Experimentations for Enhancing Data Security Resilience of Energy Infrastructure

Max Garcia, *IEEE Student Member*, Sanjeev Kumar, *IEEE Senior Member*
Department of Electrical and Computer Engineering,
The University of Texas- RGV, Edinburg, TX 78539, USA
Correspondence Email: sj.kumar@utrgv.edu

2025 IEEE 15th Annual Computing and Communication Workshop and Conference (CCWC) | 979-8-3315-0769-5/25/$31.00 ©2025 IEEE | DOI: 10.1109/CCWC62904.2025.10903923

***Abstract*—Cyberattacks against critical energy infrastructure are becoming more common for adversaries. The Smart Grid is a critical energy infrastructure used in distribution and management of electrical power needed for everyday life. One of the advantages of a smart grid is its scalability due to its remote monitoring capabilities provided by Smart Grid Power Meters. In this experimental work, we investigated the security vulnerabilities found in Smart Electric Meters, a critical component for the Smart Power Grid. In our study, we conducted experiments to mimic the operational behavior of smart meters with the goal of studying the vulnerabilities of these meters under attack scenarios. To do this, a prototype of a Smart Grid Network was designed in a lab environment using physical data networking devices and Smart Grid Power Meters. Experiments were designed to study the operation of smart meters under malicious attack traffic of different types. We discovered several vulnerabilities, and it allowed us to consider designing solutions to mitigate those problems. Our experimental work is aimed at raising awareness, which will encourage further studies and industrial implementation to strengthen the security of critical infrastructure needed for everyday life.**

Keywords—Electric Smart Grid, Smart Meter, AMI, Cybersecurity, Infrastructure

I. Introduction

The security of critical energy infrastructure, such as the Smart Grid, is becoming increasingly important due to the rising frequency of cyberattacks. This project investigates vulnerabilities in Smart Electric Meters, a critical component of the Smart Power Grid, through a serious of experiments that mimic operational behavior under attack scenarios. By designing a Smart Grid Network in a lab environment using physical data networking devices and Smart Grid Power Meters, we are able to study the operation of Smart Grid Power Meters under different types of malicious attack traffic.

This project focuses on how the electric Smart Grid infrastructure is affected by cybersecurity attacks. Smart Power Grids use network communication techniques seen in wired and wireless networks such as: Ethernet, Wi-Fi, ZigBee, cellular, and others. However, with this increased reliance on networking, there may be an increased risk of cyberattack vulnerabilities. Increase in commercial computing power is resulting in cyberattack execution without the need of specialized equipment or sophisticated coordinated attack networks. While specialized equipment or sophisticated attacks are more potent, modern laptop computers can send enough traffic to disrupt devices of lesser computational resources. Experimentation in this paper demonstrates how network exploits using a typical computer affect the Smart Power Grid critical infrastructure.

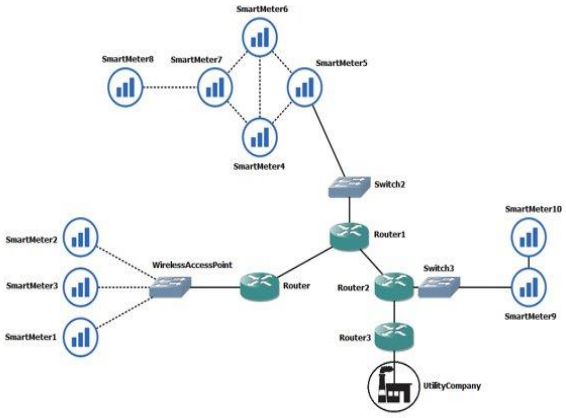

Figure 1. Example Smart Grid Data Network

Figure 1. is an example of what a smart grid system may look like from a data network perspective. On the left, is an example of a wireless local area network. On the top, an example of an ad-hoc network where meters can connect to other meters to relay the data. On the right is a wired local area network. All of these can also be used in combination to communicate data over the network to the utility company. It is important to note that since these power meters may handle information for more than one power meter, if a device is disconnected it might remove more than one power meter from the network.

II. Background

In a traditional electric power grid, a power utility company would produce and provide electricity to their customers and send technicians to record power usage measured by the power meters at the customer's location, so they are able to be billed. The electric Smart Grid functions similarly to a traditional electric power grid by providing electricity to consumers with additional improvements in scalability, reliability, and monitoring due to the Smart Grid's ability to have consumers actively participate in the Smart Grid network. What this means is that consumers can not only frequently provide information on their power usage but can also contribute to the energy generation on the network. For example, a homeowner with solar roof panels can provide their excess generated electricity to the Smart Grid network. This type of interaction is possible in a Smart Grid while not possible in a traditional electric power network due to the two-way communication a Smart Grid provides [1][2].

A. Smart meter deployment

Smart Grid Smart Power Meters provide the critical interface between customer premises and utility companies and are the main device utilizing the two-way data communication a smart grid provides. In 2020, U.S. electric utility companies installed over 100 million smart metering devices; 88% of which were for residential use [3]. It is

979-8-3315-0769-5/25/$31.00 ©2025 IEEE

estimated that at least 75% of U.S. households already have smart meters deployed [4].

B. Smart Grid Data Communication Protocols

Smart grid power meters are typically connected to the smart grid network through a variety of communication technologies. Some of the most common methods include wired connections, wireless connections, and hybrid connections. Smart meters can be connected to the smart grid network through wired connections such as Ethernet cables or power line communication (PLC) technology. Ethernet cables are commonly used for meters installed in commercial or industrial settings, while PLC technology allows for the use of existing power lines for communication in residential areas. Smart meters connected to the smart grid network wirelessly use technologies such as Wi-Fi, Zigbee, RF and cellular networks. Wireless connections are more flexible and allow for easier installation in areas where wired connections are difficult. A hybrid connection can combine wired and wireless technologies to provide a more robust and reliable communication path. For example, a smart meter might use a wireless Wi-Fi connection as the primary communication path, with a wired Ethernet connection as a backup. The specific method of connection used for a particular smart meter installation depends on a variety of factors, including the type of meter, the location of the installation, and the availability of communication infrastructure in the area.

Along with data transfer protocols, Smart Power Grids utilize communication and control protocols such as Modbus. Modbus is a widely used communication protocol in electric smart grid power meters. It is a serial communication protocol that allows devices such as power meters, PLCs, and other smart grid components to communicate with each other. The Modbus protocol typically uses master-slave architecture, where a master device, such as a monitoring system or SCADA, sends commands to one or more slave devices, such as power meters. In the context of electric smart grid power meters, Modbus is typically used to read and write data to and from the meter. This data can include information such as current and voltage readings, power consumption, and other operational parameters. Modbus can be implemented over a variety of physical communication media, in our case TCP/IP. The flexibility of Modbus makes it a popular choice for electric smart grid power meters, which often require communication across different types of networks.

C. Scope of our experimental study in this paper

The electric Smart Grid heavily relies on two way data communication between the utility company and the customer. Alterations in data confidentiality, integrity, or availability of data on the Smart Grid network cause interruptions to critical infrastructure. Understanding the resilience and capabilities of the Smart Grid network allows for vulnerabilities to be addressed. To better understand the Smart Grid network, we focused on the following questions:

- What is the impact on metered data communication due to the cyberattacks on the Smart Grid networking devices?
- What is the impact on metered data communication due to the cyberattacks on the Smart Grid power meters?

Cyberattacks used to answer these questions included few common flood attacks, unintended access to information, and denial-of-service attacks in Wi-Fi based smart meters.

A flood attack aims to exhaust computation resources on a network. By flooding the computational resources of a network, the attacker can slow down or halt data processing and communication. ICMP (Internet Control Message Protocol) flood and TCP-SYN (Transmission Control Protocol – Synchronization) flood attacks are used in the experimental setup, Unintended access to information is achieved by utilizing the Modbus, and exploits in the Wi-Fi protocol allow for a denial-of-service attack on the wireless smart power meter.

III. EXPERIMENTAL SET UP

A. Lab setup for an experimental Smart Grid

The Smart Grid used for testing comprised of a switch, a router, a wireless access point, two smart meters, a remote monitoring station and two lightbulbs as a load. With the network built, we were able to obtain baseline data so that we are able to compare the baseline data to data acquired under attack conditions. Two lightbulbs with a load of 200W was used and the meters were wired to measure power usage in Watt-Hours (Wh). Figure 1. shows what the lab setup looked like.

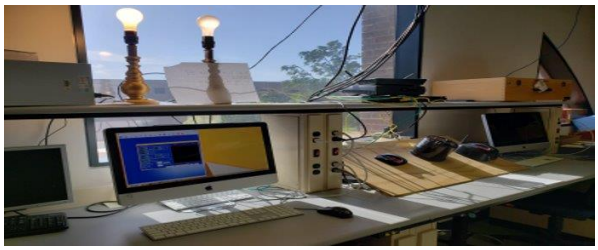

Figure 1. Lab Experimental Setup for Smart Grid Network

B. Data network Topology used for experiments

Figure 2. is what the network topology of our experimental setup looks like. From left to right, the wireless smart meter is wirelessly connected via Wi-Fi to a wireless access point which is connected to the rest of the network via a router. To the right of the router is the wired network consisting of the wired smart meter and the remote monitoring station; both connected via wired ethernet.

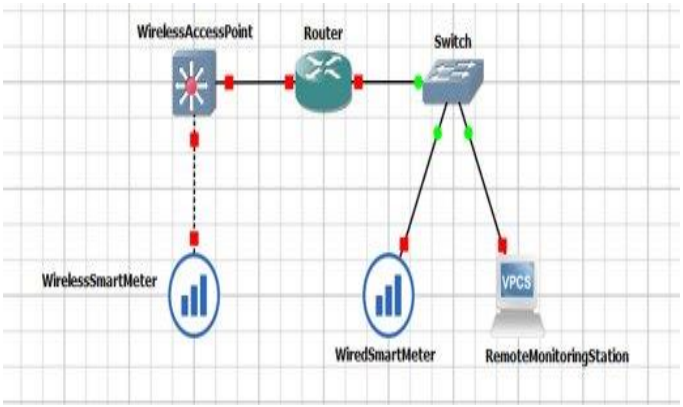

Figure 2. Lab Smart Grid Topology

C. Smart meters used for security vulnerability testing

In this paper, two commercial grade smart meters were used, viz. the General Electric EPM 6100 and the General

Electric 7000. The GE EPM 6100 is capable of wireless communication via Wi-Fi. As such, the GE EPM 6100 was connected to the network via a wireless access point [5]. The GE EPM 7000 is capable of only wireline Ethernet, as such it was connected via Ethernet to a switch on the network [6]. This setup allows for an environment that may represent a simple smart grid network for data communication. Power delivery to the meters and the loads are done through the lab bench's power outlets with the meters configured to measure the power usage of the load (Figure 1).

Figure 3. GE Electric Power Meter, EPM-6100

Figure 4. GE, Electric Power Meter, EPM-7000

D. *Measurement results for Baseline operation (no attack)*

With the smart grid network constructed we ran a baseline test for 5 days to see what the meters should report under no attack conditions. Figure 3. shows results. The numbers gathered are within our calculated expected values per day.

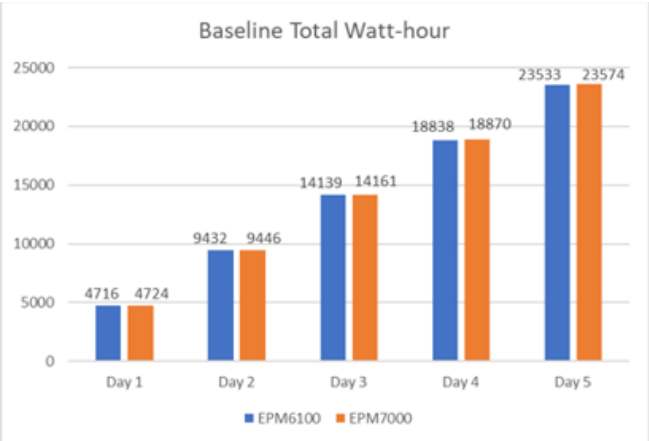

Figure 3. Baseline Results Under No Attack

E. *Cybersecurity attacks used for vulnerability testing*

There have been some previous experimental works done in studying the vulnerabilities of smart meters [7-11], however in this paper, we have considered different approaches and vulnerabilities affecting operation of smart meters in the network. Figure 4 represents possible entry points for malicious actors into a network. Assuming access to the network, an attacker can send malicious data to networking devices or the meters themselves. The attacks we focused on were ICMP ping floods and TCP/SYN floods which are types of resource exhaustion attacks [8]. Modbus command vulnerabilities and Wi-Fi De-Authentication vulnerabilities are types of device specific exploit attacks and were also used. Every device, excluding the attackers, shown in Figure 4. Were independently targeted in resource exhaustion attacks. The meters were additionally targeted with Modbus exploits and the wireless access point was targeted with Wi-Fi De-Authentication attacks.

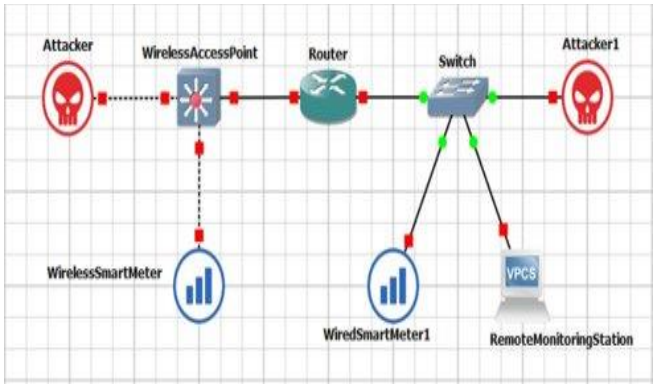

Figure 4. Malicious Actor Entry Points

IV. EXPERIMENTAL RESULTS AND DISCUSSION

A. *Flood based DDoS attacks*

The results of an attack targeting the remote monitoring station with an ICMP [12] ping flood are shown in Figure 5. On day 1, after several hours under attack, the communication between the monitoring station and the EPM7000 smart meter was severed and remained disconnected throughout the duration of the attack. On Day 4, the attack was stopped, and the meter was able to recover. Importantly, the integrity of the data was not affected by the attack. Meaning, the meter continued to accurately accumulate power usage even though it was unable to remotely report the data. Results like those shown in Figure 5. are seen on tests targeting other networking devices on the smart grid network.

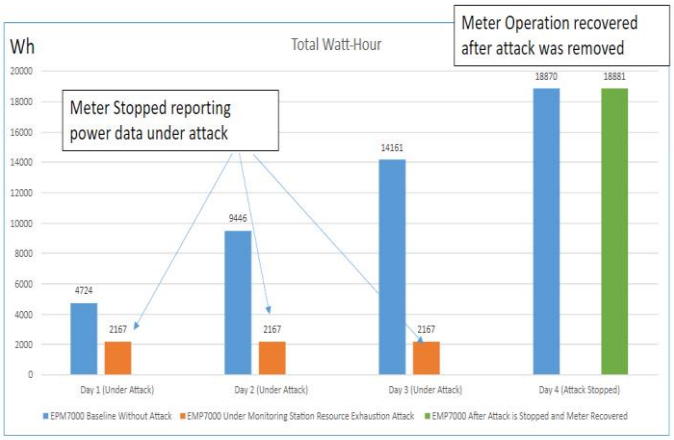

Figure 5. Monitoring Station Under Resource Exhaustion Attack

B. *Resilience measurements for the Smart Meters*

Using ICMP Ping [12] and TCP/SYN messages [13], we conducted experiments directed towards smart meters which allowed us to create a performance profile of the smart meters regarding how resilient they were to the flood attacks. We

measured the parameter, “Time-to-Stop”, which is the time it took for an attack to completely stop smart meter communication with the remote monitoring station. This parameter was used to measure the resilience profile of the smart meters. Bigger the Time-to-Stop value, bigger was the resilience of the meter to the attacks. The results for the EPM7000, shown in Figure 6., were not obvious before this experiment, since a relatively small flood of 3Kbs was able to disconnect the meter within an hour. Note that the meters are rated to support 10Mbs.

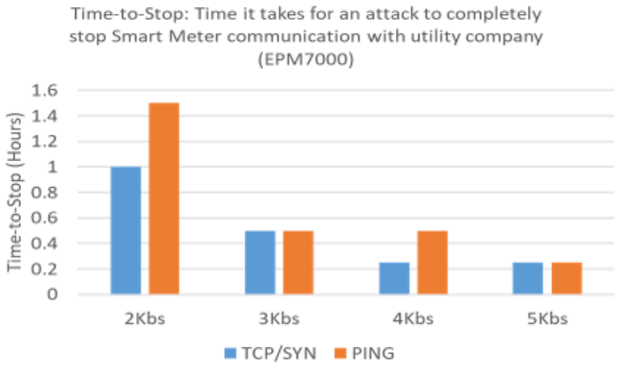

Figure 6. EPM7000 Resilience Profile

A similar resilience profile was measured for the EPM6100. However, the EPM6100 was found to be more resilient compared to the EMP7000 since it was able to handle an attack at its 10Mbs rating for multiple hours before disconnection. These results are interesting because common personal computers and laptops come with networking capabilities of at least 1Gbs which is more than enough to cause this type of attack.

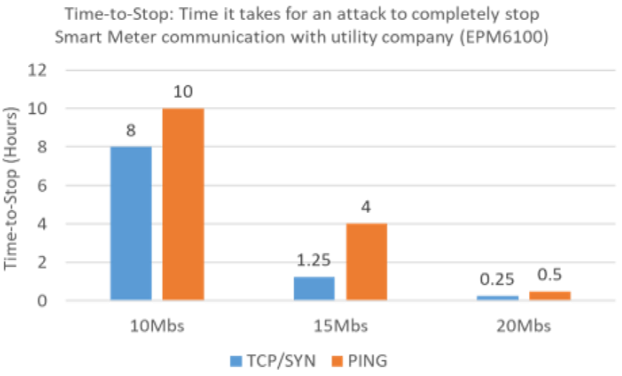

Figure 7. EPM6100 Resilience Profile

C. *Modbus protocol security vulnerability*

The Modbus protocol is a common protocol used by control and monitoring systems like smart meters. Modbus allows for memory reading and memory writing which is how data is stored and read [14]. The Modbus protocol rides on the TCP in the TCP data unit. TCP provides a way to establish connections and the Modbus protocol executes any command riding on an established TCP connection. What this means, is that if you can connect to the meter, which is how remote monitoring is handled, then you can send it Modbus commands to read or write to registers without authentication. When we tested this on our meters, we were able to read the registers of one of the meters (EPM 6100) but not on EPM 7000, and we were unable to write to either of those meters. What this means is that there is a nonstandard configuration that, if the manufacturer ignores or is unaware of, could cause privacy violation of power-usage data stored in a smart grid environment.

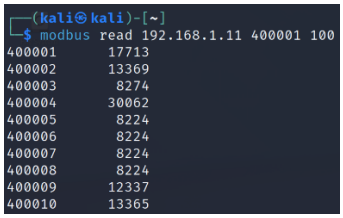

Figure 8. Unintended Access to Smart Meter Information

D. *Wi-Fi De-Authentication Attack*

Wi-Fi De-Authentication targets a wireless access point and causes a victim device to become disconnected from the network. This attack exploits the good-faith nature of a wireless access point by sending malicious requests to the wireless access point using a wireless networking adapter. The wireless networking adapter used to perform this can be configured into monitoring mode which allows for capture of all nearby packets on all channels of the Wi-Fi frequency to be received [15]. Normally this isn’t an issue since these packets are encrypted. However, when a device requests to connect or disconnect to a wireless network via Wi-Fi, the header must be unencrypted so the wireless access point may understand it. Under this condition, and by acquiring the media access control address (MAC) of the wireless access point and the target, an attacker can forge packets to instruct the wireless access point to disconnect the smart meter.

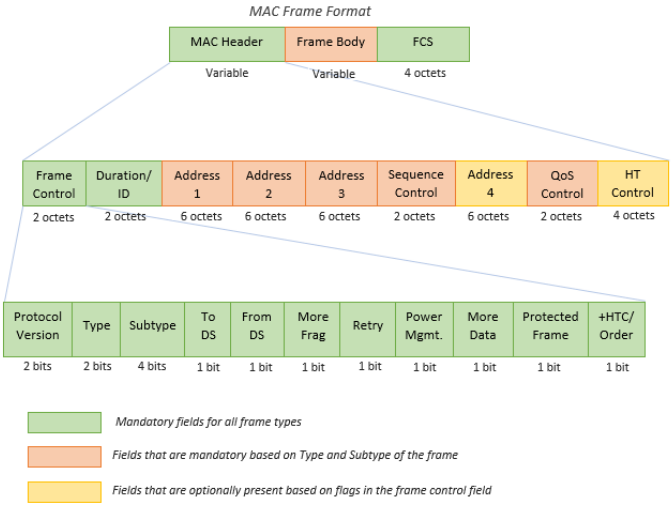

Figure 9. Wi-Fi MAC Frame Format [16]

In our experimentation, we were able to cause the wireless Smart Grid Power Meter to be disconnected from the network under the Wi-Fi de-authentication attack. The attack was executed even without knowledge of the Smart Grid Power Meter’s MAC address. It was achieved by allocating all MAC addresses, 00:00:00:00:00:00 – ff:ff:ff:ff:ff:ff, as targets. A more covert attack can cause only the targeted Smart Grid Power Meter to disconnect in order to avoid detection. We

theorize that this type of broad Wi-Fi de-authentication attacks covering the entire MAC-address space can be effective on commercial buildings with public Wi-Fi and poor cybersecurity protection. A shopping mall, for example, may have its wireless Smart Grid Power Meters connected to the network via the same wireless-access-point that provides public Wi-Fi. In this scenario, the attacker may utilize the public Wi-Fi to execute the attack.

V. Conclusions

In this paper, we conducted experiments and discovered some security vulnerabilities associated with two commercial grade smart power meters being deployed today. We found these smart-meters to have different level of resilience to the cybersecurity attacks. They were overwhelmed by low bandwidth flood attacks causing a disruption in remote collection of power usage data. We also discovered that the good-faith nature of the Modbus protocol allows for malicious commands to be executed if connection to a smart meter is established. Additionally, we found that the exploits in the Wi-Fi protocol allowed for spoofed packets to cause a smart meter to be disconnected from the smart grid network. The significance of this work is that it has helped us discover vulnerabilities in some of the commercial grade smart meters and the smart grid network infrastructure, which will help us design efficient mitigation strategies to make our critical energy infrastructure more secure.

ACKNOWLEDGEMENTS

This research was, in part, funded by the US DHS Science and Technology Summer Research Team program ORISE, ORAU under DOE contract *DE-SC0014664*; and in part, supported by NSF Award number *2334389*. All opinions expressed in this article are the authors' and do not necessarily reflect the policies and views of DHS, DOE, ORAU/ORISE, or the NSF.

References

[1] "What is the smart grid?," *The Smart Grid | SmartGrid.gov*, 16-Dec-2019. [Online]. Available: https://www.smartgrid.gov/the_smart_grid/. [Accessed: 16-Aug-2022].

[2] The Smart Grid and Renewable Energy – IEEE Innovation at Work, Aug 2020. https://innovationatwork.ieee.org/smart-grid-transforming-renewable-energy, Accessed: 26-Dec-2024

[3] Internet Standards Come to the Advanced Metering Infrastructure (electricenergyonline.com), by R. Acra, M. Thaker, EE Online (ElectricEnergyonline.com) Accessed Aug 2, 2022.

[4] Stockmar, B. (2018). *Staying big or getting smaller*. Energy Atlas 2018: Figures and Facts about Renewables in Europe. Retrieved from https://energytransition.org/2018/04/europe-must-choose-a-green-future

[5] EPM 6100 Multi-function Power Metering System, 1st ed. GE Digital Energy., Markham, Ontario, 2011.

[6] Multilin EPM 7000/7000T Power Quality Meter, 1st ed. GE Grid Solutions., Markham, Ontario, 2016.

[7] H. Kumar, O. A. Alvarez and S. Kumar, "Experimental Evaluation of Smart Electric Meters' Resilience Under Cyber Security Attacks," in *IEEE Access Journal*, vol. 11, pp. 55349-55360, 2023, doi: 10.1109/ACCESS.2023.3278738.

[8] S. Kumar, A. Guerrero and C. Navarro, "Cyber Security Flood Attacks and Risk Assessment for Internet of Things (IoT) Distributed Systems," *2023 IEEE World AI IoT Congress (AIIoT)*, Seattle, WA, USA, 2023, pp. 0392-0397, doi: 10.1109/AIIoT58121.2023.10174553.

[9] Nnaji, H. Kumar and S. Kumar, "Wireless Smart Electric Meter Operation under Data Security Attacks," *2022 IEEE 4th International Conference on Data Intelligence and Security (ICDIS)*, June, 2022, pp. 182-187, doi: 10.1109/ICDIS55630.2022.00035.

[10] Harsh Kumar and Sanjeev Kumar , "Effect of Intermediate Network Systems on Remote Power Data Collection in Smart Grid," *Proceedings of IEEE International Conference on Data Intelligence and Security, vol. 3,* pp. 49-55, June 2020.

[11] S. Kumar, H. Kumar and G. Gunnam, "Evaluation of a Smart Electric Meter under Cyber Attacks," *IEEE International Conference on Data Intelligence and Security, ICDIS'19,* June 2019.

[12] Postel, J., "Internet Control Message Protocol", STD 5, RFC 792, DOI 10.17487/RFC0792, September 1981.

[13] Postel, J., "Transmission Control Protocol", STD 7, RFC 793, DOI 10.17487/RFC0793, September 1981.

[14] Acromag, Inc. (2005). *BusWorks® 9Series 10/100M Industrial Ethernet I/O Modules w/ Modbus Technical Reference – Modbus Tcp/Ip*.

[15] "Documentation," *Aircrack*. [Online]. Available: https://www.aircrack-ng.org/documentation.html#. [Accessed: 20-Aug-2024].

[16] "802.11 mac frame decoding," *802.11 MAC Frame Decoding - MATLAB & Simulink*. [Online]. Available: https://www.mathworks.com/help/wlan/ug/802-11-mac-frame-decoding.html. [Accessed: 20-Aug-2024].