)$ refers to the probe signals $s_d(t)$, and $c(t)$ corresponds to control signals I_{dref}, the attack detection function of D_{do} can be expressed as:

$$D_{do} = \frac{1}{\mathrm{T}}\int_t^{t+\mathrm{T}} s_d(t)\cdot I_{\mathrm{dref}}dt. \tag{11}$$

Since Fig. 3 shows that I_{dref} can be further expressed as:

$$I_{\mathrm{dref}} = (U_{\mathrm{dref}} - U_d + s_d(t))\cdot K_{do}\left(1 + \frac{1}{T_{do}s}\right). \tag{12}$$

Then, by using (12), D_{do} can be rewritten as:

$$\begin{aligned} D_{do} &= \frac{1}{\mathrm{T}}\int_t^{t+\mathrm{T}} s_d(t)\cdot(U_{\mathrm{dref}} - U_d + s_d(t))\cdot K_{do}\left(1 + \frac{1}{T_{do}s}\right)dt \\ &= \frac{1}{\mathrm{T}}\int_t^{t+\mathrm{T}} s_d(t)\cdot U_{\mathrm{dref}}\cdot K_{do}\left(1 + \frac{1}{T_{do}s}\right)dt \\ &\quad - \frac{1}{\mathrm{T}}\int_t^{t+\mathrm{T}} s_d(t)\cdot U_d\cdot K_{do}\left(1 + \frac{1}{T_{do}s}\right)dt \\ &\quad + \frac{1}{\mathrm{T}}\int_t^{t+\mathrm{T}} s_d^2(t)\cdot K_{do}\left(1 + \frac{1}{T_{do}s}\right)dt. \end{aligned} \tag{13}$$

Since the first two terms of the above integration are zero, D_{do} can be expressed as:

$$\begin{aligned} D_{do} &= \frac{1}{\mathrm{T}}\int_t^{t+\mathrm{T}} \alpha_d^2\sin^2(\omega_d t)\cdot K_{do}\left(1 + \frac{1}{T_{do}s}\right)dt \\ &= \frac{\alpha_d^2}{2}\cdot K_{do}\left(1 + \frac{1}{T_{do}s}\right). \end{aligned} \tag{14}$$

TABLE II
LINE IMPEDANCES BETWEEN NODES IN FIG. 4

Subsystems	From	To	$R(\Omega/km)$	$L(H/km)$	Length (m)
Microgrid 1	3	4	0.2840	$0.2202e-3$	35
	3	13	0.2840	$0.2202e-3$	35
	4	14	3.6900	$0.2493e-3$	30
	14	15	3.6900	$0.2493e-3$	30
	15	16	3.6900	$0.2493e-3$	30
Microgrid 2	17	18	1.3800	$0.2175e-3$	30
	18	19	1.3800	$0.2175e-3$	30
	19	20	1.3800	$0.2175e-3$	30
Microgrid 3	21	22	0.4970	$0.2281e-3$	30
	22	23	0.4970	$0.2281e-3$	30
	23	24	0.4970	$0.2281e-3$	30
	24	25	0.8220	$0.2042e-3$	30
Microgrid 4	26	27	0.8710	$0.2149e-3$	30
	27	28	0.8710	$0.2149e-3$	30
	28	29	0.8710	$0.2149e-3$	30
Microgrid 5	30	31	3.6900	$0.2493e-3$	30
Microgrid 6	32	33	1.3800	$0.2175e-3$	30
	33	34	1.3800	$0.2175e-3$	30
	34	35	1.3800	$0.2175e-3$	30
Backbone	5	6	0.2840	$0.2202e-3$	35
	7	8	0.2840	$0.2202e-3$	35
	8	9	0.2840	$0.2202e-3$	35
	9	10	0.2840	$0.2202e-3$	35
	10	11	0.2840	$0.2202e-3$	35
	11	12	0.2840	$0.2202e-3$	35

When the sinusoidal signal $s_d(t)$ has a large frequency, the above expression can be simplified as:

$$D_{do} = \frac{\alpha_d^2 \cdot K_{do}}{2}. \tag{15}$$

Similarly, the detailed derivations of (9) is given in (16) as follows:

$$\begin{aligned} D_{di} &= \frac{1}{\mathrm{T}} \int_t^{t+\mathrm{T}} s_d(t) \cdot V_{d\mathrm{ref}} dt \\ &= \frac{1}{\mathrm{T}} \int_t^{t+\mathrm{T}} s_d(t) \cdot \left\{ (I_{d\mathrm{ref}} - I_d) \cdot K_{di} \left(1 + \frac{1}{T_{di} s}\right) + I_d R \right. \\ &\quad \left. - \, I_q L + V_d \right\} dt \\ &= \frac{1}{\mathrm{T}} \int_t^{t+\mathrm{T}} s_d(t) \cdot I_{d\mathrm{ref}} \cdot K_{di} \left(1 + \frac{1}{T_{di} s}\right) dt \\ &= \frac{1}{\mathrm{T}} \int_t^{t+\mathrm{T}} s_d(t) \cdot (U_{d\mathrm{ref}} - U_d + s_d(t)) \cdot K_{do} \left(1 + \frac{1}{T_{do} s}\right) \\ &\quad \cdot K_{di} \left(1 + \frac{1}{T_{di} s}\right) dt \\ &= \frac{\alpha_d^2 \cdot K_{do} \cdot K_{di}}{2} \left(1 - \frac{1}{T_{do} T_{di} \omega_d^2}\right). \end{aligned} \tag{16}$$

APPENDIX II
DETAILS OF NETWORKED MICROGRIDS IN FIG. 4

The line impedances of each microgrid in Fig. 4 are given in Table II. And the power load and DER generation at each node are summarized in Table III and Table IV, respectively.

TABLE III
POWER LOADS AT EACH BUS IN FIG. 4

Bus	P_n (kW)	Q_n (kVAR)	Bus	P_n (kW)	Q_n (kVAR)
4	42.75	26.34	25	61.15	37.90
14	61.15	37.90	28	72.75	46.34
17	42.75	26.34	31	62.75	57.91
23	61.15	37.90	33	40.00	24.77

TABLE IV
DER GENERATION AT EACH BUS IN FIG. 4

Bus	P_n (kW)	Q_n (kVAR)	Bus	P_n (kW)	Q_n (kVAR)
13	98.15	64.02	27	39.70	0.00
16	7.31	0.02	29	30.00	0.76
18	17.45	25.76	31	69.40	30.50
20	39.68	0.00	34	1.65	148.48
25	124.98	30.64	35	22.43	0.50

ACKNOWLEDGMENT

The authors would like to thank Professor Bing Wang at University of Connecticut for her contributions to Sections II and III. In particular, the first author would like to thank Professor Wang for providing supports on SDN technologies.

REFERENCES

[1] Y. Li, P. Zhang, and P. B. Luh, "Formal analysis of networked microgrids dynamics," *IEEE Trans. Power Syst.*, vol. 33, no. 3, pp. 3418–3427, May 2018.

[2] Y. Li, P. Zhang, and M. Yue, "Networked microgrid stability through distributed formal analysis," *Appl. Energy*, vol. 228, pp. 279–288, 2018.

[3] Y. Li, P. Zhang, M. Althoff, and M. Yue, "Distributed formal analysis for power networks with deep integration of distributed energy resources," *IEEE Trans. Power Syst.*, Oct. 2018, to be published.

[4] D. Kreutz, F. M. Ramos, P. E. Verissimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-defined networking: A comprehensive survey," *Proc. IEEE*, vol. 103, no. 1, pp. 14–76, Jan. 2015.

[5] L. Ren, Y. Qin, B. Wang, P. Zhang, P. B. Luh, and R. Jin, "Enabling resilient microgrid through programmable network," *IEEE Trans. Smart Grid*, vol. 8, no. 6, pp. 2826–2836, Nov. 2017.

[6] L. Ren *et al.*, "Enabling resilient distributed power sharing in networked microgrids through software defined networking," *Appl. Energy*, vol. 210, pp. 1251–1265, 2018.

[7] M. Dabbagh, B. Hamdaoui, M. Guizani, and A. Rayes, "Software-defined networking security: Pros and cons," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 73–79, Jun. 2015.

[8] S. Hong, L. Xu, H. Wang, and G. Gu, "Poisoning network visibility in software-defined networks: New attacks and countermeasures," in *Proc. Netw. Distrib. Syst. Secur.*, vol. 15, 2015, pp. 8–11.

[9] H. Farhady, H. Lee, and A. Nakao, "Software-defined networking: A survey," *Comput. Netw.*, vol. 81, pp. 79–95, 2015.

[10] A. Khurshid, W. Zhou, M. Caesar, and P. Godfrey, "Veriflow: Verifying network-wide invariants in real time," in *Proc. 1st Workshop Hot Topics Softw. Defined Netw.*, 2012, pp. 49–54.

[11] S. Al-Haj and W. J. Tolone, "Flowtable pipeline misconfigurations in software defined networks," in *Proc. IEEE Conf. Comput. Commun. Workshops*, 2017, pp. 247–252.

[12] S. Shin, V. Yegneswaran, P. Porras, and G. Gu, "Avant-guard: Scalable and vigilant switch flow management in software-defined networks," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2013, pp. 413–424.

[13] 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 *Proc. Netw. Distrib. Syst. Secur.*, 2013, pp. 1–16.

[14] D. Kreutz, J. Yu, F. Ramos, and P. Esteves-Verissimo, "Anchor: Logically-centralized security for software-defined networks," 2017, arXiv:1711.03636.

[15] S. Lee, C. Yoon, C. Lee, S. Shin, V. Yegneswaran, and P. Porras, "Delta: A security assessment framework for software-defined networks," in *Proc. Netw. Distrib. Syst. Secur.*, vol. 17, 2017, pp. 1–15.

[16] Y. Li, P. Zhang, L. Zhang, and B. Wang, "Active synchronous detection of deception attacks in microgrid control systems," *IEEE Trans. Smart Grid*, vol. 8, no. 1, pp. 373–375, Jan. 2017.

[17] N. McKeown *et al.*, "Openflow: Enabling innovation in campus networks," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 38, no. 2, pp. 69–74, 2008.

[18] C. Wang, Y. Li, K. Peng, B. Hong, Z. Wu, and C. Sun, "Coordinated optimal design of inverter controllers in a micro-grid with multiple distributed generation units," *IEEE Trans. Power Syst.*, vol. 28, no. 3, pp. 2679–2687, Aug. 2013.

[19] Y. Li, P. Zhang, L. Ren, and T. Orekan, "A Geršgorin theory for robust microgrid stability analysis," in *Proc. IEEE Power Energy Soc. General Meeting*, 2016, pp. 1–5.

[20] E. Robles, S. Ceballos, J. Pou, J. L. Martin, J. Zaragoza, and P. Ibanez, "Variable-frequency grid-sequence detector based on a quasi-ideal low-pass filter stage and a phase-locked loop," *IEEE Trans. Power Electron.*, vol. 25, no. 10, pp. 2552–2563, Oct. 2010.

[21] J. M. Guerrero, J. C. Vasquez, J. Matas, L. G. De Vicuña, and M. Castilla, "Hierarchical control of droop-controlled ac and dc microgrids—A general approach toward standardization," *IEEE Trans. Ind. Electron.*, vol. 58, no. 1, pp. 158–172, Jan. 2011.

[22] D. G. Holmes and T. A. Lipo, *Pulse Width Modulation for Power Converters: Principles and Practice*, vol. 18. Hoboken, NJ, USA: Wiley, 2003.

[23] A. Hussein, I. H. Elhajj, A. Chehab, and A. Kayssi, "SDN security plane: An architecture for resilient security services," in *Proc. IEEE Int. Conf. Cloud Eng. Workshop*, 2016, pp. 54–59.

[24] S. Scott-Hayward, G. O'Callaghan, and S. Sezer, "SDN security: A survey," in *Proc. IEEE SDN Future Netw. Services*, 2013, pp. 1–7.

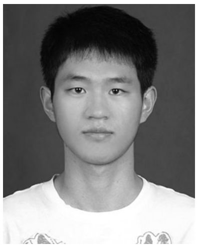
[25] F. Tomonori, "Introduction to Ryu SDN framework," *Open Networking Summit*, pp. 1–14, 2013.

[26] M.-H. Wang, P.-W. Chi, J.-W. Guo, and C.-L. Lei, "SDN storage: A stream-based storage system over software-defined networks," in *Proc. IEEE Conf. Comput. Commun. Workshops*, 2016, pp. 598–599.

[27] P. Chithaluru and R. Prakash, "Simulation on SDN and NFV models through mininet," in *Innov. Softw.-Defined Netw. Netw. Functions Virtualization*, 2018, pp. 149–174.

[28] R. Montante, "Using scapy in teaching network header formats: Programming network headers for non-programmers," in *Proc. 49th ACM Tech. Symp. Comput. Sci. Educ.*, 2018, p. 1106.

Yan Li (M'18) received the B. Sc. and M. Sc. degrees in electrical engineering from Tianjin University, Tianjin, China, and the Ph.D. degree in electrical engineering from the University of Connecticut, Storrs, CT, USA, in 2008, 2010, and 2018, respectively. Her research interests include microgrids and networked microgrids, formal analysis, power system stability and control, software-defined networking, and cyber-physical security.



Yanyuan Qin received the B.S. degree in automation from the Nanjing University of Aeronautics and Astronautics, Nanjing, China, and the M.S. degree in control science and engineering from Shanghai Jiao Tong University, Shanghai, China, in 2011 and 2014, respectively. He is currently working toward the Ph.D. degree with the Computer Science and Engineering Department, University of Connecticut, Storrs, CT, USA. His research interests include software-defined networking and wireless networks.

Peng Zhang (M'07–SM'10) received the Ph.D. degree in electrical engineering from the University of British Columbia, Vancouver, BC, Canada, in 2009. He is currently working as the Centennial Chair Professor and the Associate Professor of electrical engineering with the University of Connecticut, Storrs, CT, USA. He was a System Planning Engineer at BC Hydro and Power Authority, Vancouver, Canada. His research interests include microgrids, power system stability and control, cyber security, and smart ocean systems.

He is an individual member of CIGRÉ. He is an Editor for the IEEE TRANSACTIONS ON POWER SYSTEMS and the IEEE POWER AND ENERGY SOCIETY LETTERS and an Associate Editor for the IEEE JOURNAL OF OCEANIC ENGINEERING and the IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS.

Amir Herzberg received the Ph.D. degree in computer science from Technion, Israeli Institute of Technology, Haifa, Israel, in 1991.

From 1991 to 1995, he was with the IBM T. J. Watson Research Center, where he was a Research Staff Member and the Manager of the Network Security research group. From 1996 to 2000, he was the Manager of e-Business and Security Technologies with the IBM Haifa Research Lab. From 2002 to 2017, he was the Faculty of the Bar Ilan University, Ramat Gan, Israel. He is Chair of the Comcast Center for Excellence for Security Innovation with the University of Connecticut, Storrs, CT, USA. He worked for many years in different areas of cybersecurity, in both industry and academia, mostly with IBM Research and Bar Ilan University. He has authored and coauthored more than 150 research papers, five book chapters, and 24 patents. His research interests include broad areas of cybersecurity, including network security, applied cryptography, security of cyber-physical systems, and usable security.

Dr. Herzberg has served on technical program committees of more than 40 conferences and delivered keynote and plenary addresses on cybersecurity at ten conferences and organized multiple professional events. He is the Co-Chair of the TPC of the IEEE CNS conference, in 2019.