Internship Report on

GPRS System for Smart Metering Networks in Bangladesh

An Internship Report

Submitted to the Dept. of Electronics & Communications Engineering, East West University and Dhaka Power Distribution Company Limited (DPDC) in partial fulfillment of the requirements for the degree of Bachelor of Science in Engineering (B.Sc. Eng.)

Submitted To

Academic Supervisor

Sarwar Jahan
Associate Professor
Dept. of ECE.

East West University

Dhaka, Bangladesh

Industrial Supervisor

Engr. Mohammad Emdadul Haque

Manager (ICT)

ICT Development Circle

Dhaka Power Distribution Company Limited
Dhaka, Bangladesh

Submitted by:

Kazi Jannatara Juti ID: 2019-1-55-001

Department of Electronics & Communications

Engineering, East West University, Dhaka,

Bangladesh

27 December 2022

Authorship Statement

I hereby state that I have completed the internship report in part fulfillment of the requirements for the East West University Bachelor of Science in Electronics and Communications Engineering (ECE) degree. The interpretations offered are based on my reading and comprehension of the original materials, and it is not a work that has been plagiarized. The additional books, journals, and websites that I consulted are properly recognized in the text where they are used.

Date**: 27 December 2022** **Signature**

Name: **Kazi Jannatara Juti**

Acknowledgments

It is my pleasure to acknowledge the extra-ordinary supervision, invaluable suggestion, and proper guidance of my supervisor, Sarwar Jahan, Associate Professor, Dept. of Electronics and Communications Engineering, East West University, and respectable trainer **Engr. Mohammad Emdadul Haque**, Manager, ICT Development Circle, Dhaka Power Distribution Company Limited (DPDC), from whom I have been very much benefitted throughout the course of my training. I express my humble gratitude to them. Without theirkind cooperation and help the internship report would never have been possible.

I am also thankful to our honorable teachers of the Department of Electronics and Communications Engineering (ECE) at East West University (EWU) and well-wishers for their valuable suggestion during the period of my internship work.

Finally, I would like to express my indebtedness to our parents for their constant support and inspiration to accomplish the job.

Date: **27 December 2022** Name: **Kazi Jannatara Juti**

Abstract

Advanced Metering Infrastructures use General Packet Radio Service (GPRS) for wireless communication in many Smart Grid installations (AMI). In this essay, I go over the authentication and encryption options that are available in GPRS security features and assess how well they work in a Smart Grid scenario. I draw the conclusion that GPRS' usefulness depends on the authentication and encryption options selected, as well as on choosing a reputable and trustworthy mobile network operator.

Keywords: Security, GPRS, Smart grid, AMI, Smart Metering

Table of Contents

Chapter 1

Introduction

1.1 Introduction

The most obvious feature of the smart grid is probably the smart meters in an Advanced Metering Infrastructure (AMI). Every residence has a smart meter installed, enabling two-way real-time communication with the distribution service operator or electricity provider. AMIs enable for the automatic collecting of data on energy usage and subsequently more precise pricing plans. Smart meters may feature breaker functionality, allowing power to be remotely switched off, and they can send signals and alarms to the DSOs. Equipment in the homes that allows for the automatic adjustment of power demand based on the current price level may be connected to meters. Smart meters communicate with DSOs using a variety of channels, although General Packet Radio Service (GPRS) is a preferred option in many rural areas. It was launched to provide GSM mobile stations with a quicker data transfer service that offers a packet-based data service in accordance with the internet protocol (IP). The serving GPRS support node, which connects to the mobile station via the currently operational Base Transceiver Station (BTS), and the Gateway GPRS Support Node (GPSN), located at the Mobile Station's home operator and connected to the public internet, are the two most important new network components that are introduced.

Undoubtedly, GPRS will accelerate a handset's internet connection, but it is yet unclear how much speed can be squeezed out of the system. It functions by combining various independent data channels. This is feasible because data is divided into tiny packets that are then put back together into their original format upon receipt. The problem is that there is no need that the number of receiving channels match the number of sending channels. Because there are more "down" channels used to receive data than "up" channels used to send data, GPRS is an asymmetrical technology. Because it operates on a 2.5G network, GPRS

builds on the network infrastructure that already exists, unlike 3G networks. Typically, it entails creating a brand-new network.

1.2 Background

DSOs urgently need to address information security and consumer privacy due to the new models and higher connections that come with the adoption of AMI. Figure 1's depiction of the scenario in which we are thinking about GPRS communication shows the interface between a smart meter and the Head End System (HES) at the DSO, which has been recognized as a threat point for AMI systems. threats consist of,

False identities: Someone may adopt the T2 meter's or the HES's identities (T1). Communication tampering: Someone interferes with the transmission of information between the HES and the meters (T4).

Repudiation: The meter disputes either the transmission or receiving of a message (T6) (T9). Eavesdropping: a meter and the HES are being communicated with, and someone is listening in (T10) Communication is impeded by a denial-of-service attack on the HES (T18), an attack on one or more meters (T19), or a communication link failure (T20).

For DSOs, it's critical to comprehend how vulnerable GPRS and other potential communication technologies are to such attacks or how well they can fend off failures of the kinds.

1.3 Objective of the study

With the use of a GSM module or by uploading the data to the cloud, the smart meter's goal is to not only track the consumer's energy usage but also send the information to the utility office every week, day, or hour.

It can be viewed in two forms:

a. General objective
b. Specific objective

General objective

This internship report is prepared primarily to fulfill the Bachelor of Science (B.Sc.) degree requirement under the Electronics & Communications Engineering Department of East West University.

Specific objective

The following parts of this study are more specifically included:

a. To provide an overview of Bangladesh's position with smart meters.

b. To talk about how much electricity is used in Dhaka. must concentrate on the GPRS system to meet people's needs.
c. To determine Bangladesh's smart metering system's opportunities and problems.

Significance of the study

The demand for electricity is rising exponentially as the population grows. The energy market is crippled because of power theft, unpaid payments, and inefficient energy use. Due to their low cost, electronics are being used more frequently, which has altered power quality. To improve power consumption efficiency, monitor power quality, and carefully track client power usage patterns. The main objective is to enable two-way contact between utility customers and the utility. Voltage, current, and power factor readings can all be taken in real time using the smart meter's GPRS system. The meter uses GPRS to calculate and save the amount of energy used. It offers thorough consumption data to lower electricity costs and raise awareness of the electricity grid's condition, which enhances the grid's functionality and the standard of service provided to customers. The paper includes information on Bangladesh's GPRS system for smart meters. For people to understand the GPRS system's prospects and difficulties in Bangladesh, the analysis of the GPRS system is the main topic.

Chapter -2

Background and Literature Review

2.1 Smart Meter

2.1.1 Smart Meter and Why it is needed

Defining the smart meter:

A smart meter is a digital electricity meter that measures the electricity entering and leaving your home and transmits the data to the utility typically every 30 minutes. A meter reader doesn't have to go to the meter after a smart meter is installed. Utility and Meter can communicate with each other in both directions.

An electrometer that measures electricity use over time is a smart meter. An electrometer that measures electricity use over time is a smart meter. The advantage of these meters is that they communicate with and receive commands from the main hub or command center. The smart meter has a two-way communication feature.

Components of Smart Meter

- Data concentrators—communicate the concentrator-owned meters.
- Meters are devices that calculate energy.
- HES, or Head End System, is a hardware and software combination. In accordance with utility guidelines, it connects with the meter. It serves as a bridge between Meter and MDM.
- Meter Data Management (MDM) is a reporting solution for meter data. Meter information (Load profile, event, and temper) is kept here using HES.

Why smart meter is needed?

- Theft and meter tampering detection
- Scheduled or on-demand meter data reading at programmable intervals; load control; and load limiting
- Reconnection / Disconnection through Remote
- Hour-by-hour (TOD)/TOU metering
- Detection, alerting, and reporting of alarms and events
- Net-metering and pre-paid
- Energy Auditing and Accounting
- Upgrade of remote firmware

2.1.2 Why Smart Meter is Essential in Bangladesh

• Checking the transformer for overload protection

• Possibility of immediate load management

• A smart meter is necessary for a smart grid.

• Worldwide Online Vending

• The client can check the meter's status from home.

• The utility can apply the new rate and meter firmware right away.

• Meter data reading on demand or scheduled at programmable intervals

• Reconnecting and disconnecting remotely

• On prepaid software, meter temper events are presented right away.

- Automatic meter monitoring system may reduce system loss.

2.1.3 ; Smart Prepaid Meter Customization

What are smart Prepaid Meter Customizations

• Set up the meter so that it functions with true prepaid features.

• It guarantees the safeguarding of revenue

• Enhancing Customer Service

Ways of smart Prepaid Meter Customization

1. Create default values for meters.

- Balance in an Emergency
- Good Will Time
- Bad Credit
- Maximum Credit Amount
- Holiday
- Negative Balance

2. Produce Tokens for

- Balance in an Emergency
- Good Will Time
- Bad Credit
- Maximum Credit Amount

3. Holiday

- Unclouded Balance
- Trademark Tokens
- Token for Load Management

Steps for Customization

- Install new feeders, transformers, and NOCS
- Adding meters
- Add clients
- A consumer and a map meter
- Access the fresh card
- Use management tokens to personalize the meter.
- Insert the fresh card in the meter slot.
- • Present the card to clients

2.1.4 Smart Meter Communication Network

Home Area Network (HAN)

To manage energy consumption, a HAN is used to collect sensor data more effectively from a range of home-based devices and transmit control information to these devices.

Neighbor Area Network (NAN) or Field Area Network (FAN)

A NAN It is the WAN concentrators' and SMs' communication network. It gathers data from numerous homes in a community and transmits it to WAN.

Wide Area Network (WAN)

Data from many NANs is combined via a WAN and sent to the utility private network. Additionally, it makes it possible for long-distance communication to occur between various data aggregation points (DAPs) found in power plants, substations, transmission and distribution grids, control centers, etc.

2.1.5 Smart Meter Data Flow

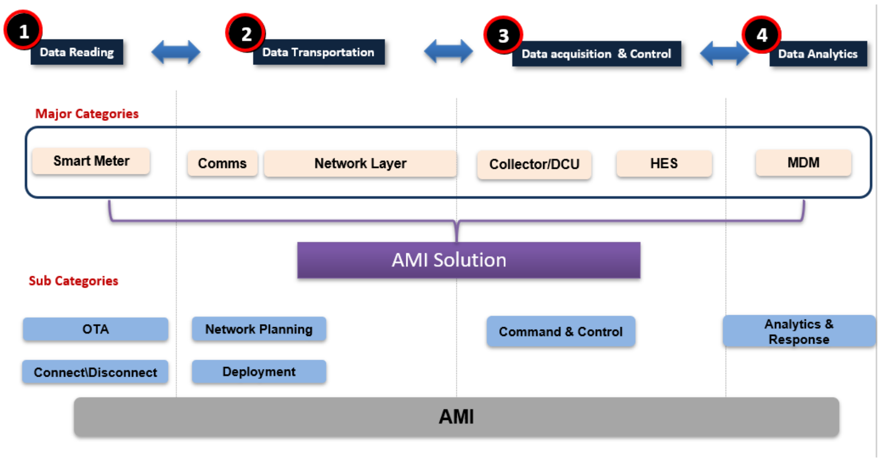


Figure 1: Smart meter data flow

The electrical current flow and voltage are measured by a smart meter at regular intervals, and the power consumed during a half-hour is calculated using this data. Like this, the flow of gas is periodically measured. Both your provider and your in-home display can receive this information. The Home Area Network may connect with your In-Home Display using a variety of communication technologies, and the Wide Area Network may send and receive data from the communications provider using a variety of communication technologies in various locations across the nation.

Meters constantly track their own performance and environment in addition to measuring energy.

2.1.6 Communication Technology in Different Layer

Table 1

Technology / protocol	Home Area Network (HAN)	Last mile/ NAN/FAN	Wide Area Network (WAN) / Backhaul
Wireless	• RF mesh • ZigBee • Wi-Fi • Bluetooth • NFC	• RF mesh • ZigBee • Wi-Fi	• Cellular/GPRS • Satellite • Private Microwave Radio
Wired	• PLC • Ethernet • Serial interfaces (RS-232, RS-485)	• PLC • Ethernet • Serial interfaces (RS-232, RS-485) • DSL	• Optical Fiber • Ethernet • PLC • DSL

In the current context, wired technologies don't always meet commercial requirements. Because of this, wireless technologies used in smart meters have begun to develop and improve upon the initial telecommunications infrastructure.

2.1.7 Smart Meter Features

Main Features

- Immediate Voltage
- Immediate Current
- Peak current and voltage
- The system's frequency
- RMS voltage and current
- Input Power Factor
- Immediate Apparent Power
- Immediately Real Power
- Event and alarm/alert capacitor
- Internet Protocol (IP) cards

2.1.8 Smart Meter Technology Perspective

- ➢ Single-phase and multiphase metering
- ➢ Over-the-Air broadcasting
- ➢ Version of the firmware

- Settings/Configuration for meters

- Information from the meter faceplate
- Point-to-point (SIM cards for mobile phones)

- Mesh

2.1.9 Smart Meter Application

- Measurements of consumption across time
- Reads in Register
- Meter Status and Health
- Sags and swells in voltage
- Alerts from temperature sensors
- Last Gasp, Meter
- Tampering notices

2.1.10 Communication flexibility in Smart Prepaid Meter

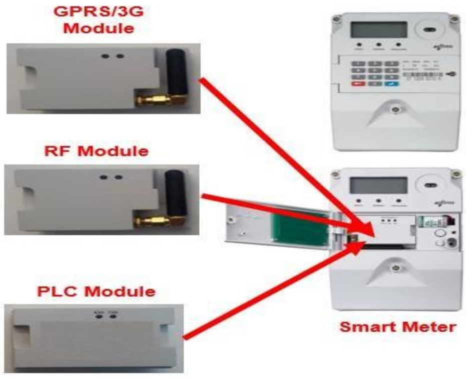


Figure 2

The next generation of energy systems has been developed as a result of the merging of power engineering with information and communication technology (ICT), also known as smart grid systems.

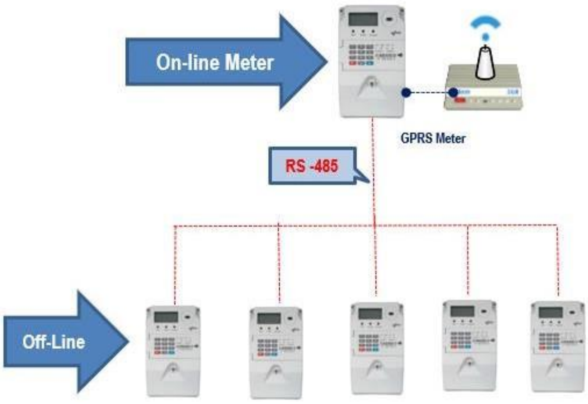


Figure 3

Smart meters are methods for monitoring usage, distribution, and other factors.

2.1.11 Power Down Events

Events Reports

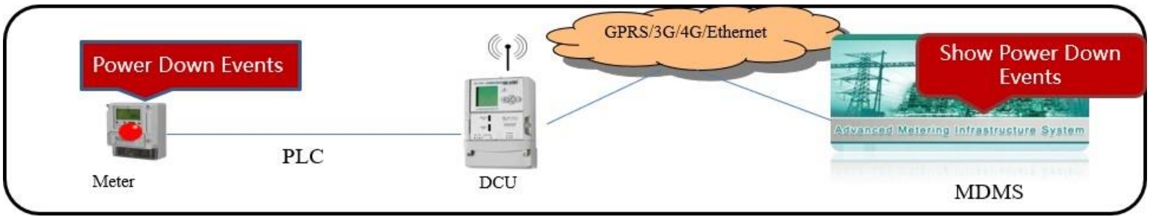


Figure 4

An electronic meter that properly measures energy information and a communication module that sends and receives data are the two major parts of smart meters. The advanced metering infrastructure (AMI) system, which includes smart meters, a communication network, and an IT application to manage the network and provide the necessary meter data and events to the utility's various IT systems, including its outage management system, includes smart meters as part of its advanced metering infrastructure (AMI) system (OMS). OMS enables a utility to manage power outages and restoration events more effectively, as well as cut down on the length and expense of outages.

2.1.11.1 Single Outage Events

When there are issues with the service in their homes, customers frequently phone their electric service provider. Some of these calls arise from a more significant outage or utility issue. There are numerous additional calls for single-client outages where the meter-side issue is with the consumer. Without a smart meter, these "no lights" situations are frequently fixed over the phone with the client or, more frequently, during a visit to the customer's home. Smart meters help the utility determine if the outage is due to a fault with the utility service or a problem on the customer's property. The utility can then take the appropriate action to address the issue quickly and affordably. Power status data is automatically and upon request provided by smart meters. The "power fail" is one of the automatically created details.

a "power outage" warning and a "power restoration" warning when power is restored. Since the installation of smart meters, a midwestern utility has significantly benefited from these capabilities. It almost eliminated all pointless no-light journeys and facilitated quicker problem-solving for clients. Average annual no-light calls represent 1.5% of all customer calls, and up to 30% of calls from a single customer were found to not be an outage occurrence. This would be equivalent to

4,500 non-utility-based outage incidents each year.

2.1.11.2 Multiple Outage Events (Storms)

Multiple outage situations can range in size and shape from a single fuse to a significant outage brought on by a significant event like a hurricane or ice storm. Customers are harmed by all of these outages. For utilities, it is of utmost importance to carry out repairs promptly and resume service. Understanding the extent of the present power loss is the first step in restoring power as quickly as feasible. Many utilities use OMS to identify the number and location of impacted consumers by utilizing all available information, including customer phone calls. Prior to the development of smart meters and other cutting-edge technology, OMS only received input from customers via phone calls or utility inspection teams. Calls from consumers are always vital, but less than 20% of those who are affected by an outage will typically report it for a variety of reasons, such as being away from home or believing that the problem has already been reported. To ascertain the impact, OMS analyses and analyzes the data that AMI collects and provides utilizing the tracing and prediction analysis functions of a Realtime distribution network model. Based on the facts at hand, OMS will forecast the location and size of the outage and send the right teams to resume service. Prior to losing power, smart meters transmit a last-ditch notification to the utility's OMS system. Not all last-ditch communications are sent, but often enough are for the utility to properly identify whose customers are impacted. Smart meter outage data can improve the precision of outage predictions and assist utility staff in quickly and accurately responding power issues. As a result, power is restored to customers more quickly, utilities run more effectively, and costs are reduced. Verification of power restoration is another advantage of smart meters. A meter reports in after being reenergized, which completes the restoration verification process. Before restoration teams depart the affected locations, this will offer automated and conclusive confirmation that all customers have been restored, there are no nested outages, and related trouble orders are closed. This lowers expenses, improves client happiness, and further decreases outages duration. Prior to the development of smart meters, it was typical for utilities to. Prior to the development of smart meters, it was normal practice for utilities to dispatch staff to restore service to a customer whose service had already been restored during a large event. Utility companies simplify their connection with AMI and OMS to get the most out of smart meters for service restoration. Utility staff members may now effectively carry out service repairs and see the entire extent of damage thanks to this connection.

2.1.11.3 Summary of Outage Management Improvement Benefits

Utility companies can avoid needless and expensive truck rolls by using smart meters to verify whether an outage is occurring on their own infrastructure or at a private house. Utilities can swiftly identify and fix utility-side issues by collecting data from smart meters. Smart meters are used to identify nested issues, which are frequently brought on by extreme weather. Benefits include less miles traveled, especially during bad weather, which enhances worker safety and lowers carbon emissions from vehicles. Utilities can reduce outage times and costs by using smart meter data to view, evaluate, and efficiently manage repairs. This data can also be used to verify service restoration rapidly and precisely. Outage Prevention Reducing the frequency and length of power outages is a goal shared by utilities, their clients, and their regulators. Tree pruning, grid upkeep, and the use of automation for service restoration are tools that lower the number of prolonged outages. On a per-customer basis, smart meters record a variety of anomalous events, such as brief outages that frequently precede grid failures. A utility may be better able to prepare for a future continuous outage by using this information to predict where it would happen. Circuit reclosers and other auto-closing devices register the number of operations, but it is frequently challenging to tie these counts to the number of actual events and issues. Utilities can count the number of incidents and locate areas with a lot of activity by gathering comprehensive temporary outage data on a small number of meters. Utilities can pinpoint potential areas for extra tree pruning or equipment failure by mapping momentary data. After that, utilities can take corrective action to fix the issue and avoid a potential prolonged outage. To confirm the electrical phase to which a single-phase smart meter is attached, use mapping and analytical tools. The utility's electrical maps in its OMS can then be verified and corrected using data from smart meters. For the OMS to accurately forecast the size of the outage, the connection between a smart meter and its electrical circuit must be correct. The single-phase loading will also be enhanced by having a precise awareness of the phase that a meter is attached to. Better asset use results from this. History of outages and reliability metrics Each time a device is powered on or off, smart meters record the time. As a result, exact outage durations and times may be calculated. Utilities can use this data to determine the overall performance as well as the best and worst performing circuits in order to calculate their reliability measures (SAIFI, CAIDI, SAIDI, etc.) more precisely. Then, utilities may create the most economical action plan for upcoming grid modernization investments. Smart meters are advantageous for both single and repeated situations since they speed up power restoration and outages.

To assist prevent future power outages and ensure that the electrical maps in the OMS are accurate for the most precise predictions, smart meter data can be used with mapping and analytical tools. Utility companies have long placed a high priority on improving operational efficiency, energy efficiency, and grid resilience. Investments in AMI will enable utilities to further fortify and strengthen crucial utility infrastructure before and after storms, lowering restoration costs and decreasing customer disruptions. These investments can be combined with distribution automation and grid resilience programs.

2.1.12 Smart meter architecture

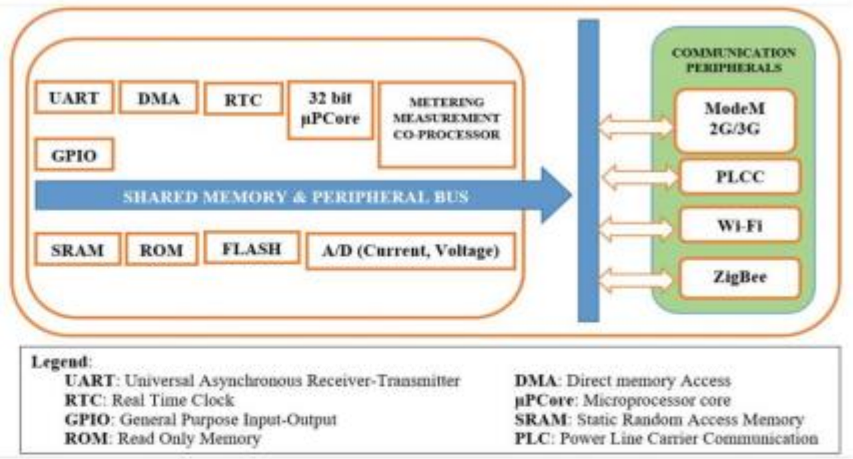


Figure 5

These data are used to load a form representation into a digital format and store information in the device's internal memory. The power usage and outage occurrences are recorded using these data. Star, tree, and mesh topologies are the most often utilized in smart electricity meter communications. The hardware architecture of a silicon-and-chip-based smart power meter is depicted in Figure-3. Its primary parts are a metering measuring co-processor, an analog-to-digital converter, a shared memory and peripheral bus, and common peripherals.

Chapter-3

GPRS System

3.1 Architecture of GPRS System

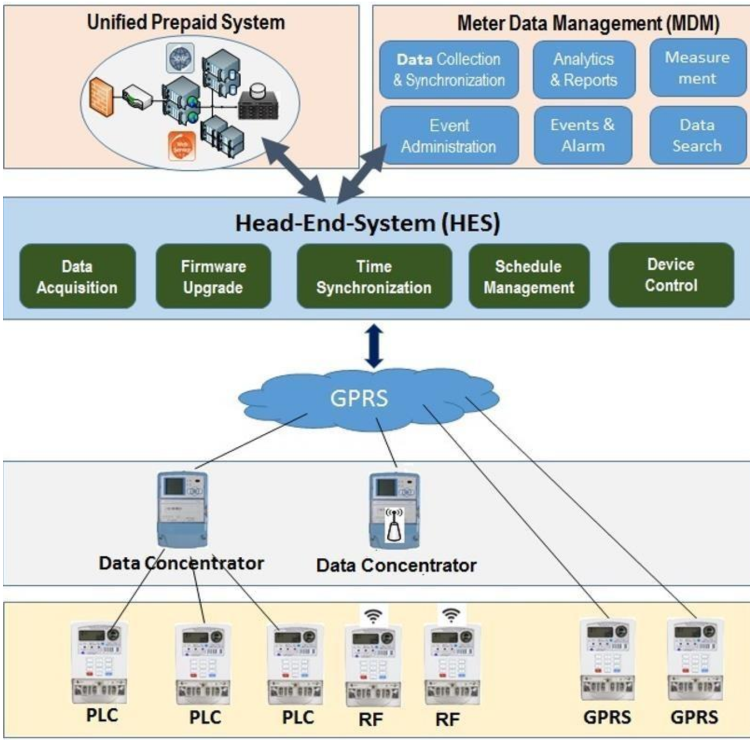


Figure 6

Electricity meters are being replaced by smart meters because they are more capable, dependable, and precise than conventional electric meters. Smart meters monitor energy use, automatically replenish prepaid electricity credits, and inform users of the energy usage of their household or commercial equipment. The components of the smart meter system include metering apparatus that is attached to the electrical circuit and measures overall electric usage. It functions as a lightweight communications gateway and contains a software-based application for managing gathered data. The gateway offers real-time data from a database through a mobile user interface. Each meter typically contains several communications technologies that can be chosen according to data rates, range, data type, and protocols. For utilities and consumers to better estimate their base and peak loads, enable demand-side management, 5 and provide quick automatic outage detection and restoration, communications and data exchange help quantify demand behaviors. The lifespan of smart meters is approximately

20 years.

3.2 Working Principle of GPRS System

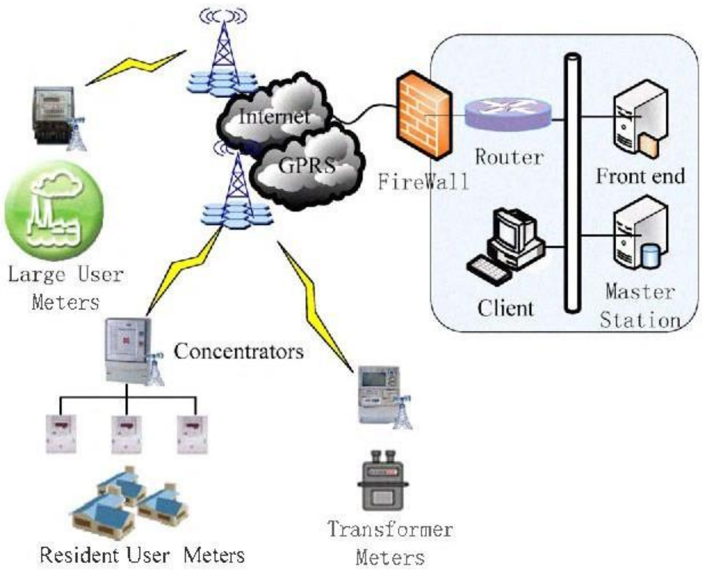


Figure 7

The usage of GPRS may be made possible via Internet protocols, which provide a range of services, including corporate and enterprise applications. The data is split up into individual packets before being transferred through radio and the main network. At the receiver's end, the data is reattached.

3.3 GPRS Roaming

Operators promoted roaming within Europe and eventually internationally when the unified European GSM standard was implemented. Data transmission speeds have greatly risen thanks to the GPRS1 standard, which offers transfer over a constant connection. Mobile carriers had only partially established bridges between their switching networks and data networks prior to the launch of GPRS. This study's objective is to demonstrate the new architectural designs required for GPRS roaming and their economic repercussions.

3.3.1 Mobile operators and GPRS roaming

Since the mobile Internet is already a reality, mobile operators who may provide Internet access to their clients must establish connections with operators from the data industry. Mobile carriers occasionally graft themselves onto the current Internet architectures, although they typically prefer their own to reduce the risks to the reliability and security of communications, dedicated infrastructures only enable access to the public Internet when it is required. This meant that mobile carriers had to establish connections between mobile networks in each of the countries to conduct the roaming data flow. The IP backbone operators' suggested solution, GRXs, was chosen by the operators.

3.3.2 Why GRXs?

There are several ways of There are three ways to connect the GPRS/IP networks of various mobile operators: directly between mobile operators, indirectly through the Internet, and indirectly through connections to GRXs (GPRS Roaming exchange).

The highest security and finest service are provided via direct connections between operators.

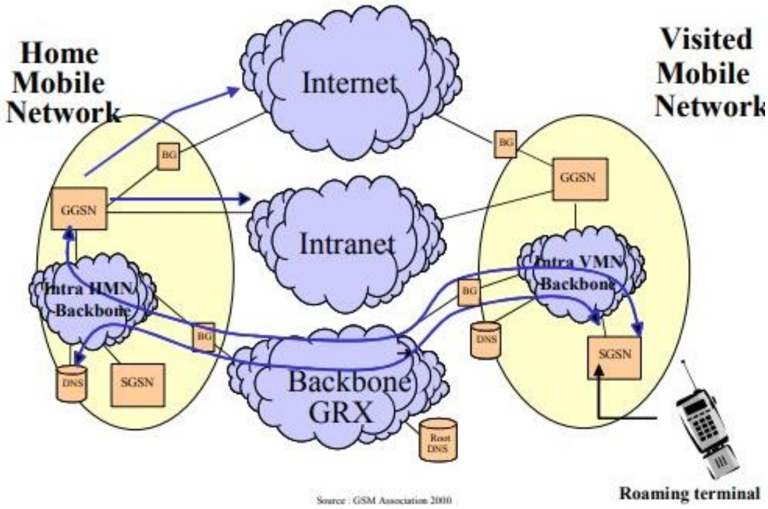


Figure 8

but also, the most money. In contrast, installing an indirect connection through the Internet's middleman is less expensive, but the security and service quality are subpar. Operator arbitration was therefore required.

They chose the GRX solution because it offers the best quality to cost ratio of all the alternatives offered due to the trade-off between quality/security and installation expenses.

3.3.3 The GRX operators: the international GPRS infrastructure

A new group of participants are GRX providers. They come from a variety of backgrounds, and after the GSM Association's move in 2000, they first became visible in the open. This "officialization," which acknowledged a strong partnership with mobile carriers, was required to speed up the global rollout of GPRS roaming. The majority of GRX operators have global IP infrastructures and have had to find solutions to challenging technical issues to provide a highly distinct private Internet from the public Internet.

The new arrangement in the ties between GRX operators and the mobile operators who use them is very advantageous to all the mobile carriers in Europe. The GRX operator shared by the group is typically chosen, even if the GRX is chosen independently by each of the overseas mobile subsidiaries. The GRX operator shared by the organization improves the value of its network through this "option,"

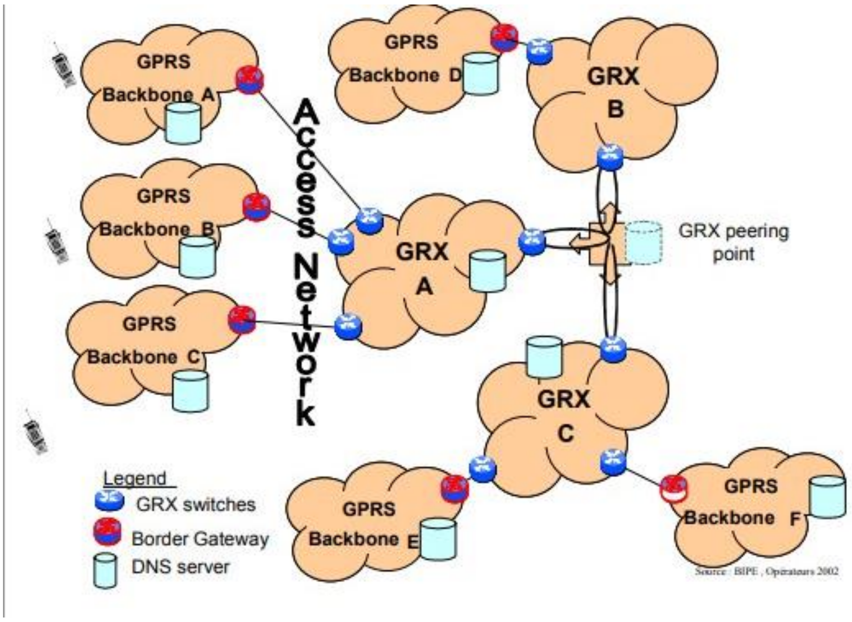


Figure 9:GRX Architecture

Exchange points between GRXs: The small quantity reflects the market's infancy. To overcome the model's inherent constraints, GRX operators have established the concept of places of exchange, like those found on the Internet (with GRX specific features). Currently, 15 GRX operators (Belgacom, BT, Deutsche Telekom, France Telecom, Sonera (with Equant), Telecom Italia, Telefonica Data, Telenor, Telia International Carrier, Cable & Wireless, UUNet, Equant (with Sonera), Aicent, Camphone, and TSI) interconnect through a single facility called AMSIX, which is situated in Amsterdam. The inherent imbalance of the architecture is somewhat addressed by this point of exchange (based on free peering).

This point is still distinct in Europe, but at least one additional point from Asia should shortly join it. However, if we contrast this small number of points with the numerous places of exchange that the public Internet currently has, we can see that it is due to the infancy of the national GPRS markets.

3.3.4 The Central DNS Problem

However, the issue of the central DNS for resolving addresses between the DNSs of the GRX operators remains unresolved. All the participants are actively debating the benefits and drawbacks of establishing a centralized DNS ("master root DNS") that can handle all address resolves between GRX operators and mobile providers. The advantages of a centralized DNS server are not well understood by all parties involved, even though the method is well known; the GRXs that federate many mobile operators are less interested in setting up this structure than their smaller equivalents.

Finally, the roaming of content remains an issue. Currently, a travelling user can access the same resources that they do on their home network. This trait may restrict the services available while roaming. Counterparts.

3.3.5 GRX: infrastructures without traffic flows but ready for the UMTS

The main issue that all GRX operators are currently dealing with is the inability of the GPRS roaming traffic flows to fully utilize the installed global infrastructures. Forecasters predict that the GPRS service will become widely used in 2003. Mobile providers will continue to have their dominant position in the GSM market as a result.

The core network changes required to implement the UTMS will undoubtedly be less significant than those impacting the radio component. The GRXs are prepared for this evolution, depending on the technological decisions made (migration of the IP networks now in use or creation of ad hoc IP networks for the mobile Internet traffic).

3.3.6 GPRS roaming billing flows: a new model that will develop

With GPRS, new players, procedures, and billing keys have been introduced. Operators have had to extensively alter their billing systems and related processes because of the shift from billing by time to billing by volume (the kilobyte has replaced it as the reference value). Due to their direct interaction with end users, mobile operators, who are at the center of the issue, have implemented creative billing strategies for roaming. However, the cost of roaming is still a deterrent at the present. Operators still must find a solution to the conjoined issues of their rates and enticing content.

According to whether they are flows between GRX operators (now based on free exchange) or flows between mobile operators (based on the roaming model), the financial flows are divided agreements reached between them, which are centered on the IOT2, among other things. As the service matures, the retail pricing for roaming, which are currently still expensive, could decrease. Last but not least, the money flows intended for content creators and aggregators employing GPRS are still not fully understood. The graphic below depicts all of these flows between mobile and GRX operators:

These financial flows do not forecast the financial flows, merely display the transport section.

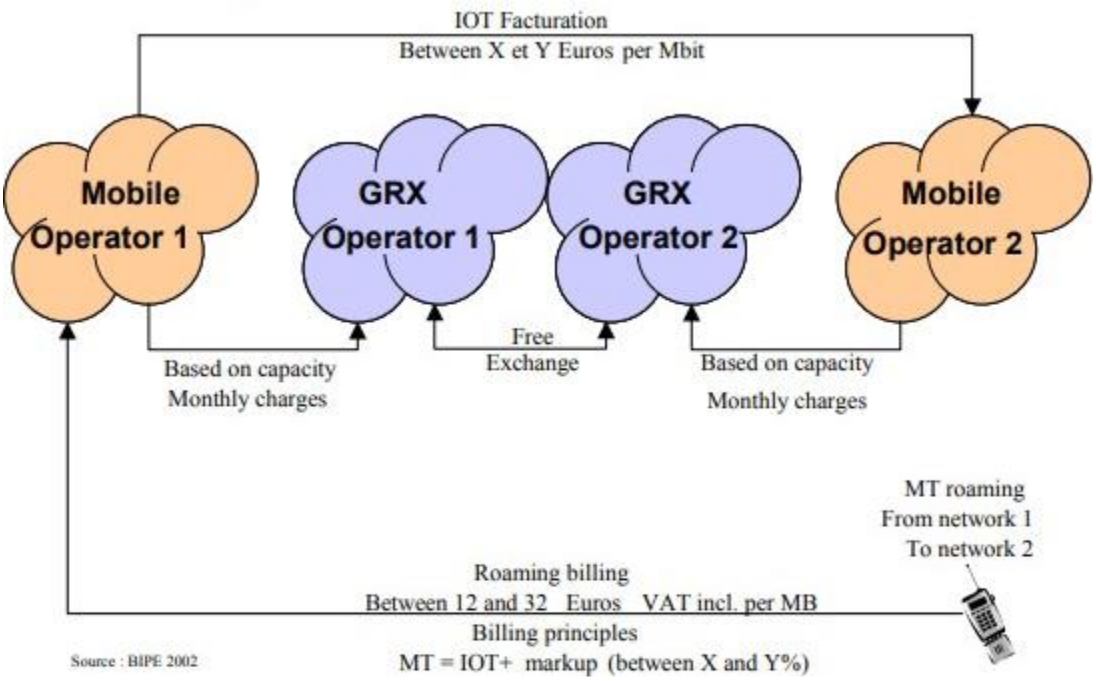


Figure 10: Financial Flows

service companies.

Finally, roaming costs are considerable and vary depending on whatever European nation is chosen. This makes it more difficult to understand the prices that roaming clients are charged. There is little doubt that users would want to pay a set charge in the very near future rather than one that varies from €12 to €32 depending on the country they are roaming in.

3.3.7 Pan-European operators at the center of GPRS roaming.

In the new world that GPRS will usher in, pan-European operators will play a crucial role. They will provide GRX operators the ability to establish a crucial position in the market because they are their primary clients. This means that if all or some of a pan-European operator's national subsidiaries choose a GRX operator, it gives that operator a significant competitive advantage in terms of market structure. Pan-European mobile operators truly do represent major actors for the business of GRX operators, especially if we consider the inherent asymmetry in roaming traffic flows.

Since GPRS traffic flows are currently minimal, there aren't any major conflicts arising between the various participants. Due of the significant pricing differences across nations and the national under-development of GPRS services, users are only minimally using the roaming feature in practice. Pan-European operators could have a substantial impact on the prices suggested in this situation.

3.4 GPRS Security for Smart Meters

3.4.1 GPRS Security Functions

On the interface between the mobile terminal and the GPRS core network, GPRS provides security functionality. The functionality that can be attained by using UICC/USIM in place of a SIM is described in this section, along with security functionality. It also gives a brief overview of security in the GPRS core network and ways to safeguard data sent from the core to the DSO across open networks like the internet.

3.4.2 Authentication and key agreement

Mobile users are authenticated to the network in GPRS. The circuit-switched GSM system uses the same native 2G authentication and key agreement (AKA) protocol as the packet-switched GPRS system, but the Serving GPRS Support Node (SGSN) handles the challenge-response process instead of the Visitor Location Register/Mobile Switching Center (VLR/MSC). When there is no difference between GSM and GPRS cases, we refer to these situations as VLR/SGSN cases. GSM-AKA, which utilizes interface3 functionalities A3 and A8, is the name of the authentication protocol (TS 43.020 [4]). Although the exact implementation depends on the operator, the GSM Association has several example methods on hand.

3.4.2.1 3.4.2.1 The GSM-AKA protocol is a two-stage protocol, as depicted in Fig. 2. Request transmission from VLR/SGSN to HLR/SGSN and triplet (authentication set) transmission from HLR/AuC to VLR/SGSN (steps 1 and 2)

3.4.2.2 3.4.2.2 Steps 3 and 4 of a network-initiated challenge-response (VLR/SGSN - SIM)

Elements used in the GSM-AKA Authentication and Key Agreement protocol

Table 2

Kc	SIM and HLR/AuC calculated a secret and communicated it with VLR/SGSN
Ki	SIM and AuC share a secret key.
RAND	VLR/random SGSN's challenge selection process
RES	Challenge outcome determined by SIM and emailed to VLR/SGSN
XRES	expected outcome of the task as determined by forwarded to VLR/SGSN by HLR/AuC

The per-subscriber authentication secret Ki, the AKA algorithms (A3/A8), and the tamper-resistant SIM card are all included on the permanent subscriber identification (International Mobile Subscriber Identity, or IMSI). The Ki is a pre-shared secret and is one-to-one related with the IMSI. While the Ki is only known to the SIM and the HLR/AuC, the IMSI will be known to numerous nodes and networks.

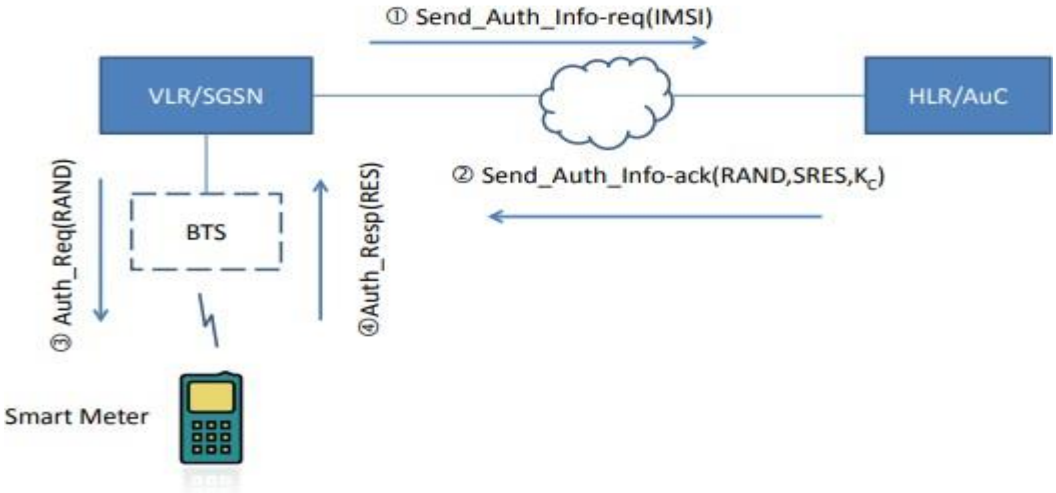


Figure 11: The GSM-AKA Authentication and Key Agreement protocol

Upon request, the HLR/AuC will generate triplets (RAND, SRES, and KC) and send them to the VLR/SGSN. The (pseudo) random challenge is represented by the 128-bit RAND, while the signed response is represented by the 32-bit SRES. the three A3/A8s the different Ax, charge functions specified by GSM and UMTS (A3, A5, f1, f2,...) are only standardized at the interface level, i.e., the required input and output is specified but the actual implementation is left to each operator. However, as will be discussed further in this article, many operators choose one of the example implementations that The GSM Association and 3GPP have disclosed.

One-way functions (Fig. 3), which should make it computationally impossible for an attacker to figure out the Ki and the KC after seeing the challenge-response exchange in plaintext

Procedure 4: After receiving the triplet, the VLR/SGSN challenges the SIM by sending the RAND. The SRES will be sent as the answer to the VLR/SGSN after the SIM computes the KC and SRES. Upon request, the SIM will transmit the encryption key to the MS. The authentication is deemed successful if the SRES from the HLR/AuC matches the outcome from the SIM. The outcome also entails sharing of the KC encryption key between the SIM and the VLR/SGSN. The 64-bit KC key for GPRS and GSM is the ciphering key that is employed.

It should be emphasized that certain A3/A8 implementations, particularly the original "example" method known as COMP128, are shoddy (completely broken [5, 6]). Additionally, keep in mind that GSM-AKA only creates a 64-bit session key, which is obviously not future-proof given the ongoing advancements in processing speeds for thorough key search applications. We advise using the GSM-Mileages [7] implementation of standard GSM-AKA, which implements the A3/A8 functions using UMTS mileages AKA functions and a set of conversion functions.

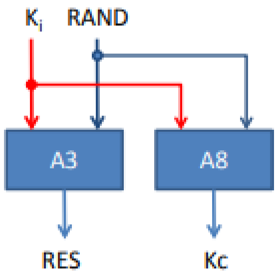


Figure 12: Using the GSM A3/A8 functions to perform GSM-AKA calculations

Keep in mind that, preferably also for chosen plaintext assaults, it must be computationally impossible to recover Ki even when the attacker can see numerous challenge-response exchanges. Ki shouldn't be recoverable even if an attacker has access to the entire triplet (including SRES and Kc).

3.4.3 UMTS Authentication and Key Agreement

If the subscriber uses a UICC/USIM module rather of the outdated GSM SIM, it is feasible to use the UMTS Authentication and Key Agreement (UMTSAKA) [8, 9] protocol via the "GSM Edge Radio Access Network" (GERAN). The functions of the UMTS AKA protocol are depicted in Fig. 4 and are defined in 3GPP TS 33.102 [10]. The secret key K and a random challenge RAND are the only inputs required by all interface functions f1 through f5, though f1 also requires a sequence number SQN and an authentication management field AMF. The following results are produced by the functions:

MAC- An authentication code for messages
XRES- Goal of the challenge
CK - Cipher Key for encrypting a later communication
IK - Integrity Is Crucial
AK - Key to Anonymity (for obfuscating the sequence number in case this exposes the identity of the client) The Authentication Center (AuC) computes these numbers, and further

$$AUTN = SQN \oplus AK||AMF||MAC\text{-}A$$

$$AV = RAND||XRES||CK||IK||AUT$$

The Authentication Vector (AV) can be thought of as the GSM triplet's UMTS counterpart. For a detailed list of the components utilized in UMTS-AKA, see Table 2.

The GSM triplet and the Authentication Vector (AV) are similar in many ways. The sequence number is covered up with the AK. The (RAND, AUTN) tuple is part of the SGSN challenge. The calculations shown in Fig. 4 are performed by the UICC/USIM, which then returns the value of f2 (RES). If the RES from the MS and the XRES from the AV match, this SGSN determines that the MS has been authenticated.

Table 3

Acronym	Explanation
AK	Anonymity Key, 48 bits
AMF	Anonymity Key, 48 bits
AUTN	Values for authentication calculated by AuC
AV	AuC's computation of the authentication vector sent to SGSN (the GSM triplet equivalent)
CK	128-bit Cipher key used for data encryption (Key to confidentiality)
IK	Integrity key of 128 bits
K	Pre-shared 128-bit Secret key between USIM also AuC
MAC-A	Message Authentication Code 64-bit, "signature" to verify the difficulty
RAND	128-bit challenge chosen at random VLR/SGSN
RES	the challenge's 32-128-bit result as estimated by Sending USIM to SGSN (default 64 bit)
SQN	the 48-bit sequence number
XRES	32–128-bit expected outcome of the challenge as determined by AuC and sent to SGSN (default 64 bit)

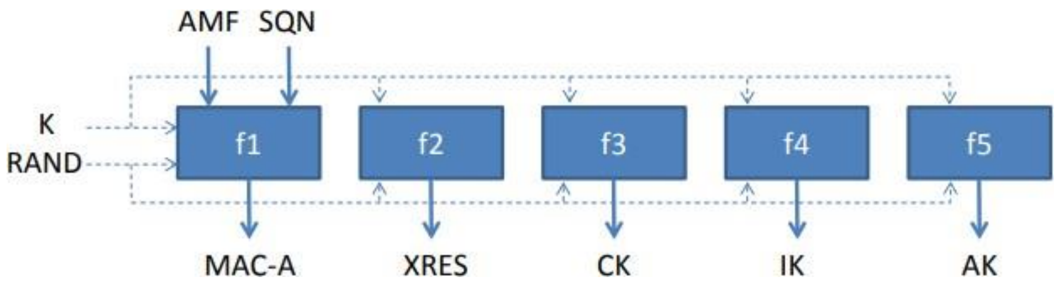


Figure 13 UMTS Authentication and Key Agreement (AKA) functions

The mileages algorithm given [11] by 3GPP serves as an illustration of how the f1-f5 functions are implemented. The Rijndael cryptographic algorithm, which implements the Advanced Encryption Standard (AES), is part of the mileages algorithm set, together with a collection of constants and parameters that allow all of the UMTS AKA functions to provide independent output.

3.4.4 GPRS Encryption

With GPRS, all data and signaling traffic between the mobile station and the GPRS core is encrypted across the wireless interface. The GPRS family of ciphering algorithms is known as the GEA family of algorithms (GEA, GEA2, GEA3, GEA4). TS 41.061 [12] contains a definition of the GEA interface. We should reiterate that, in contrast to GSM, where ciphering ends in the BTS, 2G GPRS ciphering ends in the core network (CN) in the SGSN. The A5 series of algorithms (A5/1, A5/2, A5/3, and A5/4) are the GSM equivalent ciphering algorithms; the A5/2 algorithm has been deprecated, and the A5/1 algorithm is now beginning to show its age.

Except for GEA4 (and A5/4), which uses a 128-bit key, both GSM and GPRS employ the 64-bit KC key as their ciphering key. Although the 64-bit architectures of the original GPRS algorithms (GEA and GEA2) are comparable, the GEA method has been updated to only use 54 significant bits. This is a result of the loosening of export restrictions following the end of the Cold War, which allowed the GEA2 algorithm to recover the 10 lost bits.

The Keystream Generator Core (KGCORE) block cipher mode, which in turn employs the KASUMI5 block cipher, defines the GEA3 algorithm. The interface accomplishes this by employing the KC key twice, while the KGCORE primitive is internally based on a 128-bit key. The GEA4 encryption technique with the KC128 128-bit key is also compatible with GPRS. Although the KC128 key is used directly in GEA4, KGCORE is also used there. The subscriber needs to run the UMTS AKA protocol and use a UICC/USIM to use GEA4 (or A5/4 in GSM).

While a 3G/UMTS identification module (UICC/USIM) may be utilized in a 2G device (GSM/GPRS), the cipher function invariably needs to be compliant with the over-the-air interface. This calls for the conversion of the UMTS key pair (CK, IK) into the 64-bit KC key (or the 128-bit KC128 key for GEA4).

The mobile station chooses the encryption technique by stating which GEA version(s) it supports, and the SGSN chooses which version will be used [13]. The connection might be cut off if they do not support a common algorithm. The SGSN may elect not to encrypt the data as an alternative. Contrary to appearances, KASUMI is not an acronym but a proper word (called "mist" in Japanese). Beyond the SGSN6, GPRS's built-in security features do not provide confidentiality or integrity protection; as a result, all data transferred via the GGSN's public internet interface (Gi) is sent in plaintext. GERAN receives no integrity protection at all. However, it is feasible to establish up a VPN tunnel from the Gi-interface to an external network using this approach by configuring so-called access point names (APNs) at the GGSN. Such solutions7 are already utilized in commerce to some extent.

3.4.5 Core Network Protection

The SGSN is where GPRS's access security comes to an end. GPRS Tunneling Protocol is used to transmit data between the SGSN and the GGSN (GTP). There are different GTP versions, and there is a difference between the control plane (GTP-C) and the user plane (GTP-U) (GTP-C). The core network may still be 3G or 4G compliant even though the access method may be GERAN. Any version of the GTP protocol by itself does not offer security. Although it is not strictly required by 3GPP, cryptographically protecting the GTP protocol is highly advised [10]. Specifically, the Network Domain Security (NDS) section is where the 3GPP has profiled IPsec for usage within 3GPP systems (TS 33.210 [14]). Initially designed for inter-operator use, the NDS/IP [14] is now being utilized for all IP-based interfaces in the 3GPP system. We strongly advise against using anything other than NDS/IP to protect GTP.

3.4.6 GPRS Closed User Groups

In cellular networks, it is feasible to create closed user groups [15], but because there is no substantial security offered, this can only be used as a last line of defense. Additionally, the service is somewhat meaningless because it is truly designed for circuit-switched calls.

3.5 Comparison of Popular Communication Technologies for Smart Metering – GPRS

Table 4

Advantages	Disadvantages
Advanced technologies	AMI's majority of benefits—all but meter reads—cannot be obtained.
Cost-effective and standardize communication modules	rapid technological evolution (2G, EDGE, 3G, LTE, and 4G)
The best way to automatically collect meter readings from a select group of consumers who are dispersed throughout a big geographic area	limited scope and scalability High monthly recurring costs for each SIM card for cellular operators
quickly deploy	limited reach (weak data network in villages)

Chapter -4

Methodology

METHODOLOGY Starting with the topic selection and ending with the writing of the final report, the study is carried out in a systematic manner. Identification and data collection played a crucial role. Once the important points had been determined, they were systematically categorized, examined, translated, and presented. The overall technique used in the study is described in more detail.

Selection of the topic:

The study's topic was given to me by my supervisor. Before the topic was assigned, it was thoroughly explored to enable the creation of a well-structured internship report.

Sources of Data:

Primary Sources:

The practical deskwork served as the source for the primary data. Additionally, I received assistance from my DPDC supervisor in contacting the business directly for information.

Secondary Sources:

Internal sources: The organization's many circulars, manuals, and files, as well as various documents supplied by concerned officers.

External source: Various websites and online resources relating to the GPRS technology.

Classification,analysis, interpretations, and presentation of data:

In order to analyze the data gathered and to better clearly explain specific concepts and findings, some diagrams and tables were utilized in this study. Furthermore, the collected data underwent a more thorough analysis.

Findings of the study: The acquired data were carefully evaluated, and the results were highlighted and presented as findings.

Final report preparation: The final report was created using my worthy advisor's insightful recommendations and counsel.

Chapter -5

Discussion

5.1 Smart Metering:

5.1.1 The Smart Meter

5.1.2 An electrometer that measures electricity use over time is a smart meter. The advantage of these meters is that they communicate with and receive commands from the main hub or command center. The smart meter has a two-way communication feature.

5.1.3 Smart Metering Features

- The Utility can remotely turn off all smart meters.

- The meter cover must be opened before changing plugs.

- The timestamp is recorded in the meter.

- Send the command center a quick notification of any crucial events.

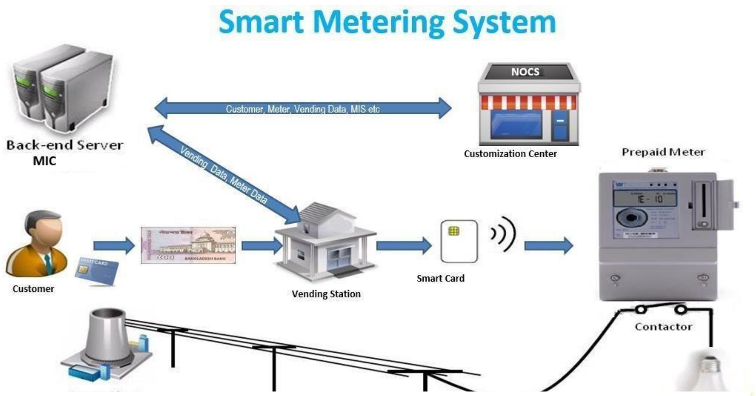


Figure 14

5.2 Benefits to Utility:

1. Commercial Advantages:

- Automated meter reading: Increasing the effectiveness of billing
- Remote Disconnection - Increasing the Effectiveness of Collection
- Enhancing Data Analytics - Increasing Tamper Detection Hit Rate - Increasing Capturing Maximum Demand - Increasing Revenue Through SAC & Fixed Charges
- Reduced Ad-hoc readings result in time and resource savings
- Real-time energy audits that detect dead meters more quickly lead to a shorter revenue billing cycle.

2. Benefits to operations:

- To determine asset use, overloading, etc., DT Meters on the same canopy are used.
- Manual Disconnection / Reconnection Removal
- quicker detection of outages
- Monitoring of Power Quality in Real Time

3. Consumer Advantages:

- Fewer outages and errors Due to no manual intervention, bills are free.
- The choice is prepayment.
- more accurate use visibility via mobile app
- Integration of Renewable Energy Facilitation
- incentive to keep PF over 0.85

5.3 Challenges of Smart Metering in Bangladesh

The development of the smart meter presents a variety of design issues. One of the first issues is defining characteristics clearly because smart meters for home and utility use fall under different feature sets with little overlap. By using the best hardware and software, the user community's definition of the criteria can reduce the cost of the smart meter. The following is a summary of some of the characteristics that can affect the price and modularity of the design:

i. **Communication Protocol:** To prevent proprietary protocols from making their way into Smart Meters, it is crucial that specific communication protocols be standardized or required by a centralized agency.

ii. **Communication Security:** As remote-control functionalities are implemented and critical revenue data is communicated, communication security in an AMI/Smart Grid context will become a top priority. It is crucial to specify which specific IEC 62351 standards must be implemented into the meter firmware for it to work with AMI and MDM systems.

iii. **Interoperability:** It should be assured that the control commands and other data formats used in smart meters are compatible with the current AMI infrastructure.

iv. **Meter Data:** Different measurement parameters are needed for different consumers (utilities, industry, and homes). It is essential to standardize parameter needs across customer segments.

v. **Communication ports:** Since Ethernet and optical Ethernet will be used for the Smart meters instead of the Serial connector and USB, the case design and upgradeability will be improved with the help of port specification.

vi. **Communication:** Smart meters provide a wide range of communication options, including wireless (Zigbee, Wi-Fi, Low Power RF) and power line. It would be ideal to identify this choice as allowing for specialized research, analysis, and application.

vii. Standardizing the size and footprint of smart meters is another crucial factor.

viii. **Power Quality Requirements:** Higher order harmonic distortions, Sag, Swell, Outages, Dips, Transients Recording, and Recording Duration will all need to be described, along with the types of power quality measurements that must be taken across various consumer groups. The cost of the smart meter will be reduced if these requirements are clearly defined since, they will affect how digital signal processors and high-speed memories are used to execute the power quality measuring feature.

5.4 Challenges of GPRS System for Smart Metering

Most AMI benefits cannot be received, except for meter readings. Rapid advancement in technology (2G = EDGE = 3G = LTE = 4G. Limitations of scalability and spectrum High operating costs, with cellular providers paying ongoing monthly fees for each SIM card. limited scope (village data networks are inadequate).

5.5 Experience as an Intern at DPDC:

Some of us East West University students took part in the DPDC's three-month internship program at the end of May 2022. The internship program places particular emphasis on the following subjects:

(a) Under the government's Power Sector Reforms 1, the introduction of electricity supply and the progressive development of PDB, REB, DESA, DESCO, and DPDC

(b) The DPDC's power supply system.

(c) The DPDC's Network Operations and Customer Service (NOCS) operations.

Activities of NOCS's supporting offices (d) (e.g.: HR, Finance, ICT, Audit, Planning, Development, Metering, System Protection, Grid, Tariff and Energy Audit).

(e) The DPDC Training and Development Department's activities.

(f) Inspecting the 33/11 KV and 132/33 KD GIS substations.

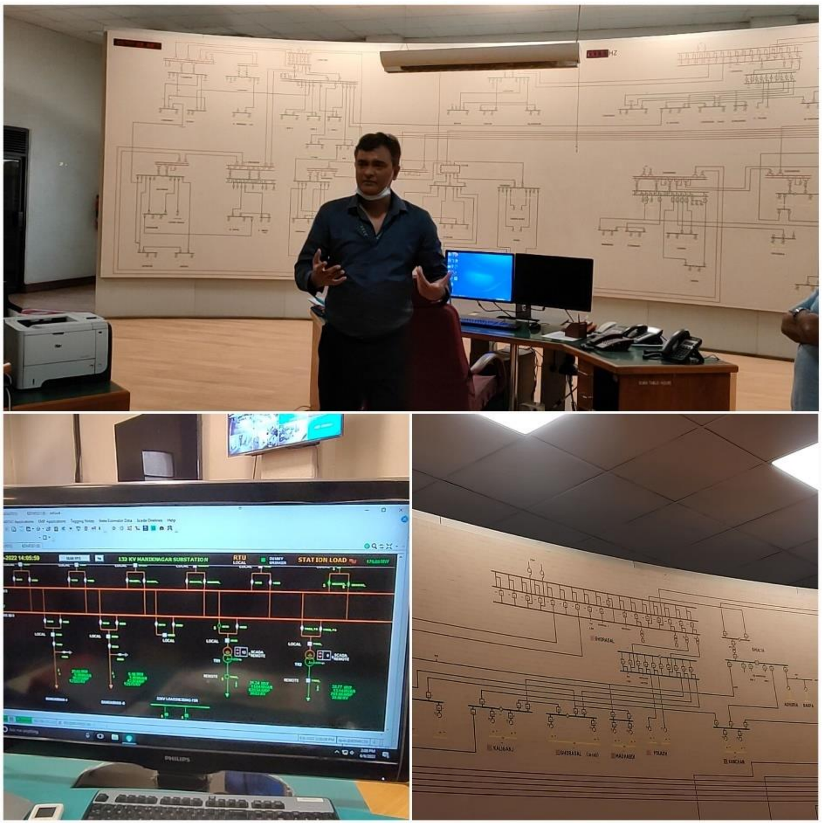
(g) SCADA system, workshop, meter testing lab, central warehouse, and DPDC medical center inspection.

5.5.1 Visiting Sites:

Dhanmondi Sub-Station:

Grid Sub-Station (Shahjahanpur):

SCADA (Supervisory Control and Data Acquisition):



DPDC Library

132/33 KV GIS:

5.6 Ongoing Projects of DPDC

1. Detailed description of self-financed projects

Projects finished during the fiscal year 2021–2022 include:

1. Project Title: Turnkey Design, Manufacture, Supply, Installation, Testing, and Commissioning of Smart Pre-Payment Meter at NOCS Kamrangirchar.

Ongoing Projects:

Mohammadi 132/33 KV Grid Substation Design, Manufacture, Supply, Repair, Service, Installation, Testing, and Commissioning on Turnkey Basis.

Smart Pre-Payment Meter Design, Manufacture, Supply, Installation, Testing, and Commissioning at NOCS Bangla Bazaar with Three Years of Maintenance Support Service on Turnkey Basis.

Projects included in the Annual Development Program (ADP): **Projects completed in FY 2021-2022:**

01. Project Name: DPDC is building a new 132/33 KV and 33/11 KV substation.

Ongoing Projects:

- **I.** Project Name: Pre-payment Metering Project for 06 NOCS under DPDC.
- **II.** Project Name: Power distribution system expansion and reinforcement in DPDC areas.
- **III.** Project Name: Power Distribution System Development Project in DPDC Areas.
- **IV.** Name of the Project: Installation of 8.5 million smart pre-payment meters in the DPDC-affected area.
- **V.** Project Name: Construction of an underground substation is being done by the DPDC in Kawran Bazaar in Dhaka.
- **VI.** Project Name: Building and renovating substations, adding capacitor banks to the power grid, and installing a smart grid system in DPDC areas.

Chapter 6:

Conclusion and Future Work

6.1 Conclusion

The strategic uses of GPRS systems over the electrical grid for smart metering have been discussed in this study. To comprehend how GPRS might fit in the Smart Metering networks, the history, benefits, and limitations of GPRS systems have been demonstrated. The paper's justification is the requirement for further development of these GPRS systems' architecture and design for them to provide the capabilities required for the Smart Grid.

In Chapters 2-3, system choices that enable GPRS systems to adapt to various Smart Metering scenarios are discussed. The MV and LV grid segments' communications architecture, which must be developed, is the first thing that needs to be considered. Here, the throughput requirements are a crucial factor to be taken into consideration, along with the isolation level of the GPRS systems used in the MV and LV segments' connection points, or the SSs. The GPRS signal injection at the SSs and the capabilities of the selected GPRS system will influence the performance results once the architecture has been decided.

To wrap off the chapter, precise low-level recommendations on the MAC layer are given, with packet size, FEC methods, and automatic retransmission being the most crucial ones. NB GPRS systems are the most used ones for Smart Metering networks.

The deployment instructions for NB GPRS systems are in Chapter 3. If signal repetition due to low SNR is required, these criteria should be followed both in the SSs (GPRS signal injection from the system masters) and at various places in the LV grid. The multi-transformer scenario outlined in the chapter and the type of the signal injection have a significant impact on signal injection method (single- or three-phase). These recommendations will be successful in producing the desired performance outcomes.

This essay also discusses our internship experience with DPDC. We also talked about the DPDC's smart meters, current projects there, etc.

6.2 Future Work

The difficulties that GPRS systems have as they develop to meet the demands of Smart Grid networks are discussed in the paper's conclusion. The necessity to better enhance the current GPRS system is stressed on one side. On the other hand, it is revealed that using the interaction between GPRS systems and the grid would help both GPRS systems work better and provide us more insight into the grid. The combination of GPRS and non-GPRS technologies is proposed as a potential solution to open the door to Smart Grids as a final thought.

References

[1] Berganza, I. et al., 2011. PRIME on-field deployment. Udine (Italy), Proceedings of the IEEE International Conference on Smart Grid Communications.

[2] https://en.wikipedia.org/wiki/Gprs

[3] https://www.researchgate.net/publication/327389488_Smart_Metering_Systems_Based_on_gprs.

[4] https://dpdc.gov.bd/site/page/816191d7-0196-4e00-aa59-4e3cf6a400a4/-

[5] https://en.wikipedia.org/wiki/Dhaka_Power_Distribution_Company

[6] https://dpdc.gov.bd/site/page/00beca42-bc18-4bb9-960e-a5ad8132815a/-

[7] https://www.ivy-emeter.com/html/bangladeshmarketBangladesh%20market-show-242.html

[8] https://bdelectricity-com.cdn.ampproject.org/v/s/bdelectricity.com/dpdc-prepaid-meter-codes/amp/?amp_gsa=1&amp_js_v=a9&usqp=mq331AQKKAFQArABIIACAw%3D%3D#amp_tf=From%20%251%24s&aoh=16739092055304&referrer=https%3A%2F%2Fwww.google.com&ampshare=https%3A%2F%2Fbdelectricity.com%2Fdpdc-prepaid-meter-codes%2F

[9] https://www.meterandcontrol.com/products/ami-devices/sx402/

[10] "Smart Energy Metering with real time Power analysis and Auto Monthly Billing", Youtube, 12th May 2019 [online]

[11] Benzi, F, Anglani, N., Bassi, E., et al.: 'Electricity smart meters interfacing the households', IEEE Trans. Ind. Electron., 2011, 58, (10), pp. 4487-4494

[12] Gungor, V.C., Sahin, D., Kocak, T., et al.: 'Smart grid technologies: communication technologies and standards', IEEE Trans. Ind. Electron., 2012, 7, (4), pp. 529-539

[13] GPRS – General Packet Radio Service a book by Regis J. "Bud" Bates

[14] https://onlinelibrary.wiley.com/doi/book/10.1002/0470869550