IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 13 April 2023, accepted 3 May 2023, date of publication 22 May 2023, date of current version 8 June 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3278738

RESEARCH ARTICLE

Experimental Evaluation of Smart Electric Meters' Resilience Under Cyber Security Attacks

HARSH KUMAR[1], (Member, IEEE), OSCAR. A. ALVAREZ[2], (Member, IEEE), AND SANJEEV KUMAR[2], (Senior Member, IEEE)

[1]Department of Electrical and Computer Engineering, The University of New Mexico, Albuquerque, NM 87106, USA
[2]Department of Electrical and Computer Engineering, The University of Texas Rio Grande Valley (UTRGV), Edinburg, TX 78539, USA

Corresponding author: Sanjeev Kumar (sj.kumar@utrgv.edu)

This work was supported in part by the U.S. National Science Foundation; in part by the Department of Homeland Security (DHS); in part by the Houston Endowment Chair in Science, Math and Technology Fellowship; in part by the Benston Jr. Endowment Chair in Engineering; in part by UTRGV's Graduate Research Assistant Scholarship; in part by the U.S. DHS Science and Technology (S&T) Directorate Office of University Programs Summer Research Team Program for Minority Serving Institutions, administered by the Oak Ridge Institute for Science and Education (ORISE) through an interagency agreement between the U.S. Department of Energy (DOE) and DHS; and in part by the ORISE through ORAU under DOE Contract DE-SC0014664.

ABSTRACT For the first time, commercial grade smart meters have been subjected to cyber security attacks to understand their operation and security resilience under different attack scenarios. Cyber security is a matter of top concern for utility companies installing smart meters for remote collection of power usage data from customer premises. Keeping power-usage data secure and to maintain system's resiliency under cyber security attacks is very important. In Smart electric grids, the power usage data from smart meters are periodically reported to the utility company. Reporting and remote monitoring of power usage data requires the use of data network protocols, which introduces security vulnerabilities. Cyber security attacks can impact reporting mechanisms in the smart grid, which may result in alteration or complete loss of power usage data as reported to the utility company. Despite the wide deployment of smart meters, there has not been much experimental work done to evaluate resiliency and data integrity of smart meters under security attacks. It is not clear how the operation of smart meters or the remote collection of power-usage data can be affected under security attacks. In this paper, we present our experimental work to test security resiliency of the commercial grade smart meters. We conducted real experiments, using smart electric meters from leading manufacturers to investigate data integrity under common data security attacks in a lab environment using real network equipment. Based on the experimental observations, it was discovered that the common cybersecurity attacks were able to adversely impact the data reporting operation of the smart electric meters. Cybersecurity attacks in some cases were found to cause complete loss of reporting of the power-usage data to the remote monitoring station.

INDEX TERMS AMI, critical infrastructure, cyber security attack, IoT, remote monitoring, smart meter, smart grid.

I. INTRODUCTION

In smart electric grid power system, smart meters play a crucial role in grid modernization. Smart electric meters use advanced communication technologies for automatic meter reading for remote data collections and resilient energy grid operations. Smart meters are specialized digital meters that utilize data communication within the smart electric grid, which makes the smart energy grid operation more reliable, controllable, and cost effective. Smart meters help in communicating the customer's power consumption information to the utility companies for monitoring, billing and easy trouble shooting from remote central offices. Smart meters allow access to real-time data which helps

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

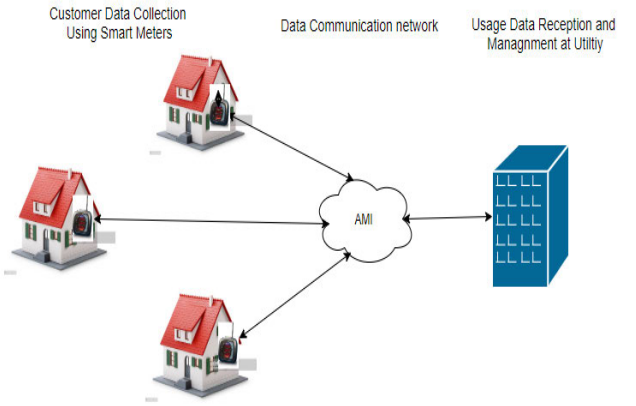


FIGURE 1. Advanced metering infrastructure (AMI).

utility companies to effectively manage electric loads and demand response, quick electricity restoration after power outages, reduced operations, and management costs, reduced peak demand, better integration of customer-owned power generation systems, including renewable energy systems and improved security [1], [2], [3], [4], [5], [6], [7], [8], [9]. Smart meters are being installed rapidly by the utility companies. According to the report [8] from Institute for Electric Innovation, 107 million smart meters were deployed which covered 2/3rd of the US households.

Smart meters of today are helping modernize the old manual data reading system and the network of smart meters are called Automatic Metering Infrastructure (AMI). Automatic metering infrastructure (AMI) helps to set up 2-way communication between the utility companies and their customers via smart meters deployed at customer premises (Figure 1).

AMI refers to the full continuous measurement and collection system used by utility companies. AMI additionally refers to the communication networks between the client and a service supplier, and data reception and management systems that make the information available to the service provider. AMI replaced AMR (Automatic Meter Reading) whose purpose was the reading of data from the meter. Automatic metering infrastructure (AMI) helps to set up 2-way communication between the utility companies and their customers via smart meters deployed at customer premises. Smart meters help improve demand response, and peak reduction efforts. Smart meters are specialized digital meters that utilize the Internet of Things (IoT) technologies and Internet based communication within the smart electric grid, which makes the smart energy grid operation more reliable, controllable, and cost effective. Smart meters are IoT-ready devices that help in communicating the customer's power consumption information to the utility companies for monitoring, billing and easy trouble shooting from remote central offices. Smart meters allow access to real-time data which helps utility companies to effectively manage electric loads, reduce power outages, and streamline energy distribution through more accurate forecasting. Smart electric meters can be connected over wireline or wireless network for remote monitoring and remote data collection by the utility companies for power consumed at customer premises. Since smart meters use Internet of Things (IoT) technologies and data communication protocols for communication between utility companies and customer premises, smart meters can become vulnerable to cyber-attack, which in turn can hamper the integrity and reliability of power usage data collection and reporting.

There are not many papers published on real experimental measurements on real smart meters using real attack traffic. In the past experimental research [10], authors conducted experiments to measure and understand the impact of cyber security attack on a smart meter where authors experimentally showed that a common cyber security attack can have adverse effect on the reliable operation of a smart electric meter, which can result in a significant financial loss in a bigger commercial deployment. In the prior work [10], experimentations were done for shorter span of time, and it was not clear what would happen if experimentation continued for longer period of time say for a complete billing cycle usually 30 days. Also, in prior work [10], only one smart meter was used, and it was not evident if the problem was particular to a given smart meter or if similar problem was occurring with other smart meters from other companies. To answer all these questions, in this paper, authors have extended the experimental work for longer durations of smart meter operations under attack conditions. We tested the operation of different smart meters from two different leading manufacturers to understand the overall resilience and reliability of remote power-usage data collection under conditions of cyber security attacks. Furthermore, direct, and indirect types of cyber-attacks were used. This research provides a better understanding of cybersecurity exposure for smart-meters and AMI, which enables utilities to be more informed regarding the cybersecurity posture of AMI especially in a large deployment.

This paper presents the following sections: Section I provides a general introduction. Section II provides a review of related literature. Different smart meters features used in the experiments have been presented in Section III and IV. Section V is dedicated to different cyber-attacks used for resilience experimentations. Section VI is dedicated to experimental set up with different meters under different attack scenarios. Section VII provides experimental results and discussion. Conclusion is provided in Section VIII followed by references.

II. LITERATURE REVIEW

There are not many papers on conducting real experimental measurements on real smart meters. However, we are providing a brief survey of some related work addressing security issues related to smart meters and AMI. AMI system is vulnerable to cyber-attacks that aim to steal electricity. These attacks can compromise smart meters and alter the

reporting of power usage data. These attacks can result in significant loss of revenues, and they can adversely impact the overall power grid operation. Many surveys related work [11], [12], [13], [14], [15] are available in literature detailing various attack scenarios on smart meters and AMIs.

Gunduz and Das in [11] presented a detailed theoretical survey of prior publications on risks and potential remedies associated with IoT-based smart grid. Different types of cybersecurity attacks, vulnerabilities, and potential remedies were presented and compared.

Similarly, work in [12], [13], [14], and [15] presented a general theoretical survey of common vulnerabilities in smart meters and AMIs that can be exploited by attackers in launching cyber security attacks on smart meters, AMIs and they provided potential solutions that can be applied for smart grid metering network. Different types of cyber security attacks have been discussed in prior work [16], [17], [18], [19] against smart meters in AMI and Smart Grid environment and they are elaborated below:

A new Denial of Service exploit named Puppet attack was presented in [16] by Yi et al. A Puppet attack-based DDoS allows an attacker to compromise a normal node to interfere with network traffic on the AMI. It showed that the Puppet attack could negatively impact the data delivery rate in AMI. Anderson and Fuloria in [17] presented effects of a Denial-of-Service attack against communication network of automatic metering infrastructure where attackers could compromise devices in automatic metering infrastructure and obstruct information transit over network.

McDaniel and McLaughlin in [18] introduced a harmful technique through which attacker could change measured meter data and target smart meters. Attackers may potentially gain access to a smart meter and alter or create additional meter data.

Cleveland in [19] gave an illustration of a potential scenario in which a hacker would breach security of AMI and issue millions of disconnect instructions remotely. A cyber-attack scenario was simulated in which attackers could breach automatic metering infrastructure's communication network to launch DoS attacks. Work in [20], [21], [22], [23], and [24] presented different schemes to detect cyber security attacks on smart meters. They included various machine learning schemes to detect cyber security attacks and evaluated their performance using simulations.

Prior work mentioned in the literature above [11], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21], [22], [23], and [24] raised many concerns related to different attack scenarios and potential solutions, most of these works were theoretical in nature, some of them used network simulation techniques or mathematical modelling of the network, however most of these attack scenarios or the proposed remedy techniques were not implemented or tested on real smart meters.

In this paper, we are adding a new dimension of experimental work using real data security attacks on real smart meters. We measured the impact of some common security attacks on real smart meters that are commercially being deployed today.

FIGURE 2. Smart multifunction meter (EPM 6100) from GE [25].

III. EPM 6100 POWER QUALITY METER FROM GE

IoT based smart electric meter EPM 6100 shown in Figure 2. is one of the commercial meters manufactured by GE [25], which helps customers to monitor and manage their energy usage within their industries, residences, businesses, school, and university campuses [24]. The EPM 6100 is a multifunction meter that features ANSI C12.20 (0.2% class) accuracy **class** where **0.2** means +/- **0.2** % ratio error and provides several interfaces such as RS485, RJ45 Ethernet and IEEE 802.11 for WiFi communication, making the smart meter deployable in new or preexisting communications systems [25]. The units use standard five or one-Amp Current Transformer's (either split or donut), surface mount to any wall [25].

GE EPM 6100 smart meters can be programmed and configured as stated in the GE manual [25]. The merits of this meter include providing a variety of voltage, current and energy measurements, which can allocate energy consumption in multi-tenant settings such as apartment complexes, university campus towers, and shopping malls [25].

Smart meters use data communications protocols for information flow from the smart meters to the remote utility company facility. Generally, all communication protocols consist of defined sequences that begin by having a requesting device identifying itself to the requested device. After the identification, there must be an exchange of parameters such as the maximum frame length, the number of frames sent, and the communication rate to establish the communication desired. Protocols also use known standards for the physical medium used. One standard for example, RS-485, defines the electrical characteristics of drivers and receivers for use in serial communications systems [26]. This smart meter EPM 6100 uses MODBUS TCP/IP protocol [27], [28].

This smart meter comes with a software called GE communicator Software [25], which benefits utility companies by having a platform to remotely access all setups and support tools required for configuring and maintaining GE

FIGURE 3. GE communicator software for data analysis and configuration used by remote monitoring computer.

FIGURE 4. E650 S4x ethernet module meter from Lyndis Gyr [29].

smart meters (Figure 3). It also helps in remotely configuring devices in real-time over network connections through which it can remotely read, record metered power consumption data, and it can also monitor status of the smart meters [25].

IV. E650 S4x ETHERNET MODULE SMART METER FROM LANDIS+GYR

Another commercially deployed smart meter Landis+Gyr E650 S4x is shown in Figure 4, which was considered in our experimental studies for impact of cyber-attacks on power-usage data collection. It is one of the commercial and industrial meters by Landis+Gyr, which allows utilities to monitor and manage their energy usage within factories, businesses, and campuses like the smart meters from GE. E650 S4x Polyphase meters are designed to cover a wide range of requirements and applications – from light commercial to industrial metering.

Landis+Gyr's polyphase meters have feature to eliminate the need for pre-programming and it automatically detects the service type and voltage, displaying the information on the LCD and by configuring the smart meter it helps in complete diagnostic installation check. By performing diagnostics on the metering installation equipment, service wiring and load characteristics, it identifies issues with equipment, installation, wiring, load conditions, power quality and tampering. Smart meter provides an Ethernet port and module for meter programming and firmware upgrades. It utilizes

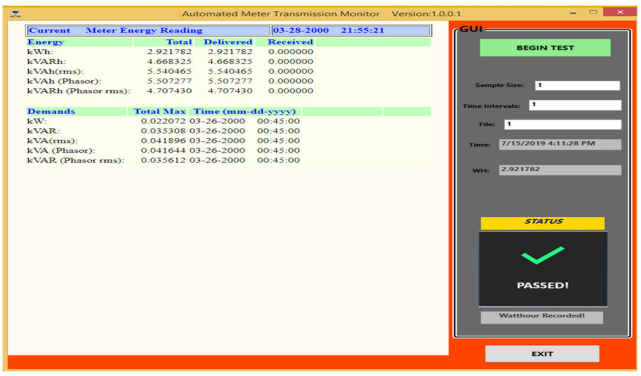


FIGURE 5. Automatic meter transmission monitor software for Landis+Gyr smart meter [29] for remote monitoring at the utility company.

advanced second-generation flushable firmware, which is well supported by the AMI network. This firmware can be upgraded remotely without losing the meter configuration or billing data. This Landis+Gyr smart meter uses ANSI 12.18 and 12.21 protocol and all information about this protocol was obtained from references [30] and [31].

Automatic meter transmission monitor software from Landis+Gyr in Figure 5 provides a platform to remotely access the instantaneous remote reading of the energy usage in real time along with remote data logging and recording of usage data over time. It is also used in monitoring and keeping track of all the electrical parameters and helps in setting up the required configuration of the meter for data communication to the remote utility location for billing for the energy usage.

V. CYBER SECURITY ATTACKS

Cyber security attacks are known to impact Confidentiality, Integrity, and Availability of data network-connected devices. Furthermore, the class of Distributed Denial-of-Service attacks (DDoS) [32], [33], [34], [35], [36], [37], [38], [39], [40], [41], [42], [43], [44] are known to impact Integrity and Availability of a network connected system. Since the smart meters at customer premises are connected via data networks to the remote utility companies, it is possible for the DDoS or flood attacks to adversely impact the operation of these smart meters making them unavailable for power usage data reporting, temporarily or for a longer time-period.

A. ICMP BASED CYBER ATTACKS

The Internet Control Message Protocol (ICMP) is primarily used to enable different error-reporting, feedback, and testing messages. ICMP messages can be divided into two categories: Error messages and Informational messages. Error messages are used to report errors that can occur during data packet delivery. Diagnostics, testing, and other informational purposes are served by informational messages [45], [46], [47], [48], [49], [50], [51]. An attacker can launch different types of ICMP based attacks, including Ping

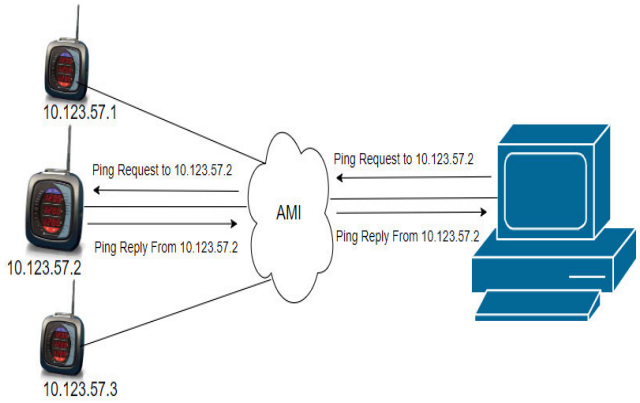


FIGURE 6. Ping utility in action for AMI connectivity.

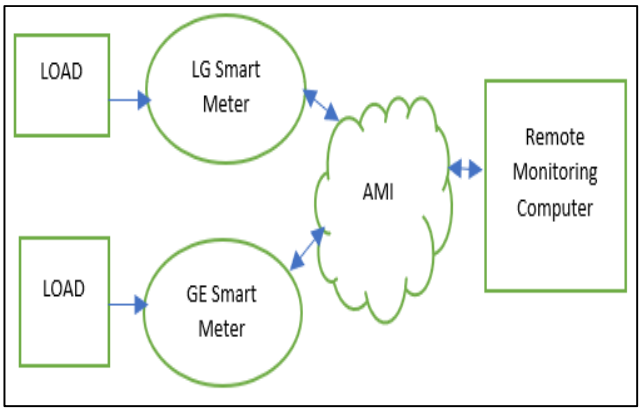


FIGURE 7. Experimental setup for baseline without attack.

flood, Ping of Death, and Smurf attacks, by exploiting ICMP "Informational messages."

There are some common types of ICMP (Internet Control Message Protocol) based cyber security attacks such as Ping flood attacks [50] and Smurf attacks [40]. In this work, we conducted experiments to investigate the impact of ICMP based Ping flood attacks on the smart meter's data reporting capabilities, and integrity of power usage data sent from the smart meters to the remote computer on Ethernet based data network.

B. PING BASED CYBER ATTACKS

Ping based cyber-attack [50] is an ICMP based cyber-attack, which generally aims to saturate the data communication network with ICMP traffic. ICMP Ping helps to verify the end-to-end internet path operation, where ICMP Echo request packet is usually sent to the target and an ICMP Echo Reply packet is expected in return to verify communication session being set up between a sender and a receiver. A host or a sender uses an ICMP echo request (ping) message to test a destination's reachability. The data enabled equipment such as a smart meter, which receives an ICMP echo request message responds back by sending an ICMP echo reply message back to the sender shown to test reachability as shown in Figure 6. The Ping based cyber security attacks consist of a huge amount of such ping request or ICMP Echo request messages (Ping flood) sent to the smart meters to adversely impact the normal operation of the smart meters. Furthermore, these attacks can cause the exhaustion of the bandwidth and computational resources of the targeted network and thus impacting all smart meters on the affect network. Under this attack, the smart meters continue to receive Ping messages and continue to generate ICMP echo reply messages as long as the attack persists [50].

C. INDIRECT AND DIRECT CYBER SECURITY ATTACKS

There are two different types of data attack traffic that can be experienced by a network connected smart meter in smart grid environment- Indirect and Direct data security attack traffic. In Indirect security attack scenario, an attacker may not know the IP address of the devices but may know about the subnet address, MAC address, and construct a range of random IP addresses for attack purposes. Under direct attack scenario, an attacker may know the IP address, or a range of IP addresses of the network connected devices [51]. Hence under data security attack scenario in smart grid environment, smart meters in an AMI network can receive two different types of attack traffic, namely the Indirect and Direct security attacks, which are further discussed below.

VI. EXPERIMENTAL SET UP WITH GE AND LG SMART METERS

In this paper, we conducted security evaluation of two different smart meters, (i) General Electric (GE) Multilin EPM 6100 Power Quality Meter [25] (Figure 2) and (ii) Lyndis+Gyr E650 s4x [29] (Figure 4) -both deployed Ethernet port for data communication, operating at a frequency of 60 HZ.

For the experiment, both meters were connected to the remote monitoring computer and the attacker network over ethernet. Remote monitoring computer had GE communicator software and AMT monitoring software installed for two different meters, and it collected power usage data remotely from the smart meters.

First, we created a baseline profile of the power consumption for the duration of the experiments, where there was no security attack on the smart meters. A schematic diagram for the baseline network configuration is given in Figure 7. The actual set up for the experiment is shown in Figure 8.

We simulated cyber-attack traffic for our experiments inside the Network Research Laboratory (NRL) at UTRGV (Figure 8). Simulated Ping based cyber-attack traffic was sent to the meters involving layer3 IP, and layer2 MAC protocols.

We conducted four independent experiments to observe the effect of direct and indirect cyber security attacks on reporting of power consumption data in Watt hour (Wh), recorded over 15 days, and for the entire billing cycle i.e., 30 days. We compared the performance with the baseline

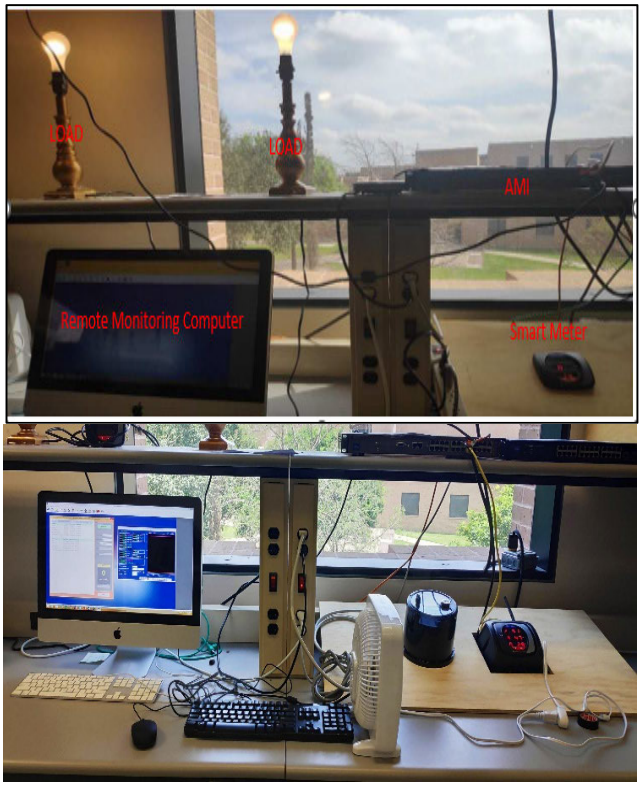


FIGURE 8. Lab set up for smart meter evaluation.

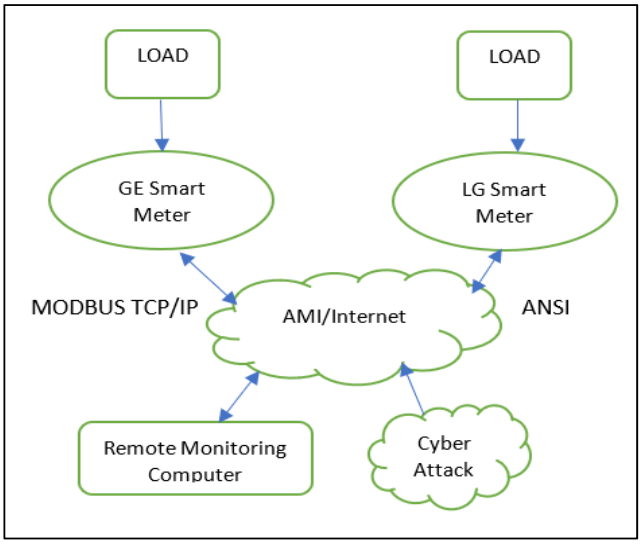


FIGURE 9. Experimental set up for smart meter security evaluation under direct and indirect cyber-attacks.

power consumption in Watt hours (Wh) when there was no attack. We did these investigations to evaluate the data integrity and resiliency aspects of the smart meter under different attack scenarios. We also estimated financial loss under such attack scenarios.

A. CASE-I: EXPERIMENT FOR BASELINE PERFORMANCE WITHOUT ATTACK

To compare the impact of cyber security flood attack on smart meters, the baseline performance for both meters were first measured without the flood attack. The baseline power consumption (Wh) due to the load was measured remotely through the remote computer for over a period of a month in the absence of attacks. Two light bulbs were used as a load for the smart meters.

B. CASE-II: EXPERIMENT UNDER INDIRECT ATTACK OVER 15 DAYS BILLING CYCLE

We measured the performance of both meters under indirect cyber-attack for a period of 15 days as per set up shown in Figure 9. For these experiments both meters used the same load and same intensity of attack for the same period of time.

For Indirect security attacks, random IP addresses were used for a given subnet and MAC addresses could be found from the front panel of the meter e.g., 00 20 4A F8 DA DO for GE and 00 80 A3 C6 9D 58 for Landis+Gyr (LG) meters respectively. All power consumption data were recorded remotely on the remote monitoring computer under indirect attacks on both the meters. Ping attack traffic experienced by the smart meters was found to be 38 Mbps, which is considered rather a lower intensity cyber-attack these days.

C. CASE-III: EXPERIMENT UNDER INDIRECT ATTACK OVER 30 DAYS BILLING CYCLE

In this case, we extended the measurement for another 15 days for a total of 30 days of data collection on power consumption under indirect attack scenario for the same experimental set up as shown in Figure 9. The 30-day measurement was intended to coincide with the typical billing cycle for a customer. In this indirect attack, random IP addresses belonging to a given subnet were used, along with the MAC addresses found from the smart meters e.g., 00 20 4A F8 DA DO and 00 80 A3 C6 9D 58 respectively. All power consumption data (in Watt hours) were reported by the smart meters to the remote monitoring computer under indirect attack scenario. Throughout this experiment, both meters had the same electric load, and they experienced the same intensity of attack. At the end of billing cycle (i.e., after 30 days) attack was removed but the meters were continued to report normal power usage data for 2 more days to further observe the data reporting behavior of the smart meters after the attack was removed.

D. CASE-IV: EXPERIMENT UNDER DIRECT ATTACK FOR GE & LG METER

In this case, the smart meters were tested under direct attack scenario for the same experimental set up as shown in Figure 9. For this experiment, both meters had the same electric load, and both experienced the same intensity of direct attack. Under this scenario of direct attack, the attacker knew the IP address of the meters. MAC addresses were known from the meters themselves. For GE meter, for

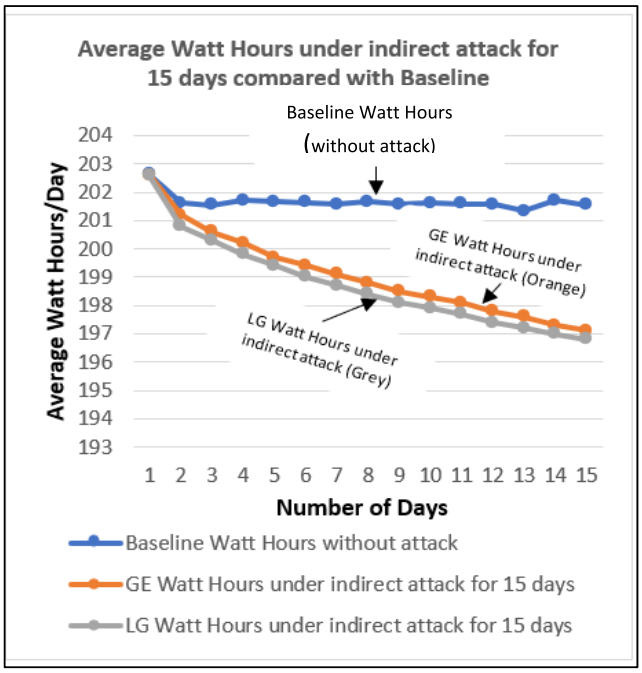


FIGURE 10. GE and LG Watt hours with no attack and under indirect attack over 15 days.

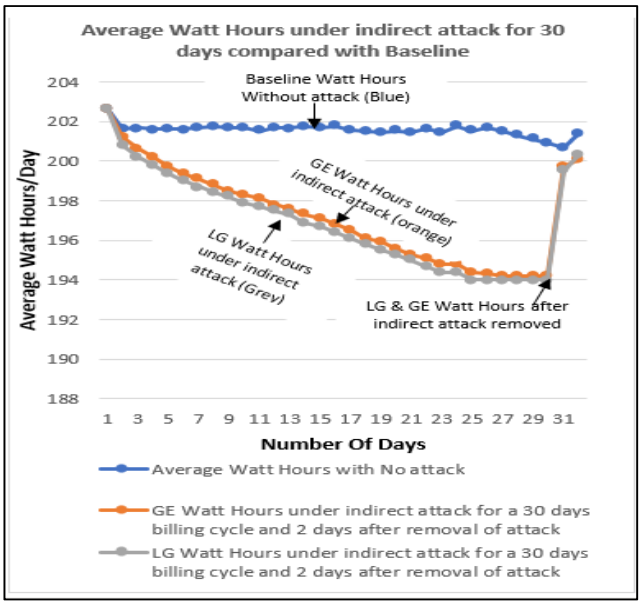


FIGURE 11. GE and Landis+Gyr performance under indirect cyber-attack for a 30-day billing cycle and for extra 2 days after removal of the attack.

example, the MAC and IP addresses were 00 20 4A F8 DA DO and 192.168.1.15 respectively. For Landis+Gyr (LG) smart meter, the MAC and IP addresses were 00 80 A3 C6 9D 58 and 192.168.1.10 respectively. To study the behavior of the smart meters under direct attack, their data reporting performances were measured for three days as follows: for the first day (24 hours), power usage data were remotely recorded without attack; for the second day (another 24 hours), power consumption data were remotely recorded under direct attack; and for the third day, the attack was removed, and the power consumption data were recorded remotely for another 24 hours.

VII. EXPERIMENTAL RESULTS AND DISCUSSION

Case- I Discussion: Experiment for Baseline Without Attack: It was observed that the baseline Watt hour recorded over a period of 15 days and 30 days by the two smart meters from GE and Landis+Gyr had no significant variation i.e., power usage recorded by LG and GE looked identical. These recorded data constituted the baseline data without attack, and it is displayed using line graph in Figure 10 and Figure 11.

Case- II Discussion: Experiment Under Indirect Attack Over 15 Days: It was observed that on the very first day (24 hours) under indirect cyber-attack there was no significant impact on the usage data and it stayed close to the baseline data. However, with time moving forward both meters started reporting declined power usage data and deviation from the baseline power usage data became more pronounced with every day over 15 days (Figure 10).

Table 1 shows the average power usage (Watt hours) for baseline and under indirect attack over 15 days. Figure 10.

TABLE 1. Average Power Usage (Watt hour) reported in 15 Days under indirect attack scenario.

Smart Meter	Average Power Usage (Baseline under no attack) in 15 days	Average Power Usage (under cyber-attack) in 15 days
GE	201.7 Wh	197.1 Wh
LG	201.7 Wh	196.7 Wh

shows average power consumption for 15 days without attack (baseline) and its comparison with average power consumption under indirect attack for both smart meters. Results show that the power usage data as reported by the smart meters under indirect attack continued to decline compared to the scenario when there was no attack (baseline power usage reporting).

A. POWER LOSS REPORTED UNDER INDIRECT CYBER-ATTACK OVER 15 DAYS FOR GE SMART METER

Equation (1), as shown at the bottom of the next page.

B. POWER LOSS REPORTED UNDER INDIRECT CYBER-ATTACK OVER 15 DAYS FOR LG SMART METER

Equation (2), as shown at the bottom of the next page.

By the end of Day 15, under indirect attack scenario, the GE smart meter reported an average power loss of 2.28 % (compared to the baseline Watt hours), and the Landis+Gyr smart meter reported an average power loss of 2.47% compared to the baseline, as calculated by using equation (1) and (2). Power loss of 2.28 % and 2.47 % may seem small, but it can make a big difference when it comes to a large commercial deployment of smart meters by a large electric company as shown in Table 3.

TABLE 2. Average power usage (Watt hour) reported for 30 days under Indirect attack scenario.

Smart Meter	Average Power Usage (Baseline under no attack) in 30 days	Average Power Usage (under cyber-attack) in 30 days
GE	201.7 Wh	194.2 Wh
LG	201.7 Wh	193.7 Wh

TABLE 3. Power reporting loss and resulting revenue Loss due to indirect cyber-attack for a large utility company.

Parameters	GENERAL ELECTRIC (GE) METER	LYNDIS+GYR (LG) METER
Power loss reported due to security attack on Smart Meters based on our experimental result over 15 days	: 137715467 kWh (Based on 2.28% loss)	148587741 kWh (Based on 2.47% loss)
Power loss reported due to security attack on Smart Meters based on our experimental result over 30 days	224693657 kWh (Based on 3.72% loss)	239190022 kWh (Based on 3.96% loss)
Financial loss to the utility company due to indirect cyber-attack on smart meters over 15 days	23.97 million USD (Based on 2.28% loss)	25.87 million USD (Based on 2.47% loss)
Financial loss to the utility company due to indirect cyber-attack on smart meters over 30 days	39.11 million USD (Based on 3.72% loss)	41.64 million USD (Based on 3.96% loss)

Case-III Discussion: Experiment Under Indirect Attack Over 30 Days Billing Cycle: It was observed during 15 days of measurements that under indirect cybersecurity attack, both smart meters continued reporting reduced power-usage data (compared with its baseline values) to the remote monitoring station. Power usage data reported to the remote station continued to decline further with every passing day under the attack traffic. To investigate the increased reduction in the reported power-usage data, we further continued the measurement of the reported power-usage data under the cybersecurity attack for the entire billing cycle i.e., 30 days. It was observed that both smart meters reported further decline in the power- usage data under indirect attack for one more week but during the last week of the billing cycle, there was no further decline and the power usage data seemed to stabilize under the low-intensity indirect cyber-attack. To further understand the behavior of these meters, we removed the attack at the end of the 30 days of the experiment. Once the attack was removed, the power usage data was observed to be reaching back to the baseline Watt hour values again as shown in Figure 11.

C. POWER LOSS REPORTED UNDER INDIRECT CYBER-ATTACK OVER 30 DAYS FOR GE SMART METER

Equation (3), as shown at the bottom of the next page.

D. POWER LOSS REPORTED UNDER INDIRECT CYBER-ATTACK OVER 30 DAYS FOR LG SMART METER

Equation (4), as shown at the bottom of the next page.

Power loss of 3.72 % and 3.96 % may look small, but it can make a big difference when it comes to a large commercial deployment of smart meters by a large Electric company as calculated in Table 3.

E. REVENUE LOSS CALCULATION DUE TO INDIRECT CYBER-ATTACK FOR A LARGE UTILITY COMPANY OVER PERIOD OF 15 DAYS AND TYPICAL CUSTOMER BILLING CYCLE I.E., 30 DAYS (CASE II AND III)

% Loss of power usage in reporting = 2.28 % for GE meter and 2.47% over 15 days respectively (calculated from the formula in (1) and (2). % Loss of power consumption = 3.72% for GE meter and 3.96 for LG meter over 30 days (calculated from the formula in (3) and (4). Here we estimate how this type of Cyber-attack on Smart meters will affect revenue of a large electric company assuming they use this type of smart meters in their deployments by using the case of both smart meters observed in table 1. Some of the power

$$\begin{aligned}&\%\text{Power loss reported after 15 days (based on data from table 1)}\\&= \frac{Power\ Consumption(Baseline) - Power\ Consumption\ (Cyber\ Attack)}{Power\ Consumption(Baseline)} \times 100\\&= [(201.7 - 197.1)/201.7] \times 100 = 2.28\% \end{aligned} \tag{1}$$

$$\begin{aligned}&\%\text{ Power loss reported after 15 days (based on data from table 1)}\\&= \frac{Power\ Consumption\ (Baseline) - Power\ Consumption\ (Cyber\ Attack)}{Power\ Consumption\ (Baseline)} \times 100\\&= [(201.7 - 196.7)/201.7] \times 100 = 2.47\% \end{aligned} \tag{2}$$

consumption data has been obtained for the Pacific Gas & Electric in 2015 from [52] and are given below:

- Total customers (Residential and Commercial) = 5,069,189
- Total power usage per month= 6,040,152,083 kWh
- Average price [52] = 17.41 cents per kWh
- Loss of power due to security attack on GE Smart Meter for 15 days = (6,040,152,083 X 2.28 % reported loss from equation 1) in 15 days = 137715467 kWh.
- Total Loss of revenue due to Cyber-attack on GE Smart Meter = (137715467 kWh X 17.41 cents per kWh [52]) = $23.97 Million in 15 days.
- Loss of power due to security attack on GE Smart Meter/Smart Grid = (6,040,152,083 X 3.72 % reported loss from equation 3) in 30 days = 224,693,657 kWh.
- Total Loss of revenue due to Cyber-attack on GE Smart Meter/Smart Grid = (224,693,657 kWh X 17.41 cents per kWh [52]) = $39.11 Million in 30 days.
- Loss of power due to security attack on LG Smart Meter = (6,040,152,083 X 2.47 % reported loss from equation 2) in 15 days = 148587741 kWh.
- Total Loss of revenue due to Cyber-attack on LG Smart Meter/Smart = (148587741 kWh × 17.41 cents per kWh [52]) = $25.87 Million in 15 days.
- Loss of power due to security attack on LG Smart Meter/Smart Grid = (6,040,152,083 × 3.96 % reported loss from equation 4) in 30 days = 239190022 kWh.
- Total Loss of revenue due to Cyber-attack on LG Smart Meter = (239190022 kWh × 17.41 cents per kWh [52]) = $49.64 Million in 30 days.

Financial loss calculation done above, and their respective values have been summarized in Table 3.

We can see the difference in percentage loss of kWh reported to the remote monitoring station (stationed at the utility company) and overall financial loss incurred because of the cyber-attack. It is also observed that the resilience of the two smart meters were different under the same attack scenarios. GE smart meter was comparatively less impacted than the Landis-Gyr smart meter in terms of lost power-usage data reported to the remote monitoring station. This may be because of hardware/software used by the smart meters and

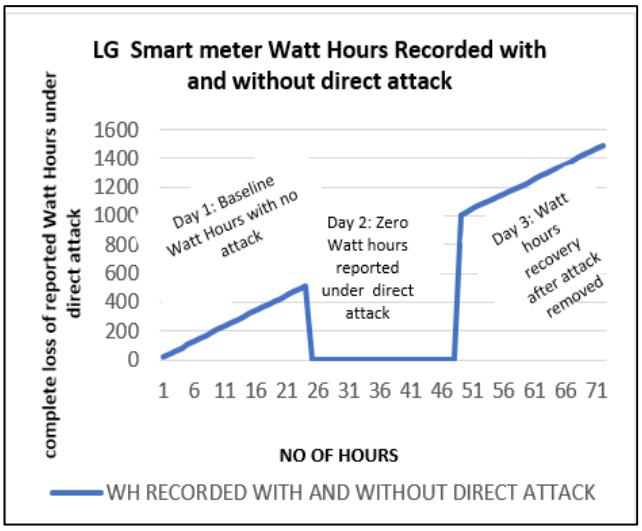


FIGURE 12. Power usage (Watt hour) reported to remote monitoring computer by Landis+Gyr meter for Day1 (normal), Day2 (under direct attack), Day3 (normal).

the fact that they didn't have built-in prevention against these cybersecurity attacks.

Based on these different experiments and the measured results it is obvious that the indirect cyber-attacks can adversely impact the operation of smart meters, which in turn can result in a significant financial loss for a large electric company deployment of smart meters.

Case IV Discussion: Experiment Under Direct Attack for LANDIS+GYR and GE Meters

Independent experiments were conducted on smart meters under direct attack scenarios (Figure 12). These experiments under direct attacks were conducted for 3 days for the two smart meters.

1) Landis+Gyr SMART METER UNDER DIRECT ATTACK

On Day 1, power usage measurement was done without any attack. There was normal data reporting done by the Landis+Gyr smart meter on Day1. On Day 2 (next 24 hours), the Landis+Gyr meter was exposed to the direct attack scenario. As a result, there was a total

$$\begin{aligned} &\%\ \text{Power loss reported after 30 days (based on data from table 2)} \\ &= \frac{\textit{Power Consumption (Baseline)} - \textit{Power Consumption (Cyber Attack)}}{\textit{Power Consumption (Baseline)}} \times 100 \\ &= [(201.7 - 194.2)/201.7] \times 100 = 3.72\% \end{aligned} \tag{3}$$

$$\begin{aligned} &\%\ \text{Power loss reported after 15 days (based on data from table 2)} \\ &= \frac{\textit{Power Consumption (Baseline)} - \textit{Power Consumption (Cyber Attack)}}{\textit{Power Consumption (Baseline)}} \times 100 \\ &= [(201.7 - 193.7)/201.7] \times 100 = 3.96\% \end{aligned} \tag{4}$$

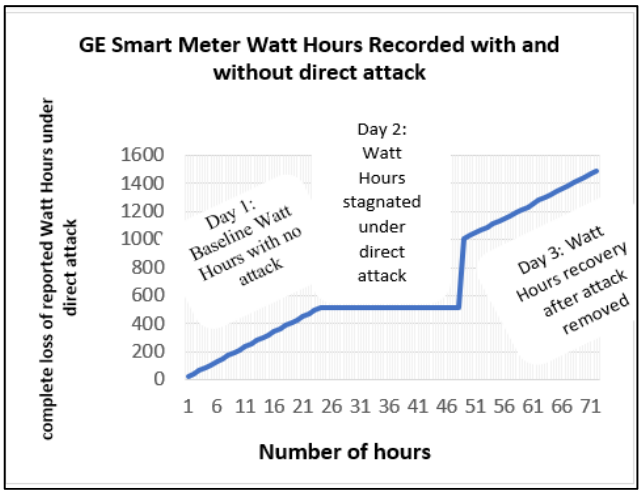


FIGURE 13. Power usage (Watt hour) reported to remote monitoring computer by GE meter for Day1 (normal), Day2 (under direct attack), Day3 (normal).

breakdown of communication of power-usage data from the Landis+Gyr smart meter to the remote monitoring computer (Figure 12). No power usage data could be reported to the remote monitoring computer on Day 2. On Day 3 (next 24 hours), the direct attack was removed, and as a result, the power-usage data started being reported to the monitoring computer in normal fashion, like the baseline Day1 (Figure 12).

This could be likely due to the fact that the Landis+Gyr smart meter used 3rd generation 1 GHZ processor and under attack it lost its processing power and communication abilities needed to implement most of functions such as power usage reporting, dynamic pricing, and other demand response features.

2) GE SMART METER UNDER DIRECT ATTACK

On Day-1 without attack there was no adverse impact on data recording for GE meter. On Day-2 under direct attack, only old power usage data was communicated repeatedly from the GE smart meter to the monitoring station. There was a problem of repeated reporting of old stale power usage data but there was no complete breakdown of communication unlike Landis+Gyr smart meter. This could be because GE smart meter used a more powerful processor i.e. Intel core duo 1.8 GHz processor and under attack it didn't lose all its processing power and communication abilities. After the attacked being removed on Day3, the data reporting returned to normal operation (Figure 13).

VIII. CONCLUSION

For the first time, commercial grade smart meters have been subjected to real security attack scenarios of different types to understand their behavior under attack conditions and to help conduct risk assessment. Smart meters are very useful for utility companies for remote collection of power-usage data from customer premises, to provide uninterrupted power monitoring and easy trouble shooting for today's smart power grid systems. The security resilience of these commercial grade smart meters against data security attacks is not well studied under real attack-traffic scenarios. In this work, we set out to conduct real experiments involving commercial grade smart meters from GE and Landis+Gyr that are being deployed by leading utility companies, to measure their performance under common cybersecurity data-attack traffic. Contributions and findings of this experimental work are summarized as follows: (i) we used commercial grade smart electric meters from two different leading vendors who are actively deploying their smart meters globally, (ii) we first established the baseline performance of meters under absence of any attacks and then we experimentally measured their performance under direct and indirect cyber security attacks to understand resilience of their operation and communication with the remote monitoring station, (iii) we conducted experiments for a duration of 15-days and then for a longer duration of 30-days separately under indirect attacks for both meters, (iv) we found that under indirect cybersecurity attack, both meters reported a gradual decline in power-loss to the remote monitoring station for both scenarios of 15-days and 30-days measurements. Landis+Gyr smart meter reported a bit larger degradation of the reported power-usage data compared with that of the GE smart meter, which was attributed to the different hardware being used, (v) under direct attack, we found that the LG meter completely lost its ability to communicate power-usage data to the remote monitoring station and in effect zero Watt hour was reported under the condition of the direct attack (as if it was not operational), (vi) On the other hand, under direct attack, GE smart meter unlike the Landis+Gyr smart meter, didn't experience a complete breakdown in data communication with the remote monitoring station during the attack, instead it continued repeated reporting of same old (stale) power-usage data that it did just before the attack, (vii) Both meters resumed their normal reporting operation when the direct attacks were removed, (viii) we discovered that even a common cyber security attack such as ICMP based flood attack of rather a low intensity had an adverse impact on operation of a smart electric meter, (xi) we calculated that these cyber security attacks can result in a significant financial loss in millions of dollars for a typical power company's large-scale deployment of smart meters. Our findings from this work show that the commercial smart meters will need to be designed differently than what has been deployed today, to include a robust, attack resistant hardware/software co-design. This will make these smart meters more resilient to common cybersecurity attacks or similar new modified attacks (zero-day attacks). In the lack of robust smart meters or network monitoring systems, zero-day attacks may go undetected by security monitoring Intrusion detection systems.

ACKNOWLEDGMENT

All opinions expressed in this article are the author's and do not necessarily reflect the policies and views of DHS, DOE or ORAU/ORISE.

REFERENCES

[1] L. L. Win and S. Tonyali, "Security and privacy challenges, solutions, and open issues in smart metering: A review," in *Proc. 6th Int. Conf. Comput. Sci. Eng. (UBMK)*, Sep. 2021, pp. 800–805, doi: 10.1109/UBMK52708.2021.9558912.

[2] A. I. Kawoosa and D. Prashar, "A review of cyber securities in smart grid technology," in *Proc. 2nd Int. Conf. Comput., Autom. Knowl. Manage. (ICCAKM)*, Jan. 2021, pp. 151–156, doi: 10.1109/ICCAKM50778.2021.9357698.

[3] S. Saadat, S. Bahizad, T. Ahmed, and S. Maingot, "Smart grid and cybersecurity challenges," in *Proc. 5th IEEE Workshop Electron. Grid (eGRID)*, Nov. 2020, pp. 1–8, doi: 10.1109/eGRID48559.2020.9330660.

[4] G. Rajendran, H. Vardhan Sathyabalu, M. Sachi, and V. Devarajan, "Cyber security in smart grid: Challenges and solutions," in *Proc. 2nd Int. Conf. Power Embedded Drive Control (ICPEDC)*, Aug. 2019, pp. 546–551, doi: 10.1109/ICPEDC47771.2019.9036484.

[5] T. Lieskovan, J. Hajny, and P. Cika, "Smart grid security: Survey and challenges," in *Proc. 11th Int. Congr. Ultra Modern Telecommun. Control Syst. Workshops (ICUMT)*, Oct. 2019, pp. 1–5, doi: 10.1109/ICUMT48472.2019.8970738.

[6] Y. Wang, Q. Chen, T. Hong, and C. Kang, "Review of smart meter data analytics: Applications, methodologies, and challenges," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 3125–3148, May 2019, doi: 10.1109/TSG.2018.2818167.

[7] P. Kumar, Y. Lin, G. Bai, A. Paverd, J. S. Dong, and A. Martin, "Smart grid metering networks: A survey on security, privacy and open research issues," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2886–2927, 3rd Quart., 2019, doi: 10.1109/COMST.2019.2899354.

[8] A. Cooper, M. Shuster, and J. Lash, "Electric company smart meter deployments: Foundation for a smart grid (2021 update)," Edison Found. Inst. Electr. Innov., IEI Smart Meter Report, Tech. Rep., Apr. 2021. [Online]. Available: https://www.edisonfoundation.net//media/Files/IEI/publications/IEI_Smart_Meter_Report_April_2021.pdf

[9] B. Chaudhari and S. Borkar, "Design considerations and network architectures for low-power wide-area networks," in *LPWAN Technologies for IoT and M2M Applications*, B. S. Chaudhari and M. Zennaro, Eds. New York, NY, USA: Academic, 2020, pp. 15–35, doi: 10.1016/B978-0-12-818880-4.00002-8.

[10] S. Kumar, H. Kumar, and G. R. Gunnam, "Security integrity of data collection from smart electric meter under a cyber attack," in *Proc. 2nd Int. Conf. Data Intell. Secur. (ICDIS)*, Jun. 2019, pp. 9–13, doi: 10.1109/ICDIS.2019.00009.

[11] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," *Comput. Netw.*, vol. 169, Mar. 2020, Art. no. 107094, doi: 10.1016/j.comnet.2019.107094.

[12] V. Kayalvizhy and A. Banumathi, "A survey on cyber security attacks and countermeasures in smart grid metering network," in *Proc. 5th Int. Conf. Comput. Methodologies Commun. (ICCMC)*, 2021, pp. 160–165, doi: 10.1109/ICCMC51019.2021.9418303.

[13] V. D. Menon, J. T. Kumar, M. Sabhanayagan, A. Ramkumar, and K. Rajesh, "Cyber security for smart meters," in *Proc. IEEE Int. Conf. Intell. Techn. Control, Optim. Signal Process. (INCOS)*, Apr. 2019, pp. 1–5, doi: 10.1109/INCOS45849.2019.8951407.

[14] S. Tweneboah-Koduah, A. K. Tsetse, J. Azasoo, and B. Endicott-Popovsky, "Evaluation of cybersecurity threats on smart metering system," in *Information Technology—New Generations* (Advances in Intelligent Systems and Computing), vol. 558, S. Latifi, Ed. Cham, Switzerland: Springer, 2018, doi: 10.1007/978-3-319-54978-1_28.

[15] S. McLaughlin, D. Podkuiko, and P. McDaniel, "Energy theft in the advanced metering infrastructure," in *Proc. 4th Int. Conf. Inf. Infrastructures Secur.*, 2009, pp. 176–187.

[16] P. Yi, T. Zhu, Q. Zhang, Y. Wu, and J. Li, "A denial of service attack in advanced metering infrastructure network," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2014, pp. 1029–1034, doi: 10.1109/ICC.2014.6883456.

[17] R. Anderson and S. Fuloria, "Who controls the off switch?" in *Proc. 1st IEEE Int. Conf. Smart Grid Commun.*, Oct. 2010, pp. 96–101, doi: 10.1109/SMARTGRID.2010.5622026.

[18] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE Secur. Privacy Mag.*, vol. 7, no. 3, pp. 75–77, May 2009, doi: 10.1109/MSP.2009.76.

[19] F. M. Cleveland, "Cyber security issues for advanced metering infrastructure (AMI)," in *Proc. IEEE Power Energy Soc. Gen. Meeting Convers. Del. Electr. Energy 21st Century*, Jul. 2008, pp. 1–5, doi: 10.1109/PES.2008.4596535.

[20] M. I. Ibrahem, M. M. E. A. Mahmoud, F. Alsolami, W. Alasmary, A. S. A. Al-Ghamdi, and X. Shen, "Electricity-theft detection for change-and-transmit advanced metering infrastructure," *IEEE Internet Things J.*, vol. 9, no. 24, pp. 25565–25580, Dec. 2022, doi: 10.1109/JIOT.2022.3197805.

[21] M. D. Hossain, H. Ochiai, T. Arisawa, and Y. Kadobayashi, "Smart meter Modbus RS-485 spoofing attack detection by LSTM deep learning approach," in *Proc. 9th Swiss Conf. Data Sci. (SDS)*, Jun. 2022, pp. 47–52, doi: 10.1109/SDS54800.2022.00015.

[22] N. Iliaee, S. Liu, and W. Shi, "Non-intrusive load monitoring based demand prediction for smart meter attack detection," in *Proc. Int. Conf. Control, Autom. Inf. Sci. (ICCAIS)*, Oct. 2021, pp. 370–374, doi: 10.1109/ICCAIS52680.2021.9624524.

[23] C. Sun, D. J. S. Cardenas, A. Hahn, and C. Liu, "Intrusion detection for cybersecurity of smart meters," *IEEE Trans. Smart Grid*, vol. 12, no. 1, pp. 612–622, Jan. 2021, doi: 10.1109/TSG.2020.3010230.

[24] A. M. Khattak, S. I. Khanji, and W. A. Khan, "Smart meter security: Vulnerabilities, threat impacts, and countermeasures," in *Proc. 13th Int. Conf. Ubiquitous Inf. Manag. Commun. (IMCOM)*, in Advances in Intelligent Systems and Computing, vol. 935, S. Lee, R. Ismail, H. Choo, Eds. Cham, Switzerland: Springer, 2019, pp. 554–562, doi: 10.1007/978-3-030-19063-7_44.

[25] *EPM 6100 Power Quality Meter Energy and Demand Submeter With WiFi, Instruction Manual, GE Grid Solutions*. [Online]. Available: http://www.gegridsolutions.com/app/ViewFiles.aspx?prod=epm6100&type=3

[26] National Instruments. (Apr. 17, 2018). *RS-232-RS-422, RS-485 Serial Communication General Concepts*. [Online]. Available: http://www.ni.com/white-paper/11390/en/

[27] Acromag. (2005). *Introduction to MODBUS TCP/IP*. [Online]. Available: https://www.prosoft-technology.com/kb/assets/intro_modbustcp.pdf

[28] Modbus-IDA. (2006). *Modbus Messaging on TCP/IP Implementation Guide V1.0b*. [Online]. Available: http://www.modbus.org/docs/Modbus_Messaging_Implementation_Guide_V1_0b.pdf

[29] *Lyndis+Gyr E650 SX4 Industrial and Commercial Meter, Instruction Manual*. [Online]. Available: https://www.landisgyr.com/product/e650-s4x-meter/

[30] National Electrical Manufacturers Association. (1996). *Protocol Specification for ANSI Type 2 Optical Port*. [Online]. Available: https://www.nema.org/Standards/ComplimentaryDocuments/ANSI%20C12.18_2006%20R2016%20Contents%20and%20Scope.pdf

[31] National Electrical Manufacturers Association. (1996). *Protocol Specification for Telephone Modem Communication*. [Online]. Available: https://www.nema.org/Standards/ComplimentaryDocuments/ANSI-C12-18.pdf

[32] S. Mishra and P. S. Chatterjee, "A systematic survey on DDoS attack and data confidentiality issue on cloud servers," in *Proc. 19th OITS Int. Conf. Inf. Technol. (OCIT)*, Dec. 2021, pp. 273–278, doi: 10.1109/OCIT53463.2021.00062.

[33] S. Alshamakhi and S. Manimurugan, "Distributed denial-of-service in IoT: Survey," in *Proc. Int. Conf. Comput. Inf. Technol. (ICCIT)*, Sep. 2020, pp. 1–4, doi: 10.1109/ICCIT-144147971.2020.9213741.

[34] A. Praseed and P. S. Thilagam, "DDoS attacks at the application layer: Challenges and research perspectives for safeguarding Web applications," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 661–685, 1st Quart., 2019, doi: 10.1109/COMST.2018.2870658.

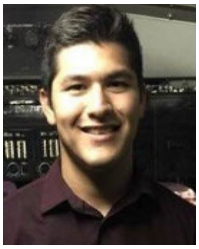
[35] A. Aldaej, "Information security and distributed denial of service attacks: A survey," in *Proc. Int. Conf. Electr. Comput. Technol. Appl. (ICECTA)*, Nov. 2017, pp. 1–6, doi: 10.1109/ICECTA.2017.8252045.

[36] A. Bhardwaj, G. V. B. Subrahmanyam, V. Avasthi, H. Sastry, and S. Goundar, "DDoS attacks, new DDoS taxonomy and mitigation solutions—A survey," in *Proc. Int. Conf. Signal Process., Commun., Power Embedded Syst. (SCOPES)*, 2016, pp. 793–798, doi: 10.1109/SCOPES.2016.7955549.

[37] T. Kaur, K. K. Saluja, and A. K. Sharma, "DDOS attack in WSN: A survey," in *Proc. Int. Conf. Recent Adv. Innov. Eng. (ICRAIE)*, Dec. 2016, pp. 1–5, doi: 10.1109/ICRAIE.2016.7939566.

[38] K. N. Mallikarjunan, K. Muthupriya, and S. M. Shalinie, "A survey of distributed denial of service attack," in *Proc. 10th Int. Conf. Intell. Syst. Control (ISCO)*, Jan. 2016, pp. 1–6, doi: 10.1109/ISCO.2016.7727096.
[39] H. Kumar, "Cyber security evaluation of smart electric meters," M.S. thesis, Dept. Elect. Eng., Univ. Texas RGV, Edinburg, TX, USA, 2020.
[40] S. Kumar, "Smurf-based distributed denial of service (DDoS) attack amplification in internet," in *Proc. 2nd Int. Conf. Internet Monitor. Protection (ICIMP)*, Jul. 2007, p. 25, doi: 10.1109/ICIMP.2007.42.
[41] K. Sundar and S. Kumar, "Blue screen of death observed for Microsoft windows server 2012 R2 under DDoS security attack," *J. Inf. Secur.*, vol. 7, no. 4, pp. 225–231, 2016, doi: 10.4236/jis.2016.74018.
[42] S. Kumar, S. Member, and R. S. R. Gade, "Evaluation of Microsoft windows servers 2008 & 2003 against cyber attacks," *J. Inf. Secur.*, vol. 6, no. 2, pp. 155–160, 2015, doi: 10.4236/jis.2015.62016.
[43] R. B. Junior and S. Kumar, "Apple's lion vs Microsoft's windows 7: Comparing built-in protection against ICMP flood attacks," *J. Inf. Secur.*, vol. 5, no. 3, pp. 123–135, 2014, doi: 10.4236/jis.2014.53012.
[44] R. Sekhar Reddy Gade, H. Vellalacheruvu, and S. Kumar, "Performance of windows XP, windows vista and Apple's leopard computers under a denial-of-service attack," in *Proc. 4th Int. Conf. Digit. Soc.*, Feb. 2010, pp. 188–191, doi: 10.1109/ICDS.2010.39.
[45] W. Stallings, *Data and Computer Communications*, 10th ed. 2018. [Online]. Available: https://nibmehub.com/opacservice/pdf/read/Data%20and%20computer%20communications%20by%20Stallings-%20William-compressed.pdf
[46] A. Gaurav, B. B. Gupta, W. Alhalabi, A. Visvizi, and Y. Asiri, "A comprehensive survey on DDoS attacks on various intelligent systems and it's defense techniques," *Int. J. Intell. Syst.*, vol. 37, no. 12, pp. 1–25, 2022, doi: 10.1002/int.23048.
[47] S. Q. A. Shah, F. Z. Khan, and M. Ahmad, "The impact and mitigation of ICMP based economic denial of sustainability attack in cloud computing environment using software defined network," *Comput. Netw.*, vol. 187, Mar. 2021, Art. no. 107825, doi: 10.1016/j.comnet.2021.107825.
[48] M. Yaibuates and R. Chaisricharoen, "A Combination of ICMP and ARP for DHCP Malicious Attack Identification," in *Proc. Joint Int. Conf. Digit. Arts, Media Technol. ECTI Northern Section Conf. Elect., Electron., Comput. Telecommun. Eng. (ECTI DAMT & NCON)*, 2020, pp. 15–19, doi: 10.1109/ECTIDAMTNCON48261.2020.9090760.
[49] F. A. Barbhuiya, S. Roopa, R. Ratti, S. Biswas, and S. Nandi, "An active detection mechanism for detecting ICMP based attacks," in *Proc. IEEE 11th Int. Conf. Trust, Secur. Privacy Comput. Commun.*, 2012, pp. 51–58, doi: 10.1109/TrustCom.2012.68.
[50] G. R. Gunnam and S. Kumar, "Do ICMP security attacks have same impact on servers?" *J. Inf. Secur.*, vol. 8, no. 3, pp. 274–283, 2017, doi: 10.4236/jis.2017.83018.
[51] S. Kumar and O. Gomez, "Denial of service due to direct and indirect ARP storm attacks in LAN environment," *J. Inf. Secur.*, vol. 1, no. 2, pp. 88–94, 2010, doi: 10.4236/jis.2010.12010.
[52] Independent Statistics & Analysis. *U.S. Energy Information Administration*. [Online]. Available: https://www.eia.gov/energyexplained/index.cfm?page=electricity_ho me#tab

HARSH KUMAR (Member, IEEE) received the bachelor's degree in electrical engineering from Gujarat Technological University, Ahmedabad, and the master's degree from the Department of Electrical and Computer Engineering, The University of Texas Rio Grande Valley (UTRGV), Edinburg, TX, USA. He is currently pursuing the Ph.D. degree with the Department of Electrical and Computer Engineering, The University of New Mexico, Albuquerque, NM, USA. He was a Shift Engineer with Prime Health Care Products and the Operations Manager with Eram Scientific Solutions Pvt. Ltd. His research interests include cyber security, the IoT, and smart electric grids.



OSCAR. A. ALVAREZ (Member, IEEE) received the bachelor's degree in engineering physics specializing in computer engineering and the master's degree in electrical and computer engineering from The University of Texas Rio Grande Valley (UTRGV). He is currently a Software Research and Development Engineer with Landis + Gyr Inc.

SANJEEV KUMAR (Senior Member, IEEE) received the Ph.D. degree from the Department of Electrical and Computer Engineering, North Carolina State University, Raleigh, North Carolina. He is currently a Full Professor with the Department of Electrical and Computer engineering, The University of Texas Rio Grande Valley (UTRGV). He is active in teaching and research in the area of computer network security, the IoT, AI applications, cloud computing, critical infrastructure security, and wireless ad hoc networks. Before joining UTRGV, he was with leading Computer Networking companies in USA. He served as a member of the technical program committee for numerous national and international conferences. He was awarded the U.S. and international patents for his inventions in internet technologies. He received many teaching excellence awards at his university, including the prestigious UT System Regents' Outstanding Teaching Award (ROTA). He served on editorial board of several journals.