Wireless Smart Electric Meter Operation under Data Security Attacks

Patrick Nnaji
Department of Electrical and Computer Engineering
University of Texas- Rio Grande Valley,
Edinburg, Texas-78539, USA
ORCID ID: 000-0003-2980-9076

Harsh Kumar
Department of Electrical and Computer Engineering
University of New Mexico, Albuquerque,
NM-87106, USA
ORCID ID: 0000-0002-3406-6978

Sanjeev Kumar
Department of Electrical and Computer Engineering
University of Texas- Rio Grande Valley,
Edinburg, Texas-78539, USA
Email: sj.kumar@utrgv.edu

2022 4th International Conference on Data Intelligence and Security (ICDIS) | 978-1-6654-5968-6/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICDIS55630.2022.00035

Abstract – Wireless Smart meters are increasingly being deployed by the utility companies to remotely collect power consumption data from customer premise periodically in real time. It gives utility companies the information needed to efficiently administer their customers for their electricity usage. Knowing how critical these data are, it is important to ensure that data recorded locally at the smart meters or communicated remotely or wirelessly are both confidential and reliable. Despite the efforts being made to secure the smart meter data, security threats on smart meters continue to evolve at the same time, with an increasing number of security breaches happening each year. At this time, not much research has been done to measure data breaches for commercially available wireless smart meters, and how they translate financial problems for the companies using such wireless smart meters. In this paper, we perform experiments to evaluate the effects of data security attacks on a wireless smart meter to understand impact on remote data collection, and how the compromised power consumption data would impact a utility company.

Keywords – AMI, Data Security, Electric Smart Meter, Electric Smart Grid, Security Threats

I. INTRODUCTION

Electric smart grid, and smart meters are used to manage, automate, and administer the rising complexities and requirements of electric power in the twenty-first century. The electric grid is referred to as "grid" [1]. Smart electric grid along with smart meters are used to remotely collect power consumption data from customers in real time.

Smart electric grid uses internet-based data technologies which enable bi-directional power usage data communication between households and utilities. The smart electric grid improves reliability, controllability, and cost-effectiveness of the electric power network.

Federal Government across world has been responding to the growing cyber danger by issuing recommendations to assist businesses in implementing good cyber-security measures [2-3]. This is not an exception in the power industry.

Smart electric meters are important components of smart grid infrastructure that are being installed at a rapid pace commercially. 75 percent of the US households have been deployed with smart electric meters. There will be upward growth in numbers aimed to reach entire households in near future [4].

Smart electric meters are supposed to report data consumption locally or remotely via wireline or wireless network communication. For example, power line carriers, can link the meter to the network. Cellular communications, Wi-Fi (which is widely accessible), mesh networks (wireless), Wi-SUN, ad-hoc networks (wireless) based on WIFI, ZigBee considered as low data and power rate (wireless), and low power but long-range (wireless) (LoRa), are all examples of wireless communication methods that are often used (Smart Utility Networks) [5].

Smart meters are very useful for the utility companies in informing in real time about the power consumption or power outages etc. Smart meters are also useful for the customers as they can easily monitor their own power usage and patterns. There have been more wireless smart meters deployed by the utility companies than fixed wireline smart meters because the cost of deployment of wireless smart meters is much less than the implementation cost of fixed wireline smart meters especially in the newly built housing or commercial areas. Commercial buildings or malls commonly deploy wireless smart meters utilizing WiFi protocols for measuring power utilizations on a finer level.

Although smart electric meters enable remote data acquisition for energy consumption via variety of network communication mechanisms, they are not immune to data security attacks [6], which can compromise the integrity of energy usage data being collected and reported.

Research has been conducted in the past [6], [7] showing that reporting of energy data by smart electric meters with fixed wireline implementations were adversely affected due to security data attacks. In this paper, we are conducting real time experiments for the wireless smart meter to find out how the energy data usage and its remote monitoring are affected by the data security attacks. Performance evaluation of wireless smart electric meter under data security attacks have been measured and analyzed for its impact on remote data collection, and for the financial outcome for a utility company.

978-1-6654-5968-6/22/$31.00 ©2022 IEEE
DOI 10.1109/ICDIS55630.2022.00035

II. Advance Metering Infrastructure (AMI)

The whole uninterrupted real-time data reading and gathering system utilized by smart meters and energy service providers intermediate systems is referred to as advanced metering infrastructure, as depicted in Figure 1. Advanced metering infrastructure (AMI) allows 2-way communication between smart meters to the energy supplier in contrast to automated meter reading (AMR) [8]. AMRs don't allow for 2-way communication.

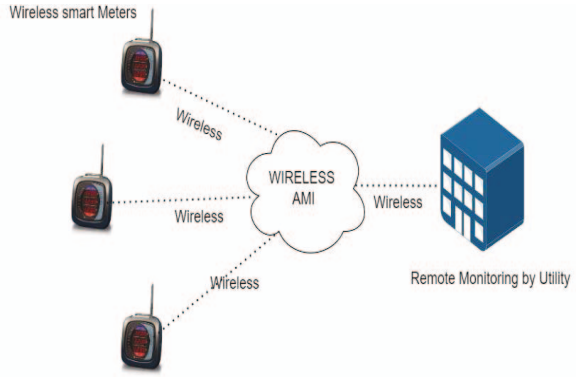

Figure 1. Wireless Advanced Metering Infrastructure (AMI)

AMI infrastructure includes data exchange networks between clients and utilities, as well as intermediate systems for energy usage information collection and monitoring, which make real-time data available to service providers, and data usage pattern available to customers.

III. Wireless Smart Electric Meter

Critical part of electric smart grid system is smart electric meter. It can keep track of things like electric energy usage, level of voltage, current level, and power factor. These meters monitor power usage data in real time and send out reports at regular intervals during the whole day. These meters allow to have bi-directional data communication between households and utilities.

Smart electric meter provides consumers with the knowledge and skills they need to make informed decisions about their energy usage, pattern of energy usage etc. Customers will no longer have to wait for a monthly bill to find out how much power they use.

There are different types of Smart meters being deployed. Wireless smart meters are more commonly deployed today and, in this paper, we are focusing on the data security aspects of wireless smart meters. The GE smart meter, EPM 6100 supports both fixed wired implementations as well as the wireless implementations in AMIs [9] used to track and control power usage in factories, enterprises, malls and residences. In this paper, we are using wireless implementations of the GE smart meter 6100 and studying impact of security attack for such wireless implementations.

A. EPM 6100 Commercial Grade Smart Electric Meter

These electric smart meters are multifunctional meter with ANSI C12.20 having accuracy class of 0.2 and various features, including Ethernet communication, serial communication, and WiFi data exchange, makes it simple to integrate into new or existing data communication networks [9]. Pre identification of power issues are aided by Total Harmonic Distortion and meter's warning capabilities. The devices surface attach to any wall and utilize ordinary five or one-amp CTs (donut or split).

Figure 2. Multifunctional Commercial Smart Electric Meter 6100, from GE [9]

This GE 6100 multifunction smart meter can measure voltage, current, and energy in multipurpose environments like housing complexes, educational campus buildings, commercial store etc. it may also help apportion energy usage in these environments.

B. Remote Monitoring EnerVista Software.

GE's EnerVista Software [9] provides a platform for service providers with remote access of entire settings and tools required to configure and maintain General Electric smart electric meters. The program allows to configure devices remotely in real time through a network connection, as well as read metered power usage statistics and monitor smart meter condition.

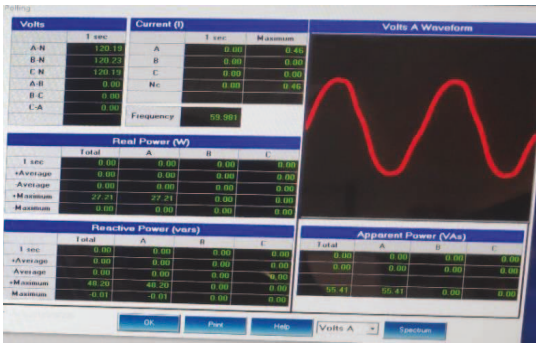

Figure 3. Real View of General Electric Enervista software

III. DATA SECURITY ATTACK

Data security attacks have been increasing with every passing day. There are many different types of data security attacks depending on the protocol level they are being used for [10-13]. For our experiments, we will consider ICMP based flood attacks, which are known creating denial of service, making systems perform poorly or become inaccessible, and hence blocking services for the host connected over such affected data networks [10-13]. In our studies, we deployed a low-intensity Ping-based ICMP flood to see how it affected smart meter data transfer and storage (Figure 4).

An ICMP dependent echo request packets are used to check the reachability of a computer. When designated target receives ICMP echo request packet, it replies to the sending entity, an ICMP echo reply packet depicted in Figure 4. ICMP echo request and reply work together in determining the reachability in data networks.

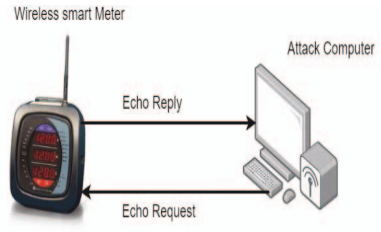

Figure 4. Ping Utility.

The flooding of numerous Ping packets delivered to the targeted destination in these Ping-based Cyber-attacks is found as being highly harmful to the availability of internet-dependent services. These ping threat can deplete bandwidth and processing resources of target computer [10]. The target computer continues to receive Ping messages, which create an ICMP echo reply packets that is delivered to the originator of spoofed Echo Request packets.

IV. EXPERIMENTATION SET UP

For experimentation, "3 ELWYE" Meter Programming Setup has been used for General Electric smart meter (Figure 5). 200-Watt load (two light bulbs each having capacity of 100 watts) was deployed for smart electric meter as show in Figure 6.

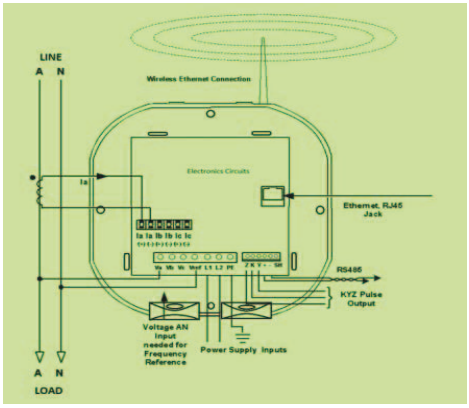

Figure 5. Programming Layout of Smart electric Meter [8]

General Electric (GE) multifeatured commercial smart electric meter (Figure 2) having wireless feature has been used. Commercial smart electric meter (EPM 6100) and attack generating computer have been connected via wireless to distant remote computer via NETGEAR WAP (wireless access point) WAC 104 [14] depicted in Figure 6.

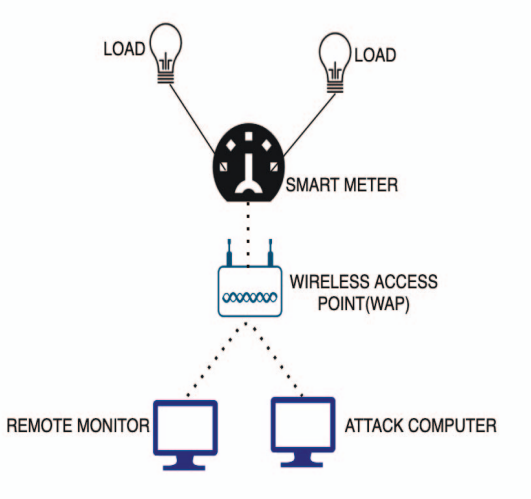

Figure 6. Experimental Set up/Configuration

The experimental set up used for this experiment has been shown in Figure 6. Using remote computer, energy usage information was recorded wirelessly that were reported by the wireless smart electric meter.

For experimentation, GE's commercial smart electric meter (EPM 6100) was deployed energy usage measurement and reporting to the remote computer. Energy consumption data was wirelessly accessed by the remote monitoring computer using General Electric communication software named EnterVista, that was deployed on the monitoring remote computer as shown in Figure 7.

V. EXPERIMENTAL RESULT AND DISCUSSION

For the Experiment two incandescent light bulbs of 100 watts each were used resulting in total load of 200 watts for the smart meter.

The baseline for energy usage values used for this experiment were determined by observing the actual readings of the aggregate load on the smart meter for continuous remote monitoring and recording of energy usage data for 15 days (360 hours) duration of the experiment in the absence of any attack traffic on the communication network. The baseline energy usage (Watt hours) is shown in the second column of the Table 1.

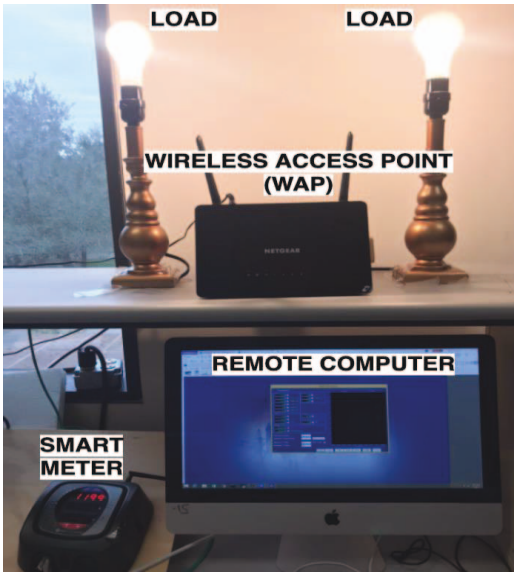

Figure 7. Experimental set up displaying the Electric Smart Meter, deployed load, wireless access point (WAP) and the monitoring remote computer.

After determining the baseline value for energy usage data (in Watt hours) without security attack traffic for 15 days, we further collected the energy usage data under the presence of Ping flood (attack) traffic, for the next 15 days. The average energy usage data (under the presence of attack traffic) are shown in the third column of Table 1.

Table-1: Average energy usage without attack (baseline), energy usage under security attack conditions, and Percentage loss (compared to baseline values) for the Wireless smart electric meter tabulated over 15-day period

No of Days	Average energy usage without attack (Baseline) in Watt hour	Average energy usage under Ping flood attack (Watt hour)	Percentage loss
1	203.32	203.21	0.0541
2	203.33	203.15	0.0885
3	203.23	202.53	0.3444
4	203.25	202.34	0.4477
5	203.24	202.23	0.4969
6	203.28	202.19	0.5362
7	203.26	202.17	0.5363
8	203.23	202.08	0.5659
9	203.16	202.00	0.5710
10	203.35	201.99	0.6839
11	203.25	201.86	0.7380
12	203.26	201.75	0.7478
13	203.28	201.74	0.7723
14	203.29	201.67	0.7969
15	203.31	201.67	0.8066

To determine the impact of data security attack, we calculated the percentage wattage loss through the 15 days period compared to the baseline values. The percentage power loss is shown in the fourth column of Table 1.

This experiment shows that the security attacks have adverse impact on the remote data reporting of the Wireless smart meter. Figure 8 shows the comparison of energy usage data remotely collected (wirelessly) under conditions of no security attack (baseline values) and under conditions of security attack. Energy usage data were collected continuously for over 15 days. From Figure 8, we observed that the longer the duration of attack, the lower the energy usage readings were reported (based on 15 days or 360 hours of data collected).

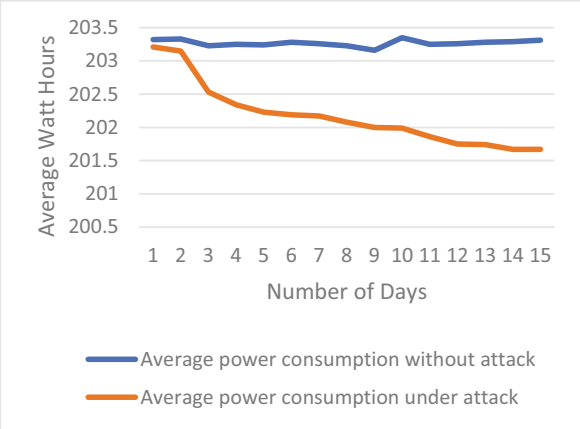

Figure 8. Average Watt hour without cyber-attack (baseline) and with cyber-attack

Figure 9 shows a plot of the percentage power loss compared with the baseline value due to data security attack. The graph shows there was a non-linear increase in the percentage loss from day 1 to day 15.

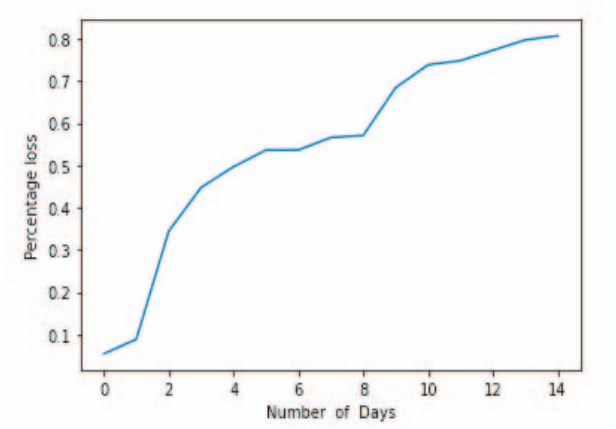

Figure 9. Percentage loss plot

VI. LOSS IN REVENUE DUE TO SECURITY ATTACK.

In this section, we estimate potential loss in terms of revenue that would be incurred over 15-days of data security attack on the wireless smart electric meter. We consider a hypothetical large commercial deployment scenario where this type of wireless smart meters were deployed on a mass scale. We then estimate the revenue loss due to lowered reporting of energy usage by the wireless smart meters under data security attack conditions. For our calculations, we would like to use some data obtained from a large utility company due to same type of data security attacks on the wireless smart electric meters.

For a commercial deployment scenario for this type of wireless smart meters, we considered deployment data available from a leading energy utility company, Pacific Gas & Electric. The deployment data are given below based on the report made available in 2021 [15]:

Company Name: Pacific Gas & Electric –

- Total customer served = 8,122,389
- Total number of wireless smart meters = 8,122,389 (considering 100% deployment of such meters)
- Total energy usage over 15 days = 5,421,088,172 kWh, [15]
- Average energy price [15] = 17.41c/kWh
- Loss of energy usage data because of the data security attacks (that was considered in this paper) on the Wireless smart Meter = 3,020,076,041 * 0.0080666 = 43,729,750 kWh per 15 days
- Total revenue loss because of data security attack on Smart Meter = 17.41 * 43,729,750 = $7,613,349 over 15 days.

Even though the percentage loss seems very small for a single wireless smart electric meter, the cumulative revenue loss for a large-scale deployment comprising of millions of smart meters would be very large, as shown above under the conditions of power data collections under data attacks.

VII. CONCLUSION

Wireless smart electric meters are rapidly being deployed in USA, and all over the globe. Smart electric meters are very valuable in a smart grid environment, since they send information about power usage to utility company for invoicing, troubleshooting etc. The smart electric meters also allow customers to review the energy usage pattern in their locations and take proper actions to reduce the waste caused by reduced reporting of power consumption data. There has not been much research done to evaluate the smart meter operation and reporting under attack traffic conditions. Based on the experiments conducted under data security attack conditions on a real wireless smart electric meter, it is clear that data security attacks can adversely impact the normal reporting of energy usage data to the utility companies.

ACKNOWLEDGMENT

The support for this research is provided in part by the US National Science Foundation under Grant No. 0421585, Houston Endowment Chair in Science, Math and Technology

Fellowship, Lloyd M. Bentsen, Jr. Endowed Chair in Engineering fellowship, and Presidential Graduate Research Assistant (PGRA) scholarship funding.

REFERENCES

[1] Smart Grid – A Brief Overview of the Emerging Framework IJSTE - International Journal of Science Technology & Engineering, Volume 3, Issue 08, February 2017 http://www.ijste.org/articles/IJSTEV3I8054.pdf?

[2] Report on Cyber Security Awareness June 2021 https://www.coursehero.com/file/131712051/140-Cyber-Security-Awareness-21-Pagespdf/?

[3] What is Cyber Security? [Online]. Available: https://usa.kaspersky.com/resource-center/definitions/what-is-cyber-security

[4] Electric Company Smart Meter Deployments: Foundation for aSmartGrid(2021Update)https://www.edisonfoundation.net//media/Files/IEI/publications/IEI_Smart_Meter_Report_April_2021.ashx#:~:text=As%20of%20year%2D%20end%202019,expected%20by%20year%2Dend%202021.

[5] Smartmeter https://en.m.wikipedia.org/wiki/Smart_meter

[6] S. Kumar, H. Kumar and G. R. Gunnam, "Security Integrity of Data Collection from Smart Electric Meter under a Cyber Attack," 2019 2nd International Conference on Data Intelligence and Security (ICDIS), South Padre Island, TX, USA, 2019, pp. 9-13, doi: 10.1109/ICDIS.2019.00009.

[7] H. Kumar and S. Kumar "Effect of Intermediate Network Systems on Remote Power Data Collection in Smart Grid" 2020 3rd International Conference on Data Intelligence and Security (ICDIS) | 978-1-7281-9379-3/20/$31.00 ©2020 IEEE | DOI: 10.1109/ICDIS50059.2020.00013

[8] Electric Power Research Institute. 2007. "Advanced Metering Infrastructure(AMI)"page1-2 https://www.energy.gov/sites/prod/files/2016/12/f34/AMI%20Summary%20Report_09-26-16.pdf

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

[10] Ganesh Reddy Gunnam, Sanjeev Kumar,(2017) "Do ICMP Security Attacks Have Impact on Servers?" Journal of Information Security,8, 274-283, July 2017 https://doi.org/10.4236/jis.2017.83018

[11] Sanjeev Kumar, "PING attack – How bad is it?" Computers and security (2006) Page(s):332-337

[12] S. Kumar, "Smurf-based Distributed Denial of Service Amplification Attacks in Internet," International Conference on Internet Monitoring, San Jose, California, pp. 25-29, July 2007. Available from IEEE online library Xplore

[13] S. Kumar and Orifiel Gomez, "Denial of Service due to direct and indirect ARP storm attacks in LAN environment," – Journal of Information Security, vol. 2, no.3, pp. 88-94, Oct. 2010, DOI:10.4236/jis.2010.12010;

[14] NETGEAR WAC 104 802.11ac Wireless access point https://www.netgear.com/sg/business/wifi/access-points/wac104/

[15] Independent Statistics & Analysis, U.S. Energy InformationAdministrationhttps://www.eia.gov/energyexplained/index.cfm?page=electricity_home#tab2