IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received June 26, 2020, accepted July 8, 2020, date of publication July 15, 2020, date of current version July 28, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3009611

Prosumer Nanogrids: A Cybersecurity Assessment

YOUSIF DAFALLA[1], BO LIU[2], (Graduate Student Member, IEEE), DALTON A. HAHN[1], HONGYU WU[2], (Senior Member, IEEE), REZA AHMADI[1], (Member, IEEE), AND ALEXANDRU G. BARDAS[1]

[1]Department of Electrical Engineering and Computer Science, The University of Kansas, Lawrence, KS 66045, USA
[2]Department of Electrical and Computer Engineering, Kansas State University, Manhattan, KS 66506, USA

Corresponding author: Yousif Dafalla (yousif.dafalla@ku.edu)

This work was supported by the National Science Foundation under Grant 1850406.

ABSTRACT Nanogrids are customer deployments that can generate and inject electricity into the power grid. These deployments are based on behind-the-meter renewable energy resources and are labeled as ''prosumer setups'', allowing customers to not only consume electricity, but also produce it. A residential nanogrid is comprised of a physical layer that is a household-scale electric power system, and a cyber layer that is used by manufacturers and/or grid operators to remotely monitor and control the nanogrid. With the increased penetration of renewable energy resources, nanogrids are at the forefront of a paradigm shift in the operational landscape and their correct operation is vital to the electric power grid. In this paper, we perform a cybersecurity assessment of a state-of-the art residential nanogrid deployment. For this purpose, we deployed a real-world experimental nanogrid setup that is based on photovoltaic (PV) generation. We analyzed the security and the resiliency of this system at both the cyber and physical layers. While we noticed improvements in the cybersecurity measures employed in the current nanogrid compared to previous generations, there are still major concerns. Our experiments show that these concerns range from exploiting well-known protocols, such as Secure Shell (SSH) and Domain Name Service (DNS), to the leakage of confidential information, and major shortcomings in the software updating mechanism. While the compromise of multiple nanogrids can have a negative effect on the entire power grid, we focus our analysis on individual households and have determined through Simulink-based simulations the economic loss of a compromised deployment.

INDEX TERMS Cyber-attacks, cyber-physical systems, cybersecurity, distributed energy resources, CPS gateway, microgrids, nanogrids, prosumers, photovoltaic (PV) systems.

I. INTRODUCTION

The operational landscape of the power grid is undergoing a radical transformation with the increased penetration of renewable energy systems. According to the United States Department of Energy [1], we are witnessing a paradigm shift from the traditional one-way power consumers to the more involved energy prosumers. A *prosumer* is an entity that both produces and consumes energy. Prosumer deployments are slowly becoming foundational elements of the power grid in the United States, as more Americans generate their own power from distributed energy resources. These prosumer setups inject power back into the grid and, therefore, affect the operation and reliability of the entire system [2]. Prosumer deployments are often viewed as microgrids, nanogrids, or even picogrids. According to Nordman [3], a microgrid is an electricity distribution system that is under the control of a single management entity. A microgrid contains loads, distributed energy resources and/or storage devices that can be operated in a controlled and coordinated way while isolated from any utility grid. On the other hand, a nanogrid is a single house, building or business that has some load, generation and/or storage capability. Finally, a picogrid is a single device that uses its own internal battery for operation in the absence of external power sources. While in some communities these terms are used in an interchangeable manner, it is more cautious to consider prosumer deployments as nanogrids, since a nanogrid implies a small microgrid for a single home or building while picogrids are often used to refer to individual devices [3].

Prosumer deployments, referred to as *nanogrids* hereinafter, are made up of a physical layer that consists of a

The associate editor coordinating the review of this manuscript and approving it for publication was Canbing Li.

small-scale electric power generation system and a cyber layer for the necessary supervisory functions. The cyber layer of the nanogrid allows power system operators to remotely monitor and control the physical layer and coordinate the nanogrid's energy interactions with the power distribution system (e.g., remote microinverter upgrades to enable grid integration [4]). The interconnection between the physical and cyber layer of the nanogrid is performed using cyber-physical system (CPS) gateways. These devices enable the physical layer of the nanogrid to be managed by grid operators through remote servers over the internet. Figure 1 pictures a typical nanogrid deployment with its associated physical and cyber layers.

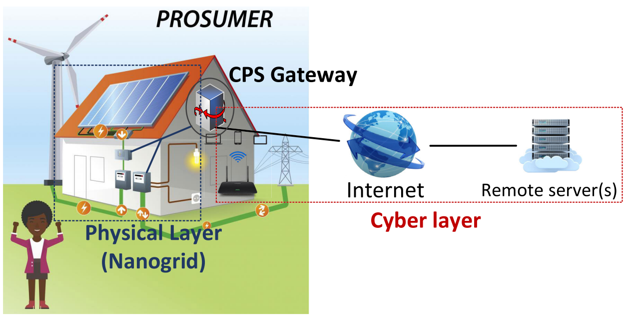


FIGURE 1. Prosumer deployment (nanogrid) – A prosumer environment adds the generation capability to the consumer, transforming the power grid into a "two-way street". The CPS gateway is the interface between the physical and the cyber layer in a prosumer setup. (Adapted from US Energy Dept., "Graphic by Sarah Harman" [1]).

This inter-connectivity between the physical and the cyber layers increases flexibility and offers unprecedented grid monitoring and management capabilities to grid operators. On the other hand, it also introduces a new set of challenges by exposing the nanogrids to new types of threats. Attacks can now come from within the household or remotely through the cyber layer. Recent efforts such as [5]–[12] have revealed major cybersecurity shortcomings in nanogrid deployments that have the potential to result in severe consequences for the households and the power grid alike.

In this paper we take a unified perspective by assessing attacks on both the physical and cyber layers of a residential PV based nanogrid deployment in the presence of a powerful (but realistic) adversary. For this purpose we deployed a state-of-the-art residential nanogrid deployment based on photo-voltaic (PV) generation. We evaluated the current security status of this deployment and report on our efforts to perform a few successful attacks. We then demonstrate the extended consequences of such attacks using Simulink simulations to determine the economic ramifications for compromised households. While we noticed security-related improvements compared to the previous generations of PV-based nanogrids (e.g., [6]–[12]), our work exposes a new set of major security concerns, such as the ability to intercept SSH passwords and perform DNS hijacking attacks, "security through obscurity" inspired approaches, the leakage of private information, and a flawed software updating mechanism. The main contributions of this paper can be summarized as follows:

- Present a cybersecurity assessment on a widely used, real-world, state-of-the-art (as of 2019-2020) PV-based nanogrid deployment. We identified several shortcomings and were able to exploit the SSH and DNS services as well as the software updating mechanism of the deployment.
- Expose the leakage of sensitive information pertaining to the nanogrid deployment as well as "security through obscurity" inspired approaches employed in the nanogrid to address confidentiality and integrity concerns (e.g., "home-brewed"/proprietary encryption algorithms and clear-text device information).
- Assess the consequences for a household if the identified nanogrid vulnerabilities were to be exploited. We evaluate the economic loss for a household that results from an attacker being able to locally or remotely manipulate the physical layer settings of the PV-based nanogrid.

The remainder of the paper is organized as follows: Section II covers the background information on PV-based nanogrid deployments followed by related work in Section III. Next, Section IV describes the threat model while our testbed and the performed experiments are presented in Sections V, VI, and VII. The paper concludes with Sections VIII and IX, discussion and our conclusions.

II. BACKGROUND

Installed residential PV systems have grown rapidly in the past decade, and are predicted to reach 3 million by 2021 and 4 million by 2023 according to [13].

A typical residential PV generation nanogrid is illustrated in Figure 2, and is comprised of the physical devices and connections, alongside the CPS gateway with the communication links. This nanogrid can be viewed as a small-scale power system with generation, storage, and consumption, which is also coupled to the distribution system. The physical layer of the nanogrid consists of PV modules, microinverters, energy storage systems (batteries), household loads, and monitoring and control devices such as sensing equipment, relays, fuses, etc. In most modern residential PV systems, PV modules are individually connected to the nanogrid using microinverters (also known as smart inverters). Microinverters are used to convert the DC current output of solar panels to grid compliant AC current, allowing the nanogrid to interact with the power grid. The power generated by PV modules can be consumed by household loads, stored in an energy storage unit, or injected into the power grid.

Previously, the amount of injected energy by the nanogrids was unnoticeable and didn't impact the performance of the main power grid. However, due to the recent increased penetration of nanogrids, the amount and parameters influencing their power injection to the grid must be carefully monitored and controlled to maintain grid stability [2]. These requirements for additional monitoring and control lead to the adoption of microinverters with two-way-communication

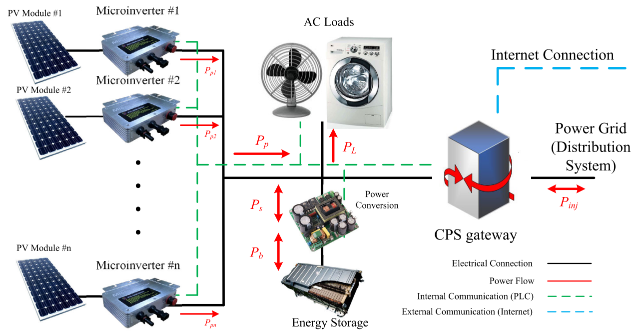


FIGURE 2. PV nanogrid deployment with PV generation, storage, and the CPS gateway – The microinverters interface the PV modules to the household AC power system. The power generated by the PV modules can be consumed locally, stored, or injected to the grid. The CPS gateway monitors and controls the physical devices based on the directives received from the grid operator and/or the nanogrid owner.

capabilities. This two-way-communication connectivity is typically realized through cyber physical system gateways.

The microinverters are directly connected over the local network to the CPS gateway. The CPS gateway faces the ''outside world'' through the internet and facilitates the communication between the physical layer of the nanogrid and external entities. In other words, it allows for remote control of the nanogrid based on the directives received from the manufacturer and/or system operator. Moreover, it reports back the system health and performance data of the solar panels to remote servers [2], [14]. It is also important to note that the CPS gateway can be incorporated into an environment where a Home Energy Management System (HEMS) is installed. In that case, the CPS gateway will be responsible for gathering and aggregating the solar panel performance data and forwarding it to the HEMS controller. For example, the CPS gateway is equivalent to the Renewable Energy Gateway (REG) that is part of the HEMS architecture described by Han *et al.* [15].

Popular examples of CPS gateways for PV systems, include Tigo's MMU, APsystems ECU, and Outback Mate [16]–[18]. The CPS gateway, referred to as *gateway* hereinafter, communicate with the physical nanogrid devices over a local network, often using power line communication (PLC) and/or Ethernet, and face the internet using a broadband connection available through the residential home network. This way, the manufacturer and/or the system operator can monitor and control the operations of a large number of nanogrids collectively, from a remote location. The gateways reside on customer's internet-connected homes and, due to privacy concerns, the power company or the deployment vendor/manufacturer cannot control and restrict a customer's home network. Thus, gateway devices sit on home networks shared with multiple other devices such as computers, phones, tablets, and various other Internet-of-Things (IoT) devices that may be compromised. Leveraging these devices to compromise gateways may lead to endangering the operation of the physical and cyber layers of the nanogrid. The nanogrid is then vulnerable to exploitation by adversaries, with the potential to disturb the operation of individual households' power systems or even the entire operation of the electric distribution system.

III. RELATED WORK

In recent years, several efforts have been devoted to characterize the cybersecurity risks plaguing nanogrid deployments. For instance, [6] was able to uncover various vulnerabilities in SMA PV systems [19] that enabled them to disconnect smart inverters remotely over the internet. Furthermore, they stated that manipulating these PV systems may lead to large scale attacks on the power grid that may cause blackouts [6], [11]. Other efforts such as [7]–[10], [20] also managed to discover vulnerabilities in either the physical or the cyber layer of PV generation systems. However, all these works either exposed well-known confidentiality and integrity concerns (e.g., plain-text passwords sent over the network) or emphasized the lack of proper authentication and authorization mechanisms. Moreover, these efforts have a singular focus, where they examined either the physical layer or the cyber layer of the nanogrid deployment. Our work provides a unified perspective on both the cyber and physical layers of the nanogrid deployment. On the other hand, [12] evaluated the resiliency of wind farms to cyber-attacks. This work discovered vulnerabilities in wind farm control systems and the capability to control wind turbines remotely [12]. Our work differs in that we focused on assessing residential PV generation systems, which have similar cyber layer concerns, but an entirely different physical layer setup.

The Smart Inverter Working Group (SIWG) [31] has proposed three high-level phases for the development of advanced inverter functionalities to reduce the risks of high penetrations of distributed energy resources (DERs). Phase 1 captures the inverters' autonomous functions, while phases 2 and 3 examine DER communication protocols and any additional advanced inverter functionalities. Additionally, Soyoye and Stefferud [21] explored from a high-level perspective the cybersecurity risks (e.g., overall information disclosure) associated with all these three SIWG phases. On the other hand, Jacobs *et al.* [22] discussed the communications needed by DERs to support their system interoperability objectives, as well as the implications of securing these communications. Furthermore, Stamber *et al.* [23] briefly explained potential gaps between manufacturers and policy makers in regards to implementing secure and reliable DER deployments. Sebastian and Hahn [24] described the cyber-physical risks of consumer-grade DER devices that are connected to the network and could be exploited by remote adversaries. Along the same lines, Gholami *et al.* [25] simulated the impact of attacks such as denial of service, bias injection, and replay attacks on the performance of DER. Overall, these studies emphasized mostly from a high-level perspective the unique cybersecurity challenges and risks emerging from the increased penetration of DER devices and how this can

TABLE 1. Related literature comparison – This table highlights the similarities and differences between our work and previous related work. Our/this work performs a cyber and physical layer assessment of a real-world residential PV-based nanogrid deployment. We identified the risks and underlying vulnerabilities in this deployment and propose a set of attack detection and mitigation strategies.

Reference	Real-world Deployment	Cyber-layer Assessment	Physical-layer Assessment	Risks Identification	Attack Detection and Mitigation
Our/This Work	Yes	Yes	Yes	Yes	Yes
Westerhof et al. [6]	Yes	Yes	No	Yes	No
Bret-Mounet et al. [7]	Yes	Yes	No	Yes	No
TUV Rienlad [8]	Yes	Yes	No	Yes	No
Sanson et al. [9]	Yes	No	Yes	No	No
Carter et al. [10]	Yes	Yes	No	Yes	No
Staggs et al. [12]	Yes	Yes	No	Yes	No
Kang et al. [20]	No	Yes	Yes	Yes	No
Soyoye et al. [21]	No	Yes	No	Yes	No
Jacobs et al. [22]	No	Yes	No	Yes	No
Stamber et al. [23]	No	No	No	Yes	No
Sebastian et al. [24]	No	Yes	No	Yes	No
Gholami et al. [25]	No	Yes	No	Yes	Yes
Johnson [26]	No	Yes	No	No	Yes
Lai et al. [27]	No	Yes	No	No	Yes
R.S. de Carvalho et al. [28]	No	Yes	No	No	Yes
Ravikumar et al. [29]	No	Yes	No	Yes	No
Qi et al. [30]	No	Yes	No	Yes	Yes

impact the performance of the grid. Similarly, our work focuses on identifying the cybersecurity risks in residential DER deployments but analyzes these risks on an actual real-world residential PV-based DER deployment.

Previous efforts also introduced multiple frameworks, architectures, and recommendations for protecting DER deployments. Johnson [26] provided a five-year road map for improving the cybersecurity of communication-enabled PV systems. The road map also includes roles for all involved stakeholders in establishing cyber-secure PV networks. Also, Lai *et al.* [27] introduced a set of cybersecurity recommendations for DER interoperability and proposed several cybersecurity requirements and risk management procedures for DER aggregators, vendors, and grid operators. On the same note, de Carvalho and Saleem [28] described current industry's best practices related to DER cybersecurity and discussed conceptual high-level functionalities such as hardening the operating system, firmware update rollback, and password management. Ravikumar *et al.* [29] further introduced a high-fidelity simulated DER CPS security testbed architecture, that can be used for analyzing the grid impacts from cyber-attacks. Furthermore, Qi *et al.* [30] established a generalized attack-resilient framework to protect heterogeneous DER devices from malicious cyber-attacks, ensuring the reliable and stable operation of the smart grid. While these works focused on conceptual solutions for protecting a wide range of DER devices, our work focuses on identifying current cybersecurity challenges in real-world residential PV-based DER deployments. Table 1 summarizes the similarities and differences between our work and previous related works.

IV. THREAT MODEL

A nanogrid setup is hosted in a private household and leverages the household's broadband internet connection. Due to obvious privacy concerns, utilities and grid operators cannot control or restrict a household's home network (local area network) and its physical layout.

Gateways are the most exposed components of a nanogrid deployment since they reside on both layers, cyber and physical. On the cyber side, these devices lie on home networks shared with multiple other devices such as computers, tablets, phones, and various IoT devices (IP cameras, thermostats, etc.). With the proliferation of IoT botnets [32] and the recognized limitations of perimeter defenses [33], [34], local area networks cannot be assumed trustworthy any longer. Realistically, a remote adversary can directly pivot to a gateway from a compromised IoT device and, potentially, manipulate the settings of the physical nanogrid deployment (e.g., change the configuration settings of microinverters). Thus, for our threat model we assume that the adversary is part of the network and is actively altering, changing, replaying, deleting, or injecting messages. This is equivalent to the *Dolev-Yao* model which is a standard threat model for cryptographic protocols [35], [36]. Specifically, in the *Dolev-Yao* model the adversary has the following capabilities:

1) The adversary can obtain any message going over the cyber network.
2) The adversary is a legitimate user of the network and she/he can therefore initiate communication with any other network entity.
3) The adversary can receive messages from any other network entity.
4) The adversary can impersonate other network entities.

However, in this model all the cryptographic primitives hold meaning that the adversary cannot "break" the cryptographic algorithms. Therefore the adversary cannot obtain secret or private keys and, thus, cannot encrypt/decrypt messages exchanged between network entities.

For this reason, a realistic setup needs to consider a powerful adversary that controls the home network and may even have physical access to the deployment. The adversary can be a malicious homeowner, that may try to lower their electricity bill, or an external attacker with various incentives.

At the physical layer, the situation is more complex than the conventional problem of securing the advanced metering infrastructure. The communication between various nanogrid components (meters, microinverters, sensors, etc.) and the gateway happens mostly using Power Line Communication (PLC) protocols over residential power lines which can be tapped into. Additionally, individual sensors may also be physically manipulated. These types of actions from a capable adversary can lead to severe consequences for the household, the utility companies, and the entire electric power grid. While this threat model is describing a very powerful adversary, these dangers are a reality for nanogrids.

V. TESTBED AND ETHICAL CONSIDERATIONS

As part of this research effort we were authorized to install in our research laboratory a fully-operational real-world PV-based nanogrid deployment, that produces electricity and injects it into the university grid. This section describes the testbed system configuration, as well as the ethical considerations followed while performing the assessments.

A. TESTBED CONFIGURATION

Our test system consists of two PV modules, each using a microinverter as an interface to the AC power system of the laboratory. A gateway device is installed to communicate with microinverters over PLC and is also connected to a household-like local area network for internet access. A high-level block diagram of the testbed with its physical and cyber layers is shown in Figure 3.

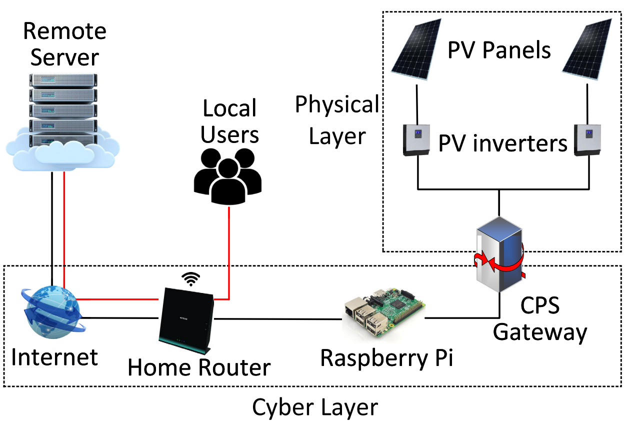


FIGURE 3. Testbed configuration – The physical layer has two solar panels and two microinverters, while the gateway is connected to both the cyber and the physical layers. Even if a user (the nanogrid owner) is connected to the same home network, the user must go through the remote server to configure the local nanogrid deployment.

1) PHYSICAL LAYER

This layer consists of two 280W PV modules, two microinverters, and the gateway device. Each PV module is connected to a microinverter. The two microinverters communicate with the gateway through Power Line Communication (PLC) when transmitting performance data regarding the solar panels.

2) CYBER LAYER

The gateway is responsible for the bi-directional communications between the PV system and the remote server. It receives the performance data from the microinverters and then sends it to a remote server over the internet. This allows for real-time monitoring of the performance data of the PV system. nanogrid owners can view their performance data by accessing the remote server through a mobile smartphone application or through a web-portal/website from any internet-connected device.

Thus, the gateway has an Ethernet port that is connected to the local area switch of the home router (in our case, Netgear R6250 [37]) to enable internet access. This way, the gateway device is assigned a private IP address from the router.

For monitoring and evaluation purposes in our testbed, the gateway is connected to the router through a Raspberry Pi. The Raspberry Pi is a low cost, small-sized computer [38]. We used the Raspberry Pi 3 Model B+ [39] as an in-line eavesdropper to collect the packets exchanged between the gateway device and the remote server. The Raspberry Pi was also used in performing the replay and man-in-the-middle attacks as detailed in Section VI-D. The main reason for choosing this device is its small size. Despite its limited computational capabilities, we were able to utilize the Pi as an "active" inline device, instead of leveraging ARP poisoning [40]. This facilitated a stable and accurate testing setup. Any general-purpose computer (with at least the computational capabilities of a Raspberry Pi 3 Model B+) can be used to implement the same functions. The wide area network port of the home router is connected to the internet and isolates the home/local area network from the rest of the enterprise network and the internet.

B. ETHICAL CONSIDERATIONS

While performing our experiments we followed strict ethical and privacy considerations to avoid affecting the operation of the device manufacturer. The testbed was deployed in a private network that is isolated from the remainder of the organization's network. All cybersecurity tests that would generate a lot of traffic, like password brute force attacks were performed while disconnecting the gateway from the internet to avoid potential disturbances.

Traffic that was sent to the remote server was very limited and controlled (e.g., only one packet at a time) to avoid disturbing the operation of any network equipment on the way to the remote server, or on the remote server itself. The experiments performed were designed with the main objective of testing the system without causing any disruptions. For ethical reasons we are not going to disclose the manufacturer of the nanogrid deployment.

VI. CYBERSECURITY ASSESSMENT

This section covers the results of the cybersecurity assessment we performed on the cyber layer of the nanogrid. In order to perform this assessment, a Kali Linux machine was placed on the same local network where the gateway resides. Kali is a Debian-based Linux distribution used for security auditing and penetration testing [41].

Briefly, the following assessments were covered throughout our experiments: reconnaissance and SSH exploitation, information leakage, assessing the gateway remote server communication, replay and man-in-the-middle attacks, and software updating mechanism manipulations. Figure 4 provides a graphical abstract overview that captures the successful attacks performed in the cyber-assessment. All experiments and tests performed follow strict ethical and privacy considerations as detailed in Section V-B.

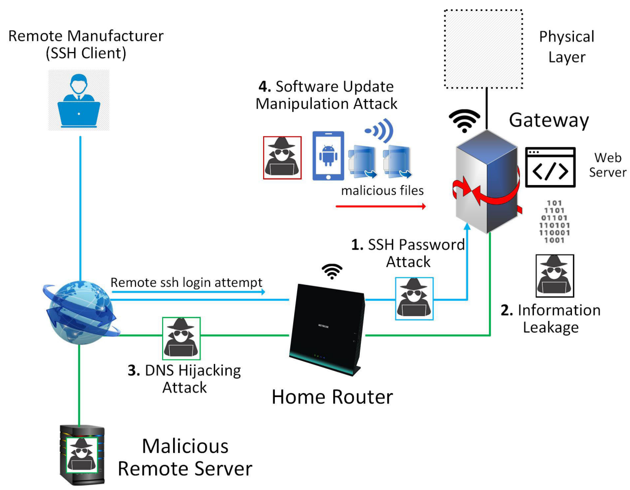


FIGURE 4. Abstract representation of the entire assessment – Our experiments resulted in four types of successful attacks: 1. Paasword-based SSH attack: An adversary can obtain the SSH credentials (username and password) and execute remote commands on the gateway. 2. Information leakage: An adversary can obtain various private information about the nanogrid deployment. 3. DNS hijacking attack: An adversary can control the interactions between the gateway and the remote server by redirecting the gateway's traffic. 4. Software update manipulation: An attacker is able to manipulate the software updating mechanisms and even upload malicious files to the gateway device.

A. RECONNAISSANCE AND SSH EXPLOITATION

Reconnaissance refers to gathering relevant information about the targeted system. The Kali machine was used to perform reconnaissance actions on the cyber layer of the testbed. Specifically, we leveraged Nmap [42], a port scanner and fingerprinting tool, to discover open ports (services). The results revealed six open ports on the gateway device with port 22 and 80 being the most interesting. We began by looking at port 22 which is the standard port for the Secure-Shell (SSH) [43] protocol. SSH is a protocol used for securing the remote login between network hosts/devices. It allows for an entity to remotely login and execute commands in a remote system. Based on the gateway's documentation, this port is open to allow manufacturers to remotely login to the gateway and perform troubleshooting and updates. The SSH service is configured as password-based and allows *unlimited* login attempts without crashing or restricting attempts. A persistent adversary, using brute-force methods could conceivably obtain the password and gain access to the gateway. On the other hand, there is a more efficient approach: SSH password-based authentication is susceptible to man-in-the-middle attacks, where an attacker can extract the password in plain- (clear-) text [43], [44]. An adversary that has a foothold on the local area network through a compromised device can perform an ARP poisoning attack [40] and intercept the password when the manufacturer logs in.

1) EXPLOITING PASSWORD-BASED SSH

To evaluate the feasibility of such an attack, we created a proof of concept to demonstrate this later possibility. In our scenario *bob* is the SSH client (the manufacturer) who is trying to access the SSH server (the gateway) for troubleshooting purposes. The attacker "sits" in the middle between the client and the server waiting for the password to be sent. The server (gateway) was replaced by a Windows machine and the attacker was operating through the Kali machine while the client was operating from a different device (inside or outside of the home network). In case of an outside connection, the user/owner will have to manually configure the router/firewall to specifically allow the incoming connection on port 22 to the gateway. The attacker acts as a man in the middle and intercepts and forwards all the traffic exchanged between the client and the server. We created an account for the client in the server with the following credentials – username: bob and password: bobpassword. When the client tries to SSH into the server (presumably for the first time) using the credentials, the password is intercepted by the attacker and obtained in clear-text, as shown in Figure 5. This attack allows an adversary to remotely login and execute commands on the gateway, thus controlling the entire nanogrid deployment. Extending this attack, if default passwords are included with other gateways, an attacker would only need to obtain one password and re-use it to access other gateway devices.

```
Received disconnect from 192.168.1.4 port 59674: 11: disconnected by user
Disconnected from user ssh-mitm 192.168.1.4 port 59674
pam_unix(sudo:session): session closed for user root
(to ssh-mitm) root on pts/3
pam_unix(su-l:session): session opened for user ssh-mitm by (uid=0)
pam_systemd(su-l:session): Cannot create session: Already running in a session or user slice
error: Bind to port 2222 on 0.0.0.0 failed: Address already in use.
error: Bind to port 2222 on :: failed: Address already in use.
fatal: Cannot bind any address
Session closed for user ssh-mitm
Connection closed by 192.168.1.4 port 59678 [preauth]
INTERCEPTED PASSWORD: hostname: [192.168.1.5]; username: [bob]; password: [bobpassword] [preauth]
Accepted password for ssh-mitm from 192.168.1.4 port 59680 ssh2
```

FIGURE 5. SSH password interception – When the manufacturer accesses the gateway over SSH an adversary is able to intercept and obtain the password in an unencrypted (plain-text) format.

B. GATEWAY WEB SERVER - INFORMATION LEAKAGE

The gateway operates a web server on port 80. The web server hosts a number of web pages that reveal a plethora of information about the nanogrid deployment.

An adversary that has a foothold on the local area network through a compromised device, can access the web pages and obtain some private information about the nanogrid deployment without needing to authenticate. For instance, the default web page displays some general information about the gateway and the performance data of the PV solar panels. Overall we were able to access 8 web pages from the gateway's web server. These web pages revealed confidential information about the gateway and the nanogrid deployment. The obtained information can be categorized as follows:

1) GATEWAY INFORMATION

This includes the gateway's serial number which uniquely identifies the gateway. Interestingly enough, part of the gateway's serial number is used as the password to authenticate to some of the protected webpages, more specific details are provided in Section VI-C. On the other hand, the web server also reveals important details about the firmware and other software packages that are running on the gateway. This includes the software version, build date and time. It also includes the name, package number, version, and the build identifier of all the packages that are running on the gateway.

2) PRODUCTION DATA OF THE SOLAR PANELS

The production data captures the hourly, daily, weekly, and lifetime power data produced by the solar panels. Moreover, this data also includes the rmsVoltage, rmsCurrent, reactive power, and the power factor of the current generated power by the solar panels. Hourly, daily, and weekly consumption data can also be viewed from the web pages without authentication.

3) GATEWAY NETWORK INFORMATION

The network information includes the Internet Protocol (IP) address, primary and secondary DNS servers of the gateway. Besides just viewing, an attacker is also able to modify the gateway network information through the web server. The ability to change the primary and secondary DNS servers of the gateway is particularly interesting as it allows the attacker to perform a DNS hijacking [45] attack as described in Section VI-C.

4) OTHER INFORMATION

Miscellaneous information includes the status of the microinverters, their serial numbers, and software versions. The status of the microinverters includes info on whether they are communicating with the solar panels and whether the solar panels are operating normally.

This data is considered confidential for nanogrid owners and shouldn't be accessible by attackers. Attackers targeting nanogrid deployments can use this information to their advantage. It can help in nanogrid network mapping, where attackers locate nanogrids with high power production for the purpose of attacking the power grid. For security reasons the gateway should authenticate users before allowing access to the web server in order to prevent the leakage and/or modification of sensitive data.

C. GATEWAY - REMOTE SERVER COMMUNICATION

We leveraged the Raspberry Pi as a bridge to eavesdrop on the communication between the gateway and the remote server, see Figure 3. Wireshark [46] ran on the Pi and captured, on a consistent basis, the packets exchanged between the gateway and the remote server. We noticed that by default the gateway sends performance reports to the remote server every 5 minutes. These reports contain the performance data of the solar panels. Figure 6 highlights one of the reports sent from the gateway to the remote server. The communication to the remote server is always initiated by the gateway behind the home router firewall. This way, the firewall on the router is "circumvented" since a home router firewall does not normally block the outgoing connections from internal devices. The owner of the deployment is able to monitor (view solar panel performance data) and configure the nanogrid remotely by accessing the remote server from any web-connected device.


```
POST /performance_report?webcomm_version=5.3.4 HTTP/1.1
Accept-Encoding: identity
Accept: */*
User-Agent: Ruby
Content-Type:
Content-Length: 972
Connection: close
Host:

121826031425.d..
.K..s\H.@.xx.fU..b82BV......JK.*......|./w....k..4\.........s.@s.......t"...
9.,.VtS.3.8..ne...R.0.........o...}
$C....2....y.6.K...n-}v2....^..f...$`..2...Y..........:.
..THo.O.A6,.........i...w.E..6..uZ.|.p.&.%.I.....@...b./
(?....q.....E...o...*.....d. ..$.%......1.^..l....k?,....L#.
[Z\Dc.D...!.._.}.#..Q.1.S...|....S^.m...J..|.~G.D..B..&......Q.
l4...B.\..Q....z
XI..m   ..
..Ss....-y.).<.O'H....P..{...:.n.Z|0..q.Q..G..).y2.     c.X.....G.[..../.....B.
3......Bg...R.$...4.a..P.|.9.nY.. y...|qw
X....S.?e..sV....8SX}.....bZ&..;.v................&?...+.e.........\....
7...SDe.....qH. .....).2..F....m.9.f1...`<-.h.?....}....
1&m.......^...........w.}....
+K..{!8..T......s.&....R.p%....z..8J%.Os...3.U.....k@Msx.....~~.`....D.].d...@..
0>.=..7..m#..n.BmMWb1FE......,v3i.....x7.K%n\.-1.....|f+...
h..
%.......`.......0[.|......V.i.X.Y...K+..`E!#!..0.!..-.:..p..
4...y.... ....l7=.......n2K..ZJ..*....G...v/iK.'..T....a..5]e
........z.Q.v#........'.."...].?..|$.U.HTTP/1.1 204 No Content
Date:
Content-Type: text/plain
Content-Length: 0
Connection: close
Server: Apache
Cache-Control: no-cache
X-Runtime: 0.132896
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Request-Id: e100811a-dfc9-4b0e-9e48-9e34e1cc2469
Set-Cookie: _mkra_ctxt=cc2e930586738972d8055aab812ec366--204; path=/; max-age=5;
HttpOnly
Status: 204 No Content
```


FIGURE 6. Performance report – A sample sent from the gateway to the server with an HTTP 204 "No Content" as the server response. The performance report contains the production data of the solar panels.

1) PERFORMANCE REPORTS

As shown in Figure 6, even though the reports are sent over the HTTP [47] protocol, their content is encrypted, except for the serial number of the gateway which is sent in plain text. The reports are sent as the payload of an HTTP POST request and are structured as follows: HTTP header followed by a 12-digit plain text serial number and then the encrypted payload (using an undocumented encryption algorithm). The gateway responds with a HTTP 204 "No Content" message.

In addition to sending the serial number in plain text to the remote server, the gateway also broadcasts the same serial number to everyone on the same local area (home) network. Based on our observations, this serial number can be part of a cryptographic key or it may be used in a search query to a database on the remote server in order to obtain the communication key of a specific gateway.

2) CONFIGURING THE NANOGRID

The owner can access the remote server through a web portal to monitor and configure the nanogrid deployment from any web-connected device. One of these configuration commands is to disable the power production of the solar panels. When a command is issued from the server to the gateway, the server waits for the next report sent from the gateway, and instead of responding with a HTTP 204 "No content" it responds with a HTTP 200 "OK" with an encrypted payload indicating the task to be performed. Figure 7 captures one of these responses that instructs the gateway to disable the power production.

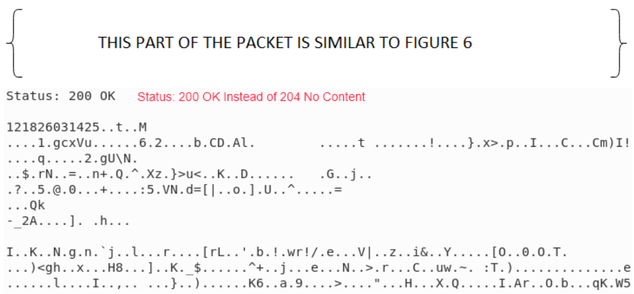


FIGURE 7. **Performance report with an HTTP 200 response – An HTTP 200 "OK" response indicates that a command is sent from the server to the gateway. The command is specified as the payload of this response.**

Despite the lack of documentation and the secrecy around the encryption algorithm, serial number, and other innerworkings, these gateway-server exchanges are still predictable. Configuration changes can be dictated only through the remote server while the connections can only be initiated from the gateway.

3) DNS HIJACKING ATTACKS

The Domain Name System (DNS) is responsible for mapping human readable domain names (e.g. "www.google.com") to IP addresses (e.g. "173.194.178.105"), that computerized devices use to identify each other on a standard TCP/IP network [48]. This translation is normally done by an authoritative or a recursive DNS server, which holds a number of DNS records with each record mapping a specific domain name to an IP address. In order for the gateway to be able to communicate with the remote server, it needs to obtain its DNS record.

One of the web pages hosted by the gateway's web server allows the attacker to change the network configuration of the gateway. In order to access this network configuration page the attacker needs to enter a username and a password. The username and the password are given in the installation manual of the gateway device, with the password being a substring of the serial number of the gateway. The attacker can obtain the serial number by accessing the home page of the gateway web server. The serial number is also broadcast in plain text to all devices in the same local area network. Accessing the network configuration page allows an adversary to change the DNS server of the gateway, to a malicious DNS server. This opens up the possibility for an attacker to perform DNS hijacking attacks [45].

As pictured in Figure 8, in case of a DNS hijacking attack, the attacker changes the DNS server of the gateway to an attacker-controlled DNS server. By doing this, all DNS queries from the gateway are redirected to the malicious DNS server, instead of the legitimate DNS server. Whenever the gateway sends a DNS request to obtain the DNS record of the benign remote server (labeled in Figure 8 as "www.remote-server.com"[1]), the request is redirected to the the malicious DNS server, which then responds with a DNS record of a (public) malicious remote server, shown in Figure 8 as "1.1.1.1".[2] From that point on, all the gateway traffic destined for the remote server will be sent to the malicious server instead. This way the attacker is able to control the gateway-remote server interactions by redirecting the gateway traffic to a malicious remote server.

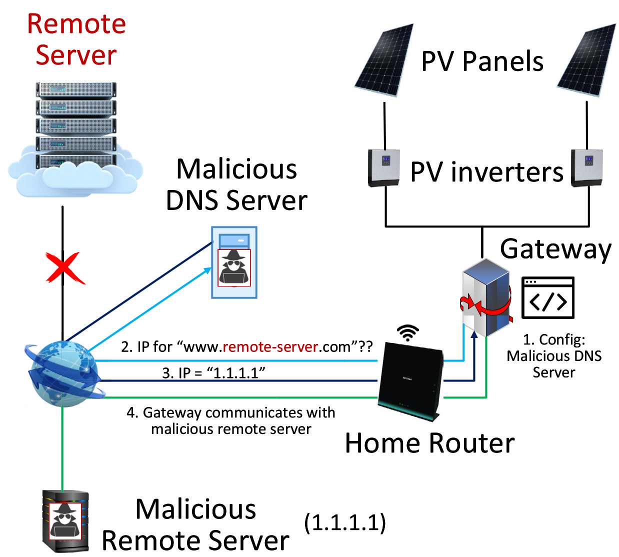


FIGURE 8. **DNS Hijacking Attack – Using the serial number of the gateway device an attacker can successfully solve the authentication process on the gateway's network configuration page. This page is protected using a known username while the password is a substring of the serial number. This information is specified in the public product datasheet. By pointing the gateway to a malicious DNS server, an attacker can now dictate who the gateway will communicate with ("remote-server.com" and "1.1.1.1" do not constitute a real DNS record, they serve only as an example).**

In this way all the solar panel performance reports are going to be sent to the malicious server instead of the legitimate server, giving the attacker complete control of the

[1] "remote-server.com" is only as an example domain, not a real domain

[2] "1.1.1.1" serves only as an example to illustrate a DNS hijacking attack, this IP address is not known to be malicious

communication between the gateway and the remote server. By doing so, the nanogrid owner and/or manufacturer will not be able to monitor and configure the nanogrid remotely through the remote server. This can be thought of as a form of denial of service where the legitimate user is denied access to an authorized service [49], but more importantly the attacker (outside the home network) can now dictate who the gateway is communicating with.

In other words, the adversary has the ability to remotely monitor and configure the nanogrid deployment. This attack can be scaled and applied to an indefinite number of gateways; given that the attacker can access their web servers, opening up possibilities for large scale attacks against nanogrid deployments and the power grid.

D. REPLAY AND MAN-IN- THE-MIDDLE ATTACKS

Once we understood the gateway-server interactions going over the local area network, we analyzed the feasibility of instantiating basic replay and man-in-the-middle attacks. As pictured in Figure 9, in a replay attack legitimate traffic is captured and reused again without modification [49]. On the other hand, in a man-in-the-middle attack the attacker also modifies the content of the messages that are exchanged between the gateway and the remote server.

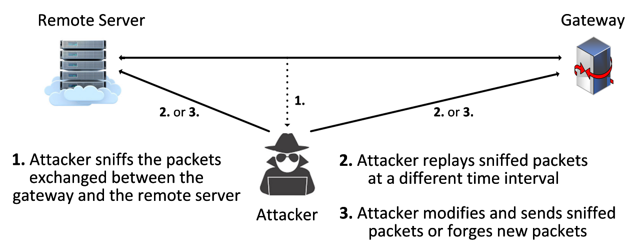


FIGURE 9. Replay and Man-in-the-middle attacks – In general a replay attack refers to capturing legitimate traffic and reusing it at a later time without modification. On the other hand, a man-in-the-middle attack involves manipulating existing network packets or forging new ones.

To perform these types of attacks we developed and leveraged a script on the Raspberry Pi that turned this device into an active, in-line man-in-the-middle. This script is designed to utilize the Netfilter queue [50] to interact with the operating system in order to examine packets that are received on its network interfaces. Next, the script examines the header of the received packets, identifies the IP addresses of the gateway and the remote server, and modifies the packets accordingly by replacing certain values before forwarding them. We noticed that these actions add minimal performance overhead and they cannot be detected by either the gateway or the remote server.

1) REPLAY ATTACKS

We captured an HTTP 200 ‘‘OK’’ message that is sent from the remote server to the gateway for disabling the power production. Then, we replayed the captured packet back to the gateway at a different time interval in place of the normal HTTP 204 ‘‘No content’’. The goal of the test is to see whether a local attacker is able to turn off the power production of the solar panels by using a straight-forward replay attack. The gateway did not accept the replayed packet. We also tried to do the same with replaying a performance report to see whether an adversary is able to create an inconsistency between what is reported and what is generated by the PV solar panels. Fortunately, this performance report was also not accepted. While this positive behavior on the gateway and server side show promise, it is important to notice that the performed experiments were the most basic attempts an adversary may try. In other words, this should not encourage the security through obscurity approaches that are currently employed by manufacturers.

2) MAN-IN-THE-MIDDLE ATTACKS

Along the same lines, we focused on changing various parameters in the packets we captured. For instance, we changed the plain-text serial number of the gateway in a packet originating from the gateway to the server. Since the replaced serial number was not a real one, the server responded with a HTTP 401 ‘‘Unauthorized’’ response. In a different scenario we captured the original message HTTP 200 ‘‘OK’’ to disable power production and modified the max-age and cookie parameters to match the values of the same parameters in the fresh HTTP 204 received from the server. This HTTP 200 message was then forwarded to the gateway in place of the HTTP 204 ‘‘No content’’. The goal of the experiment was to assess whether a local attacker is able to turn off the power production of the solar panels. Different attempts were implemented by replacing various parameters (date, cookie and max-age) in the HTTP 200 with fresh values but (fortunately) all attempts failed and the gateway rejected the modified packets.

These failures indicate that the gateway and the remote server are likely to be using a security measure such as a timestamp and/or a nonce within the encrypted part of the payload to ensure the freshness of the messages exchanged between the two parties. If an adversary *simply* tries to modify or replay previously sent packets they will be rejected. Thus, it is vital to reveal the algorithm used to generate the nonce or the length of the timestamp. Based on Kerckhoffs's principle of cryptography, the key should be the *only* secret in a cryptosystem [51]. By using a potentially weak algorithm, circumventing this ‘‘freshness’’ mechanism can be imminent.

E. MOBILE APPLICATIONS AND FIRMWARE UPDATES

Two partner mobile applications accompany the nanogrid deployment. One mobile application is targeted at users that wish to view their usage and generation data of their nanogrid while the other is targeted at individuals that setup and maintain the nanogrid. The second mobile application is particularly interesting due to the fact that it allows the user to download software updates from the manufacturer and deploy these updates to the gateway at a later time without a network connection to the manufacturer server. This structure means that the mobile application downloads and stores all software update files required for validation, configuration, and authentication directly on the mobile device.

By examining the file system of the mobile device (Figure 10 shows an overview of the software update folder from the phone), we were able to view the software update directory. The directory contains security certificates, manifest files, and an encoded/encrypted form of the software packages themselves. Each file's cyrptographic hash is computed and stored in a file that has the same name with a *.sum* extension. This is a security protection feature to detect the unauthorized modification of the update files. If the files are changed without changing the cryptographic hashes the gateway will reject the updated files. However, an attacker can modify the software update files and recompute the cryptographic hashes of the modified files and therefore bypassing this security mechanism.

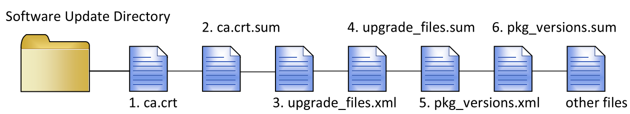


FIGURE 10. Software update directory – Contains the files that are to be pushed to the gateway in case of an update. 1&2: The security certificate of the gateway and its cryptographic hash. 3,4,5&6: Store the version numbers of files in the directory and their associated cryptographic hash. Certificates files can be replaced in this folder and hashes recomputed by adversaries.

Further, our analysis shows that it is possible to modify the manifest files in order to coerce the gateway into believing there is a legitimate update available from the mobile phone and to request these ''updated'' files. Due to this capability by the mobile application, the next area of concern is focused on how these updates can be pushed. Through our experiments, we found that it is possible to push these updates from the phone to the gateway while directly connected to the gateway's wireless access point. This means an attacker who is in close proximity to the gateway could coerce a gateway into believing a software update exists and transfer malicious files along with an unchanged security certificate to the gateway in order to flash the firmware of the device. Figure 11 shows the basic structure of the software update process and how an attacker can force a software update.

While the gateway is supposed to reject updates that have timestamps in the future of the gateway's system time, there is a time window (at least 15 minutes long) within which these timestamps are accepted. Leveraging this capability, we show that even if the gateway has just received a legitimate update from the manufacturer with a valid and current timestamp, an attacker can *always* deceive the gateway into believing there is a more recent update and subsequently transfer modified, self-signed and malicious files to the gateway.

F. ATTACK DETECTION AND MITIGATION

This section discusses various attack mitigation and detection strategies in order to address the aforementioned successful attacks summarized in Figure 4.

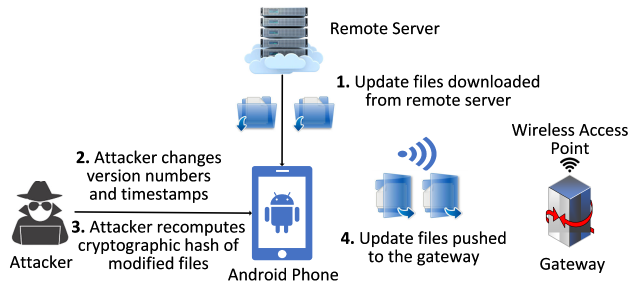


FIGURE 11. Software updating mechanism – Update files for the gateway are downloaded to a third-party mobile device, such as a smartphone, over the internet. An attacker can force a software update by modifying the version numbers and timestamps. Then the attacker recomputes cryptographic hashes for the modified files without being detected.

1) ATTACK MITIGATION

Attack mitigation refers to implementing the appropriate security measures and controls to prevent an attack from happening [52]. Below are the recommended mitigation strategies to protect against each of the specified attacks.

a: EXPLOITING PASSWORD-BASED SSH

The man-in-the-middle vulnerability against password-based SSH is well-known [44]. Thus, it is recommended to disable password-based authentication and switch to SSH public key authentication [53] for remotely accessing the gateway device. SSH public key authentication is resilient against man-in-the-middle attacks [54] and the user's ''credentials'' (i.e., private key) is not exposed, since it is never sent over the network. Although this solves the man-in-the-middle problem, other important challenges arise, especially related to SSH key management, distribution, and revocation [55]. In other words, the manufacturers need to configure an infrastructure (e.g., a x509-based approach [56]) to support the SSH remote login functionality. The design of such an infrastructure will require a separate investigation and evaluation.

b: INFORMATION LEAKAGE

For preventing information leakage, the gateway should authenticate users before allowing them access to the web server in order to protect the release of sensitive data and/or its modification. This will incur an additional processing overhead on the gateway's side depending on the complexity of the authentication scheme. This overhead needs to be carefully examined and quantified.

c: DNS HIJACKING ATTACKS

One potential solution for DNS hijacking is to adopt Domain Name Security Extension (DNSSEC) [57]. DNSSEC adds data origin authentication and data integrity to DNS records provided by a DNS server. All DNS responses from DNSSEC servers are digitally signed. By checking the signature, a DNSSEC resolver can verify that the data originated from a legitimate DNS server and that it has not been modified in transit [58]. To attain the security benefits of data authenticity and integrity, both the server and resolver must implement the DNSSEC protocol. Even though there are multiple benefits when adopting DNSSEC, it is challenging to widely deploy it. Besides the increased computational overhead for both the servers and the resolvers, cryptographic key management concerns and the lack of management tools all contribute to the complexity of implementing and adopting DNSSEC [58]. Designing a solution around DNSSEC requires further evaluation and analysis. On the other hand, a short-term solution for individual deployments should be focused on allowing only authenticated users to modify the gateway settings (e.g., DNS server settings). This approach corroborated with a trusted DNS server raises the bar significantly for an attacker.

d: SOFTWARE UPDATES MANIPULATION

When updating the firmware, it is usually more appropriate for the manufactures to directly update the gateway device from the remote server and avoid going through an untrusted third-party device (e.g., a smartphone). Manufactures could utilize over-the air (OTA) updates to remotely send files and update the gateway's firmware. This update process should be done over HTTPS to encrypt the contents of the transferred firmware. To protect against software modification attacks, code signing can be utilized to ensure the authenticity and integrity of the updated firmware. This process is being used by Amazon Web Services (AWS) to securely update the firmware of devices registered with AWS IoT [59], [60]. Despite the fact that this scheme offers more security, there are a lot of requirements and conditions that need to be met to ensure the security and reliability of this process. Looking into more reliable and secure software updating schemes is part of our future work.

It is also important to note that the National Institute of Standards and Technology (NIST), the Department of Energy (DOE), and the North American Electric Reliability Corporation (NERC) developed a series of analytical frameworks and guidelines [61]–[63] that energy sector organizations can use to develop effective cybersecurity strategies and risk management processes tuned to their particular needs.

2) ATTACK DETECTION

Attack detection refers to the process of trying to detect an attack while it is in progress. Below are some approaches that can be utilized to detect cyber-attacks.

a: INTRUSION DETECTION/PREVENTION SYSTEMS

An intrusion detection system (IDS) is usually a device that is connected to the network and generates alerts when it detects potentially malicious traffic [64]. An IDS can be used to detect and identify a broad range of attacks, including port scanning, denial of service attacks, network mapping, and operating system fingerprinting attempts. For increased performance, an IDS can be coupled with an intrusion prevention system (IPS). An IPS not only detects suspicious traffic but it also filters it out. IDS/IPS systems can leverage signature- and/or anomaly-based detection approaches.

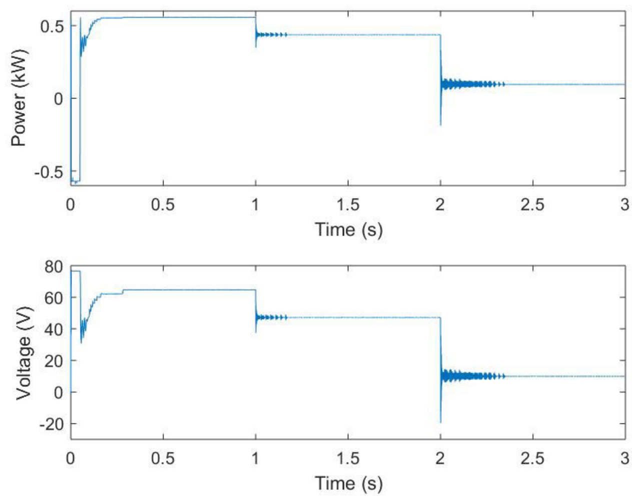


FIGURE 12. PV output power and voltage during the attack - The MPPT control automatically regulates the duty cycle and extracts maximum power 560W at t=0.14s, while the PV output power decreases since an attacker sets the power limitation to 75% and 15% at t=1.0s and t=2.0s.

A signature-based system compares each packet passing through it to a list of known attack signatures and labels traffic as malicious whenever there is a match. On the other hand, an anomaly-based system creates a traffic profile of normal traffic and considers traffic suspicious whenever it deviates from this baseline/normal profile [64]. Two well-known IDS/IPS solutions are Zeek (formerly Bro) [65] and Snort [66]. While IDS/IPS solutions are highly recommended for detecting known threats, the misclassification of traffic which results in false-positive and false-negative alerts is a well-known and important challenge with such systems [49], [67].

b: MONITORING AND LOGGING

Another technique that can help with attack detection is monitoring and maintaining logs of the network activity. A separate device on the home network can be used to store and maintain logs. The home router can be configured to send logging records in Syslog format [68] to a local logging host. Storing network activity logs and regularly examining these logs will aid identifying suspicious network activity and detecting cyber-attacks.

VII. SIMULINK-BASED PHYSICAL-LAYER ASSESSMENT

In this section we assess the possible economic loss of a household as a result of a remote attacker leveraging the shortcomings on the cyber layer to manipulate the physical layer of the nanogrid. We develop a model of PV arrays that are connected to a 25 kV grid via an inverter based on a Simulink model [69]. The model is based on our testbed described in Section V with minor simplifications. Specifically, we model one aggregated microinvertor for the two panels in our simulations since the two microinvertors behave exactly the same from the nanogrid perspective.

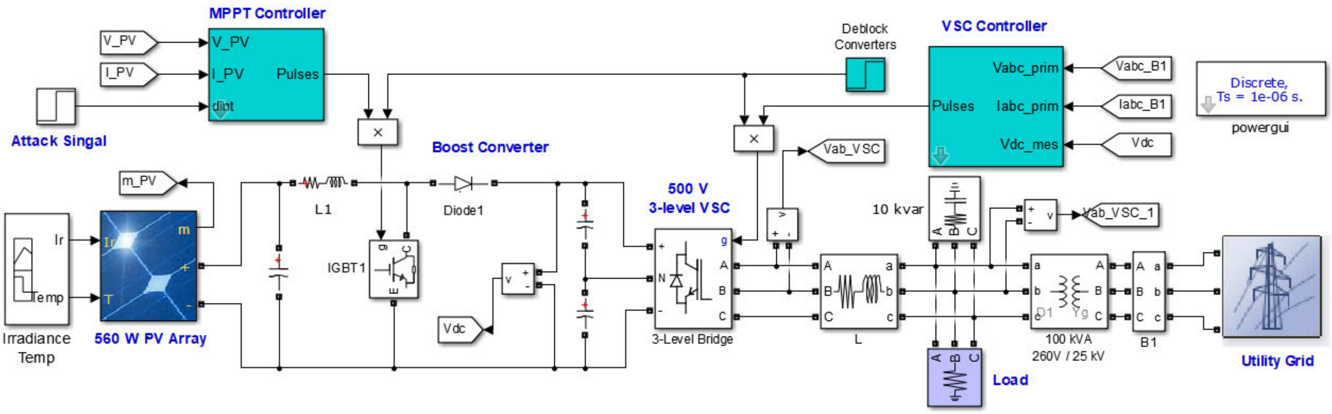


FIGURE 13. Simulation diagram – The configuration of 560W grid-connected PV array in Simulink. The PV panels controlled by an inverter are used to supply the local load and provide the surplus energy to the grid.

The configuration of the system is shown in Figure 13: two 280W PV panels with 9.47A short circuit current, 39.2V open-circuit voltage, and 32.1V max-power voltage are connected in series. The inverter is composed of a DC-DC boost converter and a three-phase, three-level voltage source converter (VSC). The boost converter increases the voltage from the PV output voltage to 500V DC, controlled by a Maximum Power Point Tracking (MPPT) algorithm [70]. The VSC converts the DC link voltage to 260V AC at a unity power factor. More specifically, the VSC is composed of an internal grid current control loop and an external DC link voltage control loop.

PV inverters allow operators to set different power limitation set-points to limit the output power of the inverter. Normally, the operator sets the power limitation to 100%, and the PV panel generates the maximum power. If the PV inverter receives a different power limitation, the PV system deviates from the maximum power point and works at the set-points by disabling the MPPT. In case the attacker can remotely manipulate the power limitation set-points of the PV inverter, this will cause an economic loss to the PV owner and might even lead to the shut down of the PV inverter [20].

The output power and voltage of PV panels in the simulation are shown in Figure 12. The boost and VSC converters start to work at t=0.05s.

The MPPT control automatically regulates the duty cycle and extracts the maximum power 560W at t=0.14s. Assume the attacker has a foothold on the network and can manipulate the power limitation of the inverter to 75% and 15% at times t=1.0s and t=2.0s, respectively. As shown in Figure 12, the PV output power drops from 560W to 420W at t=1.0s and to 84W at t=2.0s. Figure 14 pictures the PV operating point that is changed by the attacker from the maximum power point P_{max} to P_1, and from P_1 to P_2, sequentially. This attack is likely to last for a long time, if the owner of the PV system fails to notice the tempered operating points of the PV panels. For example, the average electricity rate in Hawaii is 0.327$/kWh [71]. If the attacker sets the

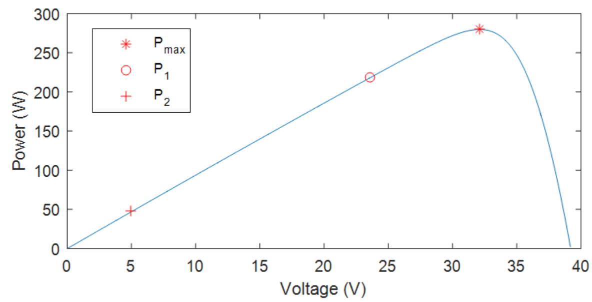


FIGURE 14. PV operating points before and during the attack – The influence of attacks on PV status. Due to the attack, PV status changes from P_{max} to P_1 and from P_1 to P_2 at t=1.0s and t=2.0s respectively.

set-point of the inverter to 15%, the PV owner will lose up to $1.57 on a sunny day. On a linear scale the PV owner may lose up to $46.8 a month. In an electric distribution network, the malicious manipulation in the MPPT operating points on a large number of inverters (especially grid-forming inverters) caused by the adversary can affect the voltage stability and may even have catastrophic consequences on the entire distribution grid. This, however, is beyond of the scope of the prosumer nanogrid and will be investigated in subsequent efforts.

VIII. DISCUSSIONS AND LIMITATIONS

Over the course of our experiments we noticed promising improvements in the employed cybersecurity measures of nanogrids compared to their previous iterations (e.g., [6]–[11]). While improvements such as the absence of transmitting clear text passwords and the raised difficulty for replay attacks constitute important steps in the right direction, we also uncovered questionable approaches. Besides the lack of adoption of well-known security solutions such as key-based SSH and Transport Layer Security (TLS) [72] for encrypted content, we also noticed few other fundamental flaws. An attacker is able to control the gateway-remote server communication as well as manipulate the software update mechanism and upload malicious files to the gateway.

We are fully aware that the manufacturer is in a difficult position. On one hand, they need to operate on home networks that they cannot control and that may contain malicious entities and devices; on the other hand, they need to provide a secure two-way communication to ensure monitoring and control while being restricted to using devices with low computational capabilities. Thus, in such cases the transparency in the mechanisms and algorithms that are used is vital for all involved parties.

IX. CONCLUSIONS AND FUTURE WORK

This research effort focuses on studying potential attacks on the physical and cyber layer of a residential PV-based nanogrid deployment. For this purpose we deployed a real-world-like residential PV system and performed a cyber assessment to investigate how nanogrids can be compromised by a powerful, but realistic adversary. Additionally, we also simulated the compromise of the physical layer that can cause economic loss to the household.

Our findings reveal major security concerns that allow an adversary to leverage different types of attacks to compromise the nanogrid deployment. For instance, an adversary can obtain the SSH credentials (username and password) and execute remote commands on the CPS gateway, thus controlling the entire nanogrid deployment. Another attack focuses on the DNS protocol. This allows an adversary to control the gateway's interactions with the remote server by redirecting the gateway traffic to a malicious entity on the internet. Moreover, an attacker is also able to manipulate the software updating mechanisms and upload malicious files to the gateway device. On the other hand, we also evaluated the economic loss of a household in the event the nanogrid deployment has been compromised. We found that a nanogrid owner in Hawaii can lose up to \$46.8 a month in case her/his deployment is compromised by an attacker.

While this research work is focused on a state-of-the art standalone PV deployment, future work will assess smarter environments where peer-to-peer energy management schemes are employed, and prosumers interact with their neighbors (consumers or prosumers) for selling or buying electricity. Future work will also investigate software updating mechanisms, with the intent of proposing a reliable and secure software updating approach that targets PV-based nanogrid deployments.

ACKNOWLEDGMENT

Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

REFERENCES

[1] US Department Of Energy. *Consumer vs Prosumer: What's the Difference?*. Accessed: Apr. 2020. [Online]. Available: https://www.energy.gov/eere/articles/consumer-vs-prosumer-whats-difference

[2] B. Arbab-Zavar, E. Palacios-Garcia, J. Vasquez, and J. Guerrero, "Smart inverters for microgrid applications: A review," *Energies*, vol. 12, no. 5, p. 840, Mar. 2019.

[3] B. Nordman, "Local grid definitions," Smart Grid Interoperability Panel Lawrence Berkeley Nat. Lab., Berkeley, CA, USA, Tech. Rep., Feb. 2016.

[4] A. Colthorpe. *Enphase Remote Upgrades Microinverters in Hawaii for Grid Integration*. Accessed: Apr. 2020. [Online]. Available: https://www.pv-tech.org/news/enphase_remote_upgrades_microinverters_in_hawaii_for_grid_integration

[5] S. Soltan, P. Mittal, and H. V. Poor, "BlackIoT: IoT botnet of high wattage devices can disrupt the power grid," in *Proc. 27th USENIX Secur. Symp. (USENIX Secur.)*. Baltimore, MD, USA: USENIX Association, 2018, pp. 15–32.

[6] W. Westerhof, "The Horus scenario," in *Proc. Still Hacking Anyway Conf. (SHA)*, Amsterdam, The Netherlands, 2017.

[7] F. Bret-Mounet, "All your solar panels are belong to me," in *Proc. DEF CON*, Las Vegas, NV, USA, 2016, pp. 4–7.

[8] T. Rienlad. *Solar Systems: Protecting Inverters From Hacker Attacks*. Accessed: Apr. 2020. [Online]. Available: https://www.tuv.com/en/corporate/about_us_1/press/news_2/newscontent_cw_371010.html

[9] J. Sanson. *Outback-Mate-Reverse-Engineering*. Accessed: Apr. 2020. [Online]. Available: https://hackaday.io/project/7624-outback-mate-reverse-engineering

[10] C. Carter, I. Onunkwo, P. Cordeiro, and J. Johnson, "Cyber security assessment of distributed energy resources," in *Proc. IEEE 44th Photovoltaic Specialist Conf. (PVSC)*, Washington, DC, USA, Jun. 2017, pp. 15–32.

[11] MITRE Corporation. *SMA: Security Vulnerabilities*. Accessed: Apr. 2020. [Online]. Available: https://www.cvedetails.com/vulnerability-list/vendor_id-16802/SMA

[12] J. Staggs, *Breaking Wind: Adventures in Hacking Wind Farm Control Networks*. New York, NY, USA: BlackHat, 2017.

[13] Solar Energy Industries Association. *United States Surpasses 2 Million Solar Installations*. Accessed: Jun. 2020. [Online]. Available: https://www.seia.org/news/united-states-surpasses-2-million-solar-installations

[14] National Renewable Energy Laboratory. *Advanced Inverter Functions to Support High Levels of Distributed Solar*. Accessed: Apr. 2020. [Online]. Available: https://www.nrel.gov/docs/fy15osti/62612.pdf

[15] J. Han, C.-S. Choi, W.-K. Park, I. Lee, and S.-H. Kim, "Smart home energy management system including renewable energy based on ZigBee and PLC," *IEEE Trans. Consum. Electron.*, vol. 60, no. 2, pp. 198–202, May 2014.

[16] *Tigo*. Accessed: Apr. 2020. [Online]. Available: https://support.tigoenergy.com/hc/en-us/articles/203630198-Tigo-MMU-Hardware-Guide

[17] *APsystems*. Accessed: Apr. 2020. [Online]. Available: https://usa.apsystems.com/products/monitor/

[18] *Outback Power*. Accessed: Apr. 2020. [Online]. Available: http://www.outbackpower.com/products/system-management/mate-mate2

[19] SMA Solar Technology. *SMA America*. Accessed: Apr. 2020. [Online]. Available: https://www.sma-america.com/home-systems/overview.html

[20] B. Kang, P. Maynard, K. McLaughlin, S. Sezer, F. Andren, C. Seitl, F. Kupzog, and T. Strasser, "Investigating cyber-physical attacks against IEC 61850 photovoltaic inverter installations," in *Proc. IEEE 20th Conf. Emerg. Technol. Factory Autom. (ETFA)*, Luxembourg, Germany, Sep. 2015, pp. 1–8.

[21] O. T. Soyoye and K. C. Stefferud, "Cybersecurity risk assessment for California's smart inverter functions," in *Proc. IEEE CyberPELS (CyberPELS)*, Knoxville, TN, USA, Apr. 2019, pp. 1–5.

[22] N. Jacobs, S. Hossain-McKenzie, D. Jose, D. Saleem, C. Lai, P. Cordeiro, A. Hasandka, M. Martin, and C. Howerter, "Analysis of system and interoperability impact from securing communications for distributed energy resources," in *Proc. IEEE Power Energy Conf. Illinois (PECI)*, Feb. 2019, pp. 1–8.

[23] K. L. Stamber, A. Kelic, R. A. Taylor, J. M. Henry, and J. E. Stamp, "Distributed energy systems: Security implications of the grid of the future," Sandia Nat. Lab., Albuquerque, NM, USA, Tech. Rep. SAND2017-0794, Jan. 2017.

[24] D. J. Sebastian and A. Hahn, "Exploring emerging cybersecurity risks from network-connected DER devices," in *Proc. North Amer. Power Symp. (NAPS)*, Sep. 2017, pp. 1–6.

[25] S. Gholami, S. Saha, and M. Aldeen, "A cyber attack resilient control for distributed energy resources," in *Proc. IEEE PES Innov. Smart Grid Technol. Conf. Eur. (ISGT-Europe)*, Sep. 2017, pp. 1–6.

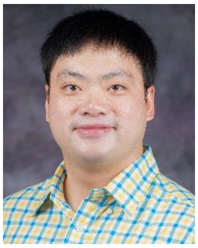
[26] J. Johnson, "Roadmap for photovoltaic cyber security," Sandia Nat. Lab., Albuquerque, NM, USA, Tech. Rep. SAND2017-13262, Dec. 2017.

[27] C. Lai, N. Jacobs, S. Hossain-McKenzie, C. Carter, P. Cordeiro, I. Onunkwo, and J. Johnson, "Cyber security primer for DER vendors, aggregators, and grid operators," Sandia Nat. Lab., Albuquerque, NM, USA, Tech. Rep. SAND2017-13113, Dec. 2017.
[28] R. S. de Carvalho and D. Saleem, "Recommended functionalities for improving cybersecurity of distributed energy resources," in *Proc. Resilience Week (RWS)*, Nov. 2019, pp. 226–231.
[29] G. Ravikumar, B. Hyder, and M. Govindarasu, "Hardware-in-the-Loop CPS security architecture for DER monitoring and control applications," in *Proc. IEEE Texas Power Energy Conf. (TPEC)*, Feb. 2020, pp. 1–5.
[30] J. Qi, A. Hahn, X. Lu, J. Wang, and C.-C. Liu, "Cybersecurity for distributed energy resources and smart inverters," *IET Cyber-Phys. Syst., Theory Appl.*, vol. 1, no. 1, pp. 28–39, Dec. 2016.
[31] California Public Utilities Commission. *Smart Inverter Working Group*. Accessed: Jun. 2020. [Online]. Available: https://www.cpuc.ca.gov/General.aspx?id=4154
[32] K. L. Lueth. *State of the IoT 2018: Number of IoT Devices Now at 7B—Market Accelerating*. Accessed: Apr. 2020. [Online]. Available: https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/
[33] J. Carson. *Black Hat Hacker Insights: What's Creating New Opportunities for Hackers?* Accessed: Apr. 2020. [Online]. Available: https://thycotic.com/company/blog/2017/08/15/black-hat-hacker-insights-new-opportunities/
[34] V. Sivaraman, D. Chan, D. Earl, and R. Boreli, "Smart-phones attacking smart-homes," in *Proc. 9th ACM Conf. Secur. Privacy Wireless Mobile Netw. (WiSec)*, Darmstadt, Germany, 2016, pp. 195–200.
[35] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. 29, no. 2, pp. 198–208, Mar. 1983.
[36] W. Mao, "A structured operational semantic modelling of the Dolev–Yao threat environment and its composition with cryptographic protocols," *Comput. Standards Interface*, vol. 27, no. 5, pp. 479–488, Jun. 2005.
[37] *Netgear—Smart WiFi Router AC1600*. Accessed: Apr. 2020. [Online]. Available: https://www.netgear.com/home/products/networking/wifi-routers/r6250.aspx
[38] *The Raspberry Pi Foundation*. Accessed: Jun. 2020. [Online]. Available: https://www.raspberrypi.org
[39] *The Raspberry Pi Foundation—Raspberry Pi 3 Model B+*. Accessed: Jun. 2020. [Online]. Available: https://www.raspberrypi.org/products/raspberry-pi-3-model-b-plus/
[40] Y. Liu, K. Dong, L. Dong, and B. Li, "Research of the ARP spoofing principle and a defensive algorithm," *WSEAS Trans. Commun.*, vol. 7, no. 5, pp. 413–417, 2008.
[41] Offensive Security. *Kali Linux Distribution*. Accessed: Apr. 2020. [Online]. Available: https://www.kali.org/
[42] G. Lyon. *Nmap*. Accessed: Apr. 2020. [Online]. Available: https://nmap.org/
[43] T. Ylonen, *The Secure Shell (SSH) Protocol Architecture*, document RFC 4251, RFC Editor, Jan. 2006.
[44] R. Andrews, D. Hahn, and A. Bardas, "Measuring the prevalence of the password authentication vulnerability in SSH," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2020, pp. 1–7.
[45] SecurityTrails Team. *DNS Hijacking: How to Identify and Protect Against It*. Accessed: Apr. 2020. [Online]. Available: https://securitytrails.com/blog/dns-hijacking
[46] Wireshark Foundation. *Wireshark*. Accessed: Apr. 2020. [Online]. Available: https://www.wireshark.org/
[47] R. Fielding and J. Reschke, *Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content*, document RFC 7231, RFC Editor, Jun. 2014.
[48] P. Mockapetris, *Domain Names—Concepts and Facilities*, document RFC 1034, RFC Editor, Nov. 1987.
[49] C. P. Pfleeger, S. L. Pfleeger, and J. Margulies, *Security in Computing*, 5th ed. Upper Saddle River, NJ, USA: Prentice-Hall, 2015.
[50] H. Welte and P. N. Ayuso. *The Netfilter.Org Project*. Accessed: Apr. 2020. [Online]. Available: https://www.netfilter.org/
[51] H. C. A. Tilborg and S. Jajodia, *Encyclopedia of Cryptography and Security*, 2nd ed. New York, NY, USA: Springer, 2011.
[52] *Managing Information Security Risk: Organization, Mission and Information System View*, Nat. Inst. Standards Technol. U.S Dept. Commerce, Nat. Inst. Standards Technol., Washington, DC, USA, 2011.
[53] SSH.Com. *Public Key Authentication for SSH*. Accessed: Jun. 2020. [Online]. Available: https://www.ssh.com/ssh/public-key-authentication
[54] SSH.Com. *Man-in-the-Middle Attack*. Accessed: Jun. 2020. [Online]. Available: https://www.ssh.com/attack/man-in-the-middle
[55] SSH.Com. *Advantages and Disadvantages of Public-Key Authentication*. Accessed: Jun. 2020. [Online]. Available: https://www.ssh.com/manuals/server-zos-product/55/ch06s02s02.html
[56] SSL.Com. *What Is an X.509 Certificate?* Accessed: Jun. 2020. [Online]. Available: https://www.ssl.com/faqs/what-is-an-x-509-certificate/
[57] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, *DNS Security Introduction and Requirements*, document RFC 4033, RFC Editor, Mar. 2005.
[58] S. Ariyapperuma and C. J. Mitchell, "Security vulnerabilities in DNS and DNSSEC," in *Proc. 2nd Int. Conf. Availability, Rel. Secur. (ARES)*, 2007, pp. 335–342.
[59] Amazon.Com. *FreeRTOS Over-the-Air Updates*. Accessed: Jun. 2020. [Online]. Available: https://docs.aws.amazon.com/freertos/latest/userguide/freertos-ota-dev.html
[60] Amazon.Com. *OTA Updates Via*. Accessed: Jun. 2020. [Online]. Available: https://aws.amazon.com/about-aws/whats-new/2019/12/ota-updates-via-https/
[61] *NISTIR 7628 Revision 1 Guidelines for Smart Grid Cybersecurity*, NIST Special Publication, Smart Grid Interoperability Panel-Smart Grid Cybersecurity Committee, Gaithersburg, MD, USA, 2014, vol. 1.
[62] *Energy Sector Cybersecurity Framework Implementation Guidance*, US Dept. Energy, Washington, DC, USA, 2015.
[63] *Electricity Subsector Cybersecurity Risk Management Process*, DOE, NIST, NERC, Washington, DC, USA, 2012.
[64] J. F. Kurose and K. W. Ross, *Computer Networking: A Top-Down Approach*, 6th ed. London, U.K.: Pearson, 2012.
[65] Zeek.Org. *Zeek*. Accessed: Jun. 2020. [Online]. Available: https://zeek.org/
[66] Snort.Org. *Snort*. Accessed: Jun. 2020. [Online]. Available: https://www.snort.org/
[67] L. Zomlot, S. C. Sundaramurthy, K. Luo, X. Ou, and S. R. Rajagopalan, "Prioritizing intrusion analysis using dempster-shafer theory," in *Proc. 4th ACM workshop Secur. Artif. Intell. (AISec)*. New York, NY, USA: Association for Computing Machinery, 2011, pp. 59–70.
[68] R. Gerhards, *The Syslog Protocol*, document RFC 5424, RFC Editor, Mar. 2009.
[69] MathWorks, Inc. *Model of a 100-kW Grid-Conn. PV Array*. Accessed: Apr. 2020. [Online]. Available: https://www.mathworks.com/help/physmod/sps/examples/detailed-model-of-a-100-kw-grid-connected-pv-array.html
[70] M. A. G. de Brito, L. P. Sampaio, G. Luigi, G. A. E. Melo, and C. A. Canesin, "Comparative analysis of MPPT techniques for PV applications," in *Proc. Int. Conf. Clean Electr. Power (ICCEP)*, Schia, Italy, Jun. 2011, pp. 99–104.
[71] ElectricChoice. *Electricity Rates by State*. Accessed: Apr. 2020. [Online]. Available: https://www.electricchoice.com/electricity-prices-by-state/
[72] E. Rescorla, *The Transport Layer Security (TLS) Protocol Version 1.3*, document RFC 8446, RFC Editor, Aug. 2018.

YOUSIF DAFALLA received the B.S. degree in electrical and electronics engineering from the University of Khartoum, Khartoum, Sudan, and the M.S. degree in electrical engineering from Washington State University. He is currently pursuing the Ph.D. degree in computer science with The University of Kansas. His research interests include cyber security, the Internet of Things (IoT) security, and smart grid security.

BO LIU (Graduate Student Member, IEEE) received the B.S. and M.S. degrees in electrical engineering from the Harbin Institute of Technology, China, in 2013 and 2015, respectively. He is currently pursuing the Ph.D. degree in electrical and computer engineering with Kansas State University, Manhattan, KS, USA. His current research interests include cyber-physical security of power systems, smart grid technologies, machine learning, and state estimation in smart grids.

DALTON A. HAHN received the B.Sc. degree in computer science from Kansas State University. He is currently pursuing the Ph.D. degree with the Electrical Engineering and Computer Science Department, The University of Kansas. His research interests include cyber security and cyber-physical systems.



HONGYU WU (Senior Member, IEEE) received the B.S. degree in energy and power engineering and the Ph.D. degree in control science and engineering from Xi'an Jiaotong University, Xi'an, China. From 2011 to 2014, he was a Postdoctoral Researcher with the Robert W. Galvin Center for Electricity Innovation, Illinois Institute of Technology, Chicago, IL, USA. He is currently an Assistant Professor and a Michelle Munson-Serban Simu Keystone Research Faculty Scholar with the Department of Electrical and Computer Engineering, Kansas State University (K-State), Manhattan, KS, USA. He is a National Science Foundation EPSCoR Research Fellow, for the period of 2020–2021. Before joining K-State, he was a Research Engineer with the Power Systems Engineering Center, National Renewable Energy Laboratory, Golden, CO, USA. His research interests include cyber-physical security of smart grids, power system planning, operation and energy management, and power grid integration of renewable energy.

REZA AHMADI (Member, IEEE) received the B.S. degree in electrical engineering from the Iran University of Science and Technology, Tehran, Iran, in 2009, and the Ph.D. degree in electrical engineering from the Missouri University of Science and Technology, Rolla, MO, USA, in 2013. He is currently an Assistant Professor of electrical and computer engineering with The University of Kansas, Lawrence, KS, USA. His research interests include modeling, design and control of power electronic converters, electric-drive vehicles, and solar energy systems.

ALEXANDRU G. BARDAS received the B.S. degrees from Romanian-American University, Bucharest, Romania, in 2008 and 2009, the master's degree in secure software systems from James Madison University, in May 2010, and the Ph.D. degree in computer science from Kansas State University, USA, in May 2016. During his B.S. studies, he was awarded a one-year scholarship to study at James Madison University, USA, from 2007 to 2008. After the scholarship ended, he returned to James Madison University as a Graduate Student. He is currently an Assistant Professor with the Department of Electrical Engineering and Computer Science, The University of Kansas. His research interests include cybersecurity mainly from a system's perspective. See www.alexbardas.com for more details.