Security Mechanism for Home Area Network (HAN) in Smart Grid

Rathod Bhargav H\textsuperscript{1} Dr. Vandana Rohokale\textsuperscript{2} Mr. Naresh Kumar Gardas\textsuperscript{3}

\textsuperscript{1}M.E. Student
\textsuperscript{1}Department of IT System Network Security
\textsuperscript{2}GTU PG School, Gandhinagar, India \textsuperscript{3}SITS, Narhe \textsuperscript{3}CDAC ACTS Pune, India

Abstract— Smart Grid is Digital Power System that comprises of two-way Communication infrastructure, IT System, Advance Sensor, and Advance Electrical Power Distribution for the smart City. The Devices controlled in smart homes have installed smart meters in apparatuses. They are sensor based and arrange empowered. As usual, Security and Safety issues are of prime Importance since it includes private information from Home Area network and Utility system. This paper introduction Smart grid Threads and Security Mechanism and in this paper propose a safe plan for Home Area Network and Utility System using ECC(Elliptic curve cryptography) Communication from Home area network to Utility System and detecting intruder using honeypots.

Key words: Smart Grid; ECC Communication; Smart Sensor; Advance Meater Interfaces; Remote Terminal Unite; Home area network; Honeypot; Utility System; DDoS.

I. INTRODUCTION

Smart Grid is to incorporate each part in power grid system with data and communication technology. The Smart Grid is a development to bring the electrical power framework state-of-the-art so it can meet the present and incoming requirement of its clients. Re script our electrical power grid could bring new security weakness into the System. This record introduces an audit of the business related to Smart Grid digital security.

The Smart Grid is an electrical power System that settles on canny decisions about the state of the electrical power System to keep up a steady domain. The most straightforward approach to dene the Smart Grid is by its attributes \[1\].The Smart Grid is a move up to the current electrical power System, so it has the majority of the usefulness of our present power System in addition to a few new functionalities.

Smart Grid has distinctive sections and resources, for instance, control eras, conveyances, clients, local control focuses, substations, field gadgets, correspondence and systems administration devices, stage measuring units, ensuring transfers, insightful electronic gadgets, remote terminal units, human machine interfaces, home apparatuses, circuit breakers, log servers, information concentrators, convention passage, brilliant meters, and so on. These parts are associated in brilliant matrix to work, screen, and control stream and estimations. These segments are associated in shrewd lattice to work, screen, and control stream and estimations \[5\].

The Communication and power Grids are interrelated with the end goal that the Communication organizes rely on upon the power network for information and the power framework relies on upon the correspondence for operational exercises.

![Smart Grid Architecture](image)

Fig. 1: Smart Grid Architecture [2]
The part of the grid is to give universal communication capacity to gathering information from sensors and meters, and give related data to bolster different exercises, for example, guaranteeing network solidness, distinguishing and determining irregularities, forecasting load, and encouraging interest reaction.

This should be done while securing the security of the Customer. Protecting basic operational information that from national adversaries and guaranteeing the respectability of the information for both business and operational needs [1][19]. The power grid is regularly isolated into transmission, dissemination, and the last mile. Transmission conveys high-voltage current over long separations to substations. Conveyance conveys bring down voltage information from substations to nearby transformers. The last mile interfaces the neighborhood transformers to customers, and it is the place utilities and customers connect to support ongoing administration of energy generation, dispersion, utilization, and productivity [2].

II. SMART GRID THREATS AND ATTACKS

Attackers can bring about a wide variety of attacks, arranged into three fundamental classes: [5]

- Segment Insightful
- Convention Shrewd
- Topology-Wise

**Segment wise:** Attacks concentrate on the field sections that fuse RTU. RTUs are generally utilized by pros to remotely arrange and look at the network keen Devices [8]. This remote get the chance to highlight can be liable to a strike that draws in unsafe clients to take control over the gadgets and issue inadequate states, for example, closing down the gadgets.

**Convention Shrewd (Protocol-wise):** Assaults focus on the correspondence convention itself utilizing strategies, for example, figuring out and false information infusions.

**Topology-wise assaults** concentrate on the topology of the keen lattice by pushing a DOS (Denial-of-Service) assault that keeps oversee

1) **Malware dissemination:** An assailant can make malware what's more; spread it to spoil splendid meters or affiliation servers. Malware can be utilized to supplant or add any capacity to a contraption or a framework, for example, sending touchy data [11].

2) **Access over database join:** Control structures record their exercises in a database on the control framework organize then reflect the logs into the business deal with. On the off chance that the underneath database association frameworks are not by any stretch of the imagination arranged, a gifted aggressor can get to the business coordinate database, and a while later utilize his aptitudes to misuse the control structure sort out[2][9][6].

3) **Compromising communication equipment:** An attacker may compromise a portion of the correspondence hardware, for example, multiplexers bringing about an immediate harm or utilizing it as a secondary passage to dispatch future assaults [3].

4) **Infusing false data (Replay Attack):** An aggressor can send bundles to imbue false information in the framework, for instance, false meter data, false costs, wrong emergency event, and etcetera wrong information can have an enormous budgetary effect on the power grid.

5) **N/W Availability** Since brilliant grid uses Internet Protocol tradition and Transmission Control Protocol/IP stack; it gets the chance to be subject to denial-of-service (DoS) assaults and to the weakness inborn in the TCP/IP stack. Denial-of-service (DoS) assault may attempt to deferment, square, or worsen information transmission with a particular ultimate objective to make savvy network resources inaccessible [7]

- Spoofing: gaining privilege by masquerades
- Tampering: Intentional modification of the product so as to cause harm to the user
- Repudiation: refute the validity of a contract or service level agreement
- Information Disclosure: disclosing the information to those who should not know
- Denial of Service: make the resource unavailable to the intended users
- Elevation of Privilege: increases for a higher role user access/privileges
- Phishing: illegal access to protected data[8]

III. SECURITY PRINCIPLES AND PROTECTION OBJECTIVES FOR SMART GRID

Smart grids comprise of a system of sensors, screens, gadgets, and also PCs for information gathering and examination. These are helpless to digital assaults. Experts have recognized five noteworthy difficulties confronted by electronic security frameworks identified with savvy matrices [EBook: Smart matrix security] including a high volume of touchy client data, appropriated control gadgets, an absence of physical insurance, feeble industry measures, and countless subject to the network[6].

The worries of smart grid security as with other regular frameworks are confidentiality, integrity, and availability. Confidentiality involves securing both customer and operations information; Integrity is likewise required both at the customer level for metering and charging and at the operational level to guarantee the stability of the grid; availability implies that the power keeps on being transmitted and got by clients, paying little mind to the status of the system[4].
IV. COUNTERMEASURES

To mitigate these dangers we can introduce IDS system, utilize VPN channel, require encryption, authenticate users, and make convention layer security, we can locate these normal strategies were utilized as a part of paper[9].

1) Identity should be confirmed through strong verification systems. Associations should execute an understood deny arrangement to such an extent that entrance to the system is conceded just through access permissions [10].

2) Malware security on both Embedded and General reason frameworks. The introduced framework is proposed to simply run programming that is provided by the producer. The maker is required to embed in its things an ensured Private that contains keying material for programming endorsement. Utilizing a key, the system can support any as of late downloaded programming going before running. In any case, broadly useful frameworks are proposed to bolster outsider programming. For this framework, a la mode and every now and again overhauled antivirus programming alongside host-based interruption avoidance are required[11] [9].

3) N/w IPS and Network IDS advances ought to increase the host-based security to shield the framework from outside and inside attacks [7].

4) Gadgets should support VPN (Virtual Private Network) structures for protected conversation [10].

5) Gadgets must Utilize PKI (Public key Infrastructure) to protected conversation. Nonetheless, there are a few requirements with respect to cryptography and key administration [3]: current gadgets don't have enough preparing force and capacity to perform propelled encryption and confirmation procedures, communication in a smart grid framework will be over various channels that have distinctive data transfer capacities, and availability, where all gadgets, testament powers, and servers must be associated at all times.

V. PROPOSED WORK

There is not perfect model or solution available right now to smart meter and the utility system. There are some analyzing methods available but it is not standardized.

So any specific Smart meter security using authentication and authorization and for utility system using honeypot or IDS and IPS. Having reviewed the real vulnerabilities and security challenges, this segment the late security arrangements. The communication between HAN to NAN is must be secure using the ECC Algorithm for Communication from HAN to NAN and Honeypot.

Fig. 3: described the current communication process of smart Grid System.
In this paper first fig described the real system communication system to smart mater send the data to neighborhood area network (NAN) and NAN is one collector to receive the data from smart mater and send the utility system. (Fig 2).

Home Area Network are Send the Data of energy Consumption to Collector in this smart grid Collector work for send to data to main Utility server Show in the fig.

![Proposed Model](image)

Fig. 4: Described the Proposed Model.

In this proposed model Communication Secured using the elliptic curve cryptography (ECC) Algorithm and in smart grid need to Security that's why using ECC Algorithm for Communication. And In Smart Grid using all intelligent devices and IOT devices For Example Smart Energy Mater, HVAC etc.

![Detection flow diagram for DDOs Attack](image)

Fig. 5: Described the Detection flow diagram for DDOs Attack

**Process Steps:**

*Step 1:* Acquired incoming packet from client.
*Step 2:* Check the Database Ip and mac is Stored or not if new IP and MAC then rejected Request.
*Step 3:* If IP and MAC are authorized then go to next step.
*Step 4:* Check the TTL value if TTL value is Abnormal then IP and mac is rejected.
*Step 5:* If not abnormal TTL fetch then Send the Data Utility Server.
VI. IMPLEMENTATION

Following are the Simulation software for Security mechanism for Home Area Network (HAN) in Smart Grid First setup Contiki operating system.
Using cooja simulation for simulate the Smart meter and Gateway and server.

A. Smart Mater
Smart Mater is a most important part of Home area network and Utility server this is Smart mater to send Consuming Power to the Utility system.

B. Concentrator
Concentrator is connected the Home area network and utility system this is work for gateway this is connected to smart mater and acquired the data from the smart meter and send to the utility server.

C. Utility Server
Show Figure 6 of cooja simulation.

![Fig. 6: Simulation on Cooja](image1)

In this screen shot Describe the smart mater (Yellow Node) connected to NAN network (Green Node) and NAN network connect the utility system (Pink Node)

![Fig. 7: Power consumption Graph](image2)
In this Figure 7 describe the smart meter sense the consumption of power and in this Fig display a graph to smart meter consumption of energy.

In this cooja simulation try to attack worm hole attack in smart meter show in Figure 8

Fig. 8: Attack occure in smart meter

Now In this System work on live system Implementation work done the Communication to smart meter to utility server using ECC Algorithm. And create Honeypot for utility system.

Smart meter send the data to collector and collector send the Data utility server in this paper use raspberry pi is as collector and collector gain Data to the Smart meter and collector send the data as encrypted format using ECC algorithm.

Fig. 9: Smart meter send unit to utility system

Figure 9 Real example of the smart meter send the data to Utility server.
In this Figure 192.168.43.129 is server and 192.168.43.127 is a smart mater and smart mater sand the Encrypted packet to the server.

If some attacker is trying to replay attack, fabrication attack and all passive attack is not effected in this ECC encryption between smart mater to utility system.

In basic Formula of Elliptic curve Cryptography [5].

\[ y^2 = x^3 + ax + b \]  

(1)

1) Formula is ECC Algorithm

Using ECC Algorithm encrypted smart mater data and send the Utility system. And using the honeypot system on utility server because the attacker thing honeypot is real system but it is a fake machine and read the all patent intruders and send instruction of intruders to main utility server.

VII. CONCLUSION

Among the Advanced use of data and communication technologies in the development of smart grid, the data security is confronting more danger and hazard. The accentuation on data security work can’t be exaggerated at whatever time, any place.

Since the smart network is seen as an essential system, all vulnerabilities should be perceived and basic plans must be executed to diminish the dangers to a tasteful secure level.
REFERENCES


