ISSN No:-2456-2165

Cybersecurity of Smart Meters

Bavisi Keval Nitin,
Diploma in Digital Electronics, Pursuing BTech in Electronics Engineering - DJSCE

Abstract: - Traditional metering systems are beginning to be obsolete now as we move towards a smarter and more efficient way of metering which is known as Advanced Metering Infrastructure or AMI.

AMI brings with it many advantages which includes Remote monitoring of the data, it also provides the facility of instant reading i.e Reading on Demand. But despite all the advantages it does have loopholes that might be used to tamper with the AMI infrastructure and hence disrupt the normal working of the devices hence, security of the AMI becomes an essential part hence the infrastructure must be given the latest security and hence it becomes a topic of research. As, the AMI infrastructure as a whole becomes a soft target by the hackers and attackers for launching various kinds of attacks it becomes necessary to provide the infrastructure a thorough security.

I. INTRODUCTION

➢ *Advanced Metering Infrastructure*

Advanced metering infrastructure investments focuses on the metering part, with the Automated Meter Reading (AMR) as the first trial, which provides utilities with basic remote information about the energy consumption records of each consumer-user. But the AMR system was limited only to remote reading and cannot provide utilities with any new additional information or data due to the support of one-way communication system. This limitation pushed utilities to move towards Advanced Metering Infrastructure (AMI) and Smart Metering. With AMI, utilities can establish bidirectional communication with the meter, to evaluate the grid status and to remotely connect, disconnect and even to configure the electricity service.

The AMI infrastructure facilitates 2-way communication which is a great advantage but also a point of vulnerability. The 2-way communication enables the AMI to send the data from the smart meter to the Data Concentration Unit (DCU) and to the control centre and vice versa when required and as and when needed or commanded to do so. This would enable many advantages like on demand response, Remote System Monitoring, dynamic pricing, cold-load pick-up, and the mitigation of greenhouse gas emissions. The AMI infrastructure captures and sends the data on an hourly or sub-hourly basis against the AMR infrastructure which provides total of daily used energy on a cumulative nature of monthly basis.

Cyber security of the AMI network is widely recognized as a critical issue. For power consumers, data privacy is a primary concern as current meters are upgraded to smart meters. To guarantee the confidentiality of data, a new communication protocol has been proposed. In, an encryption scheme has been developed for AMI network messages with minimal computation and communication overheads in encryption and decryption operations. For utilities, data integrity and availability attacks can threaten the quality of power grid services and revenues.

Due to vulnerabilities of wireless communication and physical devices, meter tampering is one of the potential attacks. In, a collaborative intrusion detection mechanism is proposed to detect False Data Injection (FDI) attacks. The work of [1] introduces a specification-based intrusion detection system for advanced metering infrastructures. Any sequence of operations executed outside the system's specifications is considered security violation.

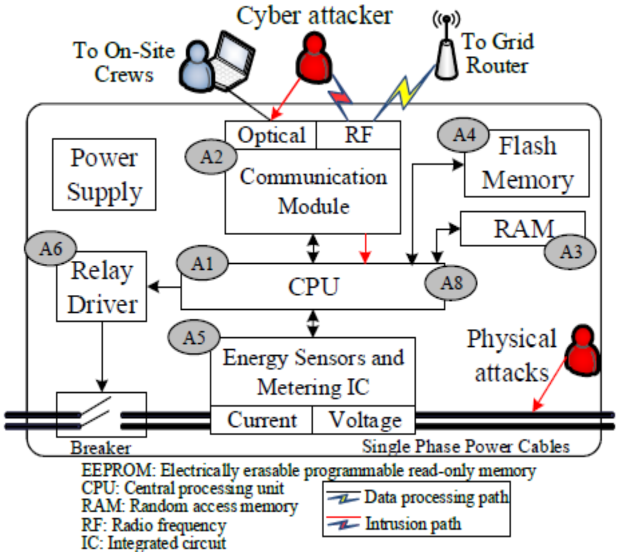
II. CYBER SECURITY VULNERABILITY OF SMART METERS

Since most of the AMI devices are not installed in a monitored environment, attackers may study the weaknesses of both wireless communication and physical devices and then launch cyber-attacks. This section will discuss the cyber security vulnerabilities of a smart meter.

➢ *Hardware Vulnerabilities*

Fig. 1 shows five primary compartments in a smart meter: (I) Central Processing Unit (CPU), (II) Random Access Memory (RAM), (III) communication module, (IV) flash memory (EEPROM), and (V) energy sensors. Since software/hardware components of smart meters are similar to those of other ICT devices, cyber attackers may adapt intrusion techniques from those employed in other software systems. In a smart meter, firmware controls the critical functions that handle the low-level sensor data, data conversion, and data reporting. Since most functionalities are accomplished through software, new functions can be added by performing updates. Firmware upgrades can be deployed using over the air mechanisms, or manually uploaded by using the on-board optical port. Firmware-based attacks can hinder the device's ability to operate as intended; multiple hardware components can be targeted when tampered firmware or settings are compromised by attackers. The possible attack behaviours for different targeted components are:

- **CPU (A1):** Exhausting CPU's computational resources by installing malware that causes dummy operations.
- **Communication module (A2):** The communication channels can be disabled or manipulated in unintended manners. In addition, AMI devices communicate in frequency bands that can be easily monitored, jammed, or compromised.
- **RAM (A3):** RAM exhaustion can also cause metering and communication applications to freeze or slow down. Operating Systems (OS) kernels terminate running application(s) or reboot to handle these faults.
- **Flash memory (A4):** Attackers can modify recorded consumption data, device calibration, and operation modes can be altered by modifying configuration registers.
- **Sensor (A5)/actuator compromise (A6):** By sending a tripping command, the utility system can disconnect a customer.
- **Inter-board communications (A7):** All components shown in Fig. 1 adopt low-level communication protocols that can be analysed and modified to suit the attacker needs. Due to physical access requirements, these attacks tend to be isolated. In summary, attackers can launch various types of cyber-attacks to impact operations in a distribution system. The consequences of these attacks are reduced utility's revenues, violation of customers' privacy, or, in the worst case, power outages.



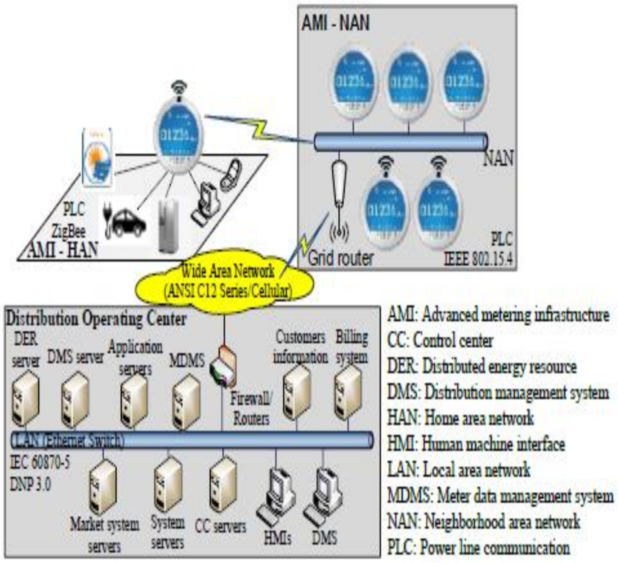
[2] Fig 1. Hardware components inside a smart meter with potential attack targets.

III. VULNERABILITY OF WIRELESS COMMUNICATION

End to end communication in the AMI environment is achieved using a mixture of network architectures, communication protocols, and interfaces between the control centre and field devices. Network architectures include: (I) Local Area Network (LAN), (II) Wide Area Network (WAN), (III) Neighbourhood Area Network (NAN), and (IV) Home Area Network (HAN).

Fig. 2 shows the communication structure of an AMI system. This paper is focused on securing the communication path within the NAN domain. The initial AMI meters deployed in North America used Zigbee, while newer models use the IEEE 802.15.4g standard, either at the sub-GHz (i.e., 900MHz) or 2.4 GHz [18]. Both frequency bands fall under the Industrial, Scientific, and Medical (ISM) regulatory domain. Therefore, frequencies are public and can be used by other devices. Furthermore, the wide availability of sniffers, signal modulators, and demodulators raises the overall risk levels since these tools are accessible and affordable. To reduce these risks, AMI devices use encrypted messages for data communication, for achieving integrity and confidentiality, while using meshed networks to provide availability under the CIA triad requirements [19]. However, security flaws have been discovered even with these mitigation efforts. Some security issues are:

- **Privacy issues:** Packet encryption protects the payload content, but it fails to protect the identity of the sender and receiver (MAC addresses). Furthermore, researchers have been able to identify the usages (e.g., control commands and consumption reports) of different network packets even when they are encrypted. Such knowledge can be used for attacks that target specific operations.
- **Integrity:** By using hardware forensics, local HAN passphrases can be recovered. These in conjunction with spoofed MACs can be used to create false network messages if the devices are not authenticated.
- **Availability:** Signal jamming, as well as DoS attacks, can limit message transmission, leading to situations where the control centre cannot send commands, or the device is unable to report its status.

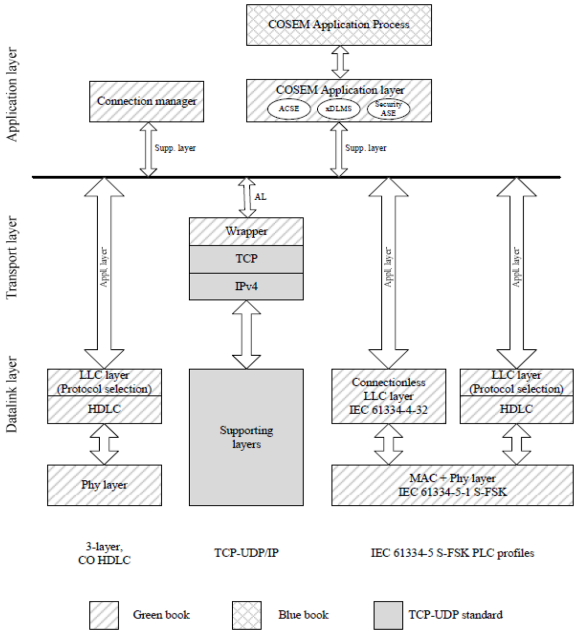


[3] Fig 2. Communication structure of AMI network

IV. RELATED WORK

A. *Understanding DLMS/COSEM Packet Structure*

Figure 3 shows DLMS/COSEM communication profiles that are classified by book colour and OSI model. DLMS/COSEM communication profiles can be separated into two parts including application layer and other layer. The part that is upper the solid line is application layer. This part has three blocks that are COSEM application process, COSEM application layer and connection manager. The only COSEM application process is described in blue book. Other part is described in green book. The part that is lower the solid line can be separated into three ways following the communication types. For 3-layer CO HDLC, this way includes data link layer and physical layer. It not has transport layer. Data link layer includes two sub layers: LLD sub layer and HDLC sub layer. Next, TCP UDP/IP has two layers: transport layer and data link layer. In transport layer, DLMS/COSEM adds wrapper sub layer before normal TCP and IPv4 sub layer. Finally, IEC 61334-5 S-FSK PLC profile is proposed for PLC communication. This way includes data link layer and physical layer like 3-layer COHKLC.



[4] Fig 3. DLMS/COSEM communication profile

B. *Sequence of DLMS/COSEM* -

Data exchanges between DCU and smart meter are based on the client and server paradigm. DCU plays the rules of the client. For DLMS/COSEM, we can classify sequence of packet transfer between DCU and smart meter into three steps: set up data link, data transfer and disconnect data link as shown in figure 4.

- *Set Up Data Link* —

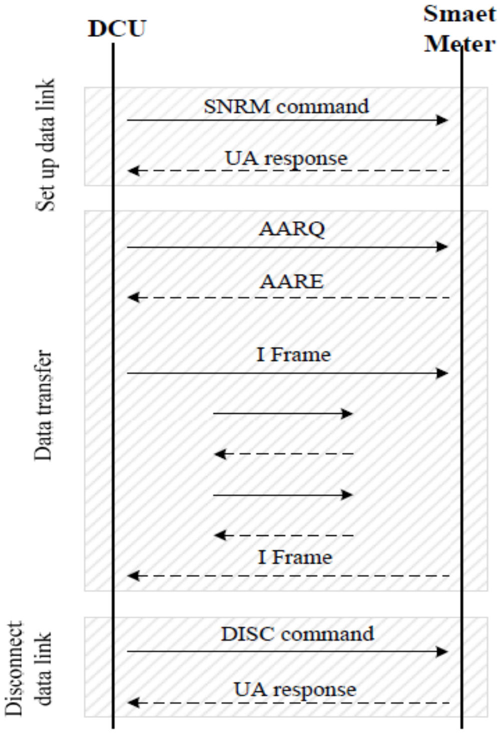
At this step, DCU sends SNRM (Set Normal Response Mode) command to smart meter. When smart meter received this command and smart meter is ready to connect, smart meter will send acknowledgment that name is UA (Unnumbered Acknowledge) back to DCU.

- *Data Transfer* —

First, DCU will check the properties of smart meter before connection. DCU sends AARQ (A-Associate Request) to smart meter and the meter will send AARE (A-Associate Response) return to DCU. AARQ includes all properties that meter can do and AARE is the properties of each meter has. After checking the property, DCU and smart meter can send I-Frame for changing its information.

- *Disconnect Data Link* —

If DCU and smart meter finish transferring data, DCU will send the DISC (Disconnect) command for disconnect and smart meter send UA response for confirm.



[5] Fig 4. Sequence of Packet transfer

C. Research Process

This process includes a thorough reading of several research papers for getting a broad and clear idea about the work that needs to be done and the work fronts that need to be explored for the same.

- The work of [6] thoroughly refers to the vulnerabilities found in the smart meters at both the hardware and communication model. It takes an in-depth view at the proposing an Intrusion Detection System based on 2 step process i.e (I) Collecting Intrusion evidence and (II) confirming an intrusion event through the detected abnormal behaviours in the system. The first stage is executed by using an SVM technique to identify suspicious activity in the normal working of a smart meter and report the same to the IDS.
- The work of [7] gives us a clear understanding about the communication IEC 62056 communication protocol i.e DLMS/COSEM. This is the protocol that the smart meters use to communicate with each other as well as the DCU. The paper mainly talks about the flow and the important codes in the communication sequence during the handshaking. It also gives us a different point of vulnerability as the HDLC frame does not encrypt the source and destination address frames. Hence a network can be easily compromised.
- The work of [8] contributes mainly to an algorithm or a method of segregating the abnormal behaviour of the meters from the attack vectors of the meters. It is thoroughly based on a Temporal Failure Propagation Graph (TFPG) model. The way TFPG works is by constructing an attack vector table which includes all the information about a potential cyber-attack pattern in terms of attack type and sequence. Once the abnormal behaviour is compared with the pre-defined attack vectors and it is found to be a match, it is declared as a cyber-attack and the steps to mitigate the same are taken.
- The work of [9] is completely based on studying the different attacks carried out on the smart metering infrastructure and explaining how the attacks were carried out. Hence it talks in detail about the MITRE ATT&CK threat modelling and how the components of the same can be useful as a mitigation technique against the cyber-attacks as it contains 14 steps and contains the methods and steps that can be used in the same hence mitigation of the same attacks becomes an easy task for the company thus securing the electric grid as well as the utility meters from the attackers and the different techniques that the attackers might use to attack.

V. PROPOSED WORK

This research paper aims at documenting the work behind the cybersecurity of smart meters and thus it is justified to have an end goal for which the research was conducted and the different theories related to the security and working of a smart meter were understood. The end goals for this project includes –

- Software emulation of the AMI infrastructure before the procurement of meters and working on it via AWS IoT Twinmaker.
- Working on a SARAL Meter to understand the communication between the meter and the host via [10].
- Identifying the vulnerabilities in the hardware, software and the communication part of the AMI infrastructure and stating the methods to mitigate the same.
- Exploiting the hardware vulnerability proposed in [11] via Buffer Overflow Attacks to crash a targeted meter or compromising a DCU.
- Creating a mesh network of user utility meters communicating with a DCU and thus trying False Data Injection on the packets.
- Using [12] as a reference for creating a threat model for all possible attacks against the meter and then moving up to the infrastructure.

VI. CONCLUSION

Thus, this paper focuses on highlighting the vulnerabilities of the smart meters and the way in which they could be exploited using different attack vectors and the different methods to mitigate them. It al so suggests an Intrusion Detection method based on TFPG models to mitigate the attacks using ML and hence doing it efficiently than today’s mitigation techniques.

REFERENCES

[1]. R. B. a. W. Sanders, “Specification-Based Intrusion Detection for Advanced Metering Infrastructure,” Pacific Rim International Symposium on Dependable Computing (PRDC), pp. 184-193, Dec 2011.

[2]. C.-C. Sun, D. J. Sebastian, A. Hahn and C.-C. Liu, “Intrusion Detection for Cybersecurity of Smart Meters,” IEEE Transactions on Smart Grid, p. 3, 2020.

[3]. C.-C. Sun, J. D, A. Hahn and C.-C. Liu, “Intrusion Detection for Cybersecurity of Smart Meters,” IEEE Transactions on Smart Grid, p. 3, 2020.

[4]. Kheaksong and W. Lee, “Packet transfer of DLMS/COSEM standards for smart grid,” The 20th Asia-Pacific Conference on Communication (APCC2014), p. 393, 2015.

[5]. Kheaksong and W. Lee, “Packet transfer of DLMS/COSEM standards for smart grid,” The 20th Asia-Pacific Conference on Communication (APCC2014), p. 394, 2015.

[6]. C.-C. Sun, D. J. Sebastian, A. Hahn and C.-C. Liu, “Intrusion Detection for Cybersecurity of Smart Meters,” IEEE Transactions on Smart Grid, pp. 1-11, 2020.

[7]. Kheaksong and W. Lee, “Packet transfer of DLMS/COSEM standards for smart grid,” The 20th Asia-Pacific Conference on Communication (APCC2014), pp. 391-396, 2015.

[8]. C.-C. Sun, R. Zhu and C.-C. Liu, “Cyber Attack and Defense for Smart Inverters in a Distribution System,” CIGRE Study Committee D2 Colloquium, Helsinki, Finland, pp. 1-9, 2019.

[9]. D. Mashima, “MITRE ATT&CK Based Evaluation on In-Network Deception Technology for Modernized Electrical Substation Systems,” Securing Smart Grid Cyber-Physical Infrastructure against Emerging Threats, pp. 1-10, 2022.

[10]. Kheaksong and W. Lee, “Packet Transfer of DLMS/COSEM Standards for Smart Grids,” The 20th Asia-Pacific Conference on Communication (APCC2014), pp. 391-396, 2014.

[11]. C.-C. Sun, D. J. Sebastian, A. Hahn and C.-C. Liu, “Intrusion Detection for Cybersecurity of Smart Meters,” IEEE Transactions on Smart Grid, p. 2, 2020.

[12]. D. Mashima, “MITRE ATT&CK Based Evaluation on In-Network Deception Technology for Modernized Electrical Substation Systems,” Securing Smart Grid Cyber-Physical Infrastructure against Emerging Threats, pp. 1-9, 2022.