DATA PRESERVATION AND ENERGY THEFT CONTROL IN SMART METERS

A. hammad GHAFFAR , B. muhammad sohaib SHAHEEN , C. aamir MEHMOOD ,

D. hassan erteza GELANI

[A,C] Center for Energy Systems, National University of Sciences and Technology Islamabad, Pakistan

[B] School of Electrical Engineering & Computer Science, National University of Sciences and Technology, Pakistan

[D] University of Engineering and Technology Lahore, Pakistan

[A]hammad.uet@gmail.com

[B]sohaib.dmc@gmail.com

[C] aamir.mehmood08@gmail.com

[D] erteza_gelani@yahoo.com

Abstract*: Smart metering is an evolving technology, which has attracted attention across the world because of its technical and economic feasibility. Despite many advantages associated with smart metering there has always remained a certain degree of reluctance among governments in implementing this technology on large scale owing to the security risks and implementation constraints associated with it. This paper addresses these security risks in depth and will focus on developing a model, which enhances the security of data transmission, preserves data using distributed network and provides a novel, GSM based, technique to control energy theft. This model can be implemented in conjunction with smart grids to triangulate the areas where energy theft is taking place, so that legal action may be taken against the culprits on solid grounds.*

Key words: *smart meter, energy theft, distributed networks, network congestion, data preservation*

1. Introduction

The need for efficient power distribution has become inevitable because of the ever-increasing demand for power distribution to far areas. Also the existing check and balance mechanism using 'dumb' meters [1] can no longer operate properly with such large user base that currently exists.

Many countries including Italy, Japan, Australia and USA have already brought smart meters into field-testing, comprehending the long-term advantages that may be derived from this technology despite having high initial cost. Also the concept of smart meters and AMR (automatic meter reading) [2] can be implemented without requiring any major functionality changes in supervisory control.

The variety of functions performed by a smart meter is particularly dependent on the demographics [3] while some general functions can be associated with all the smart meters, namely:

(i) Power Calculation
(ii) Load Management
(iii) Interconnection to data center
(iv) Remote Connection and Disconnection
(v) Ability to read meter readings on premises and by remote data center

Theft of service in electric meters is nothing new and various software attacks along with the mechanical manipulation of energy meters are likely to cause an increased energy theft [4]. However security [5][6] and costs [7] associated with smart meters will play crucial role in their ultimate acceptance by governments and general public. Much research has been carried out on cost feasibility and optimum construction of smart meters while very less emphasis has been placed on data preservation and theft control which to no

doubt be most important considerations when it comes to countries like Pakistan. In Pakistan losses were around 30% in 2007 with major contribution of energy theft to these losses [8]. Energy theft is now at intolerable level and the only viable solution to this problem is the installment of smart meters.

This paper takes systematic approach starting with construction of meter, using easily accessible components leading to the implementation of core modules that will handle security, theft control and distributed network. The prototype has been designed by keeping in mind large-scale implementation, which may lead to network congestion or possible network failure. This module also makes sure that GSM based meter communication has not been disconnected or been jammed using any kind of mobile phone jammer. The prototype utilizes client-server model for remote connection/disconnection and reading of meters.

GSM module handles the communication between smart meters and server (on nearby grid) while on-demand transfer of data makes sure the network congestion is avoided. Modular approach has been taken so that each module can be updated or replaced without affecting any other part of system. This paper also mentions the models of components used, so smart meter may be replicated to carry out further research.

2. Smart meter design (Experimental)

Through the experimental work the implementation of data preservation and theft control into the smart meters has been proposed on commercial scale. This work includes all the necessary calculations and steps description, needed for the practical design. These measurements are obtained from the designed prototype operated and tested in practical but controlled conditions.

The work starts with the designing of smart meter used to achieve the desired targets. A different approach has been adopted for the design of smart meter, which according to literature is the best technique for data preservation, power theft prevention and to avoid the network congestion.

The main features of this smart meter are:

- Power consumption calculation and record.
- Variably encrypted data transmission using the best encryption techniques ever evolved.
- Detection and Reporting of GSM jammer using Polling.
- The use of built in memory for continuous preservation and updating of stored data in case of jammer blockage.
- Mechanism to resolve network congestion using choke bit technique
- Remote switching of the supply.
- Load management with the provision to provide extra units to the customer on increased rates in case of extra demand placement and switching of phase in case of overloading on any one phase.

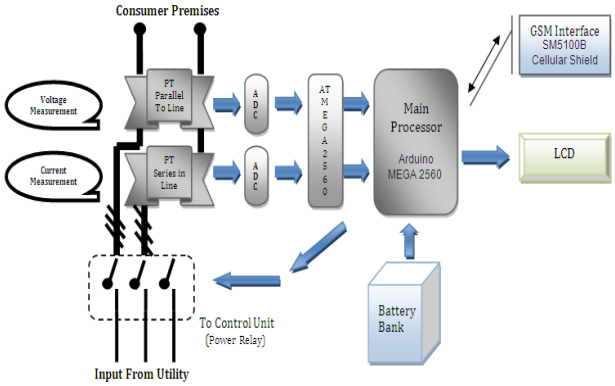

Fig.1. Main block diagram of Prototype

Construction and Working of Smart Meter:

Major parts of the smart meter are shown in the block diagram. The implementation begins with the measurement of power consumed. For this purpose two potential transformers (PT's) are used to convert the high voltage (usually 220V) and current levels down to a lower level, within operate able limits of the electronic equipment used. The potential transformer installed in parallel to the load converts the voltage level from 220V to 3V and the current transformer installed in series with the positive wire changes the high current to a range of 0 to 25mA. Another method of current measurement is the use of a low ohm value and large wattage resistor in place of potential transformer. The voltage drop across the resistor is measured and is divided by the value of resistance to get the line current. This method is used for the verification of current measurement in our prototype.

Both the analog inputs of these transformers are fed to ADC (Analog to Digital Convertors). The digital output of these analog to digital convertors are then fed to controller (AT MEGA 2560) where the calculations are performed to measure the power

consumed. The controller takes the product of current and voltage to obtain the power consumed in watts. This procedure is repeated after every five seconds and the corresponding results are saved. For a total time interval of six minutes 72, V*I samples are stored. After six minutes the average of these samples is divided by 1000 and multiplied by 0.1 to obtain the power in kWh. This is the actual value of power currently being consumed, which is saved and displayed on the LCD.

After the interval to calculate the average, the new values of VI samples start overwriting the old ones. During this procedure the Arduino waits for the message of server for data fetching. If data demand signal is received then Arduino generates an interrupt to fetch the values from the controller and transmits it to the server via GSM. If no message is received from the server then new calculated values of power in kWh are added to the previous and over written in memory.

This smart meter continues its operation even in case of electricity shut down which may result from temporary or sustained interruption. Even if the voltage level falls for short interval due to voltage sag, the battery bank supplies the backup power and keeps the data preserved. The prototype uses 3 Energizer EL2CR5 1500mAh rechargeable batteries with 6.0 V output. Total capacity is 3x1500 m-Ah = 4500m-Ah.

Components	Current Drawn
SM5100B	7 mA
Arduino MEGA 2560	50 mA
LCD matric 2x16 white backlit	45 mA
ADS8254 (Analog to Digital Converter)	3 mA
Miscellaneous (including operating current of relay, rectifiers, diodes, PTs and transistors)	100 mA (approx.)
TOTAL	205 mA

Table.1. Current drawn by components

Battery can work for 4500/205 ≈ 22 hours in case of electricity shutdown. The backup battery ensures data preservation in such cases.

3. Client-server model and GSM interfacing

In host-to-host communication, used in traditional smart meters, the meter reading is transferred continuously to the server (placed on nearby grid) giving rise to so-called real time communication. While this model ensures up-to-date data at any instant, it can lead to network congestion or possible network failure. Our prototype utilizes the client-server model to alleviate this problem. Data is stored locally on smart meters and is only transferred to server once demanded. The area is divided into physical and virtual regions. The former division makes data preservation possible while latter allows us to locate the region where energy theft may be taking place to certain degree of accuracy, which is dependent on the size of virtual segment.

Physical regions are divided, based on sub station's location i.e. meters in any specific region will be connected directly to 132KV grid station, which in turn will be connected to transmission substation, this hierarchy continues upwards till generation substation where complete data will be present.

Virtual regions are divided based on actual location of smart meters. Size for a single virtual region is highly dependent on capability of smart grid and defines the accuracy of triangulation for energy theft control. Difference in power delivered to certain area (single virtual region) and power consumed may be used to detect energy theft.

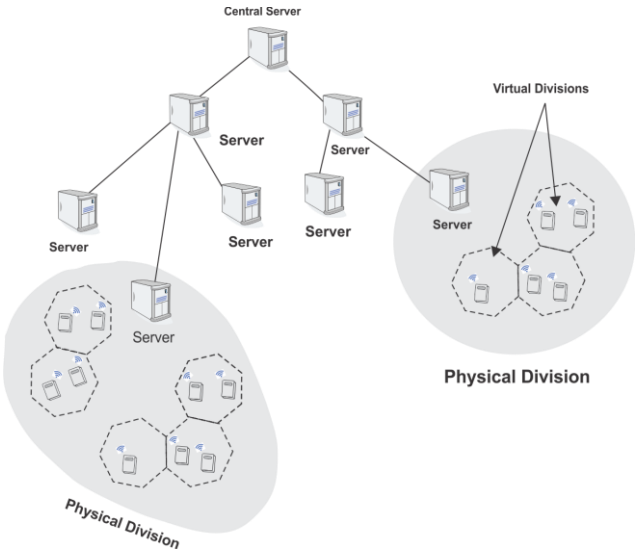

Fig.2. Physical and Virtual divisions

Another reason for using client-server model is enhanced security. In proposed model, each time a unique *rounds variable* is sent to meter, based on which the encryption code is executed which makes code decryption on client side virtually impossible. Encryption is discussed in greater detail in next section.

The model utilizes GSM for communication between server and client (smart meter). Control commands are transferred as messages with particular syntax. The use of GSM is proposed due to obvious reasons of availability and ease of implementation. While other communication methods like ZigBee [9] may equally be suitable and even better in some cases, they will add to cost overheads because whole network will need to be established. GSM has already been implemented on large scale and present system may be used to accommodate for connection of smart meters too. The European Telecommunication Standard Institute (ETSI) GSM 07.05 defines the AT-Command interface for GSM compatible modems, which was in-fact used in our model. SM5100B module used for GSM interfacing is quad-band 850/EGSM 900/DCS 1800/PCS 1900 module with baud rate of 115200 bps.

4. Encryption and data preservation

Encryption is absolute necessity when it comes to wireless transmission. If unencrypted message is sent over wireless channel it may be read, altered or destroyed easily. Our model utilizes end-to-end encryption based on AES (Advanced Encryption Standard) [10]. Symmetric keys are hard-coded into non-readable and non-programmable memory segments of controller. An off-the-shelf library for AES in C++ has been used.

Data preservation is another important consideration, which must be taken into account for successful implementation of smart meters on large scale. The data should be saved and utilized in such a way that information is not lost in case of network failure or server break down. Distributed network is an optimum solution to such problems.

Our prototype utilizes three different techniques for data preservation. First one is acknowledgment - when the server requests data from smart meter, data is transferred to server and previous values are over written but to make sure the data isn't lost in mid-way an acknowledgment is sent back by server to smart meter, on reception of which the smart meter actually starts overwriting. This ensures data has reached at destination and is safe now.

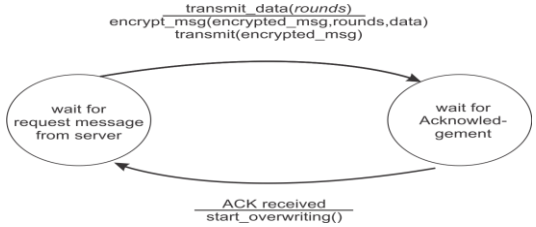

Fig.3. Data flow from smart meter to server

On receiving request from server for data (*transmit data*) the smart meters encrypts the message using technique discussed and then transmits this message to server. It then goes into wait state, waiting for acknowledgement from server. Once acknowledgement is received (*ACK received*) it starts overwriting previous values.

Second is distributed network of servers. The effects can be catastrophic if server breaks down or hard disk crashes, to prevent such hazards our model supports storage of data on distributed servers connected through conventional DSL (Digital Subscriber Line) links. We have assumed a reliable DSL connection is available. Data is collected at nearby grid, which transmits this data to far sub stations until generation substation receives the data and stores it in central database. In case of server break down last data may be recovered from central database.

Each smart meter has also built in 256 KB of memory for local storage of data. Smart meter keeps last un-delivered data stored locally, which means if server is down for some reason, and couldn't request for data transmission, the data can still be recovered after the server is reinstated.

5. Polling

The implementation of on-demand transfer of data based on client-server model has several advantages, as already discussed, but it also presents a challenge to us. While we don't want the network to get congested if large numbers of meters start transferring data simultaneously we also don't want that any meter be disconnected from network, which may be deliberate or unintentional. To control such situation our model uses polling, as we call it, to keep check if meter has been disconnected or jammed. Mobile phone blocker can pose great security risk. It can be used to seize the

communication between client and server, which means that user's power consumption record, will no longer be transferred/registered with server and the billing cycle may be severely affected. This paper addresses the above issue in detail and a model is presented, based on choke bit, which ensures meter is on-line all the time and has not been jammed.

The so-called Choke bit techniques has its roots in networking where network congestion is detected on base of choke bit, while we have utilized it to detect if the meter is online. To avoid network congestion only one virtual region is polled at a time starting with the one having smallest segment identifier i.e. 0001. All meters in one virtual division are sent a particular message having format '**POLL** *choke bit*'. A successful poll means that smart meter on receiving this message should acknowledge by sending '**ACK** *choke bit*' message. While data loss is quite probable in today's networks having huge speeds, so each meter is given 3 chances. If first acknowledgment is lost another poll message is sent until total of 3 messages are sent. If smart meter fails to acknowledge any of the poll messages then it is flagged for manual inspection.

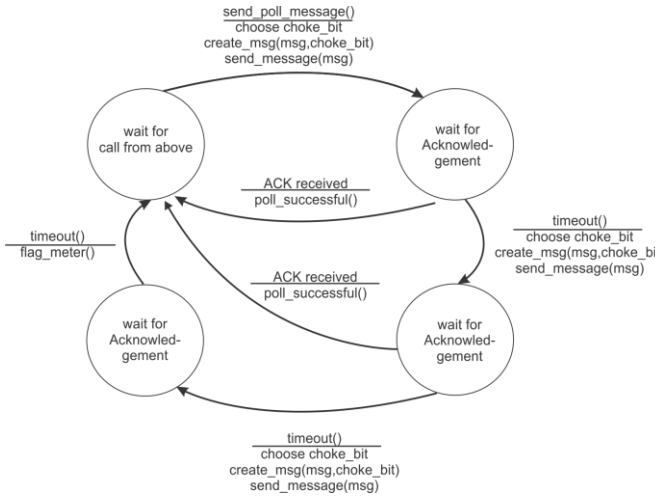

Fig.4. Server side polling state flow diagram

Once all the meters in certain virtual segment have been marked *OK* or *Flagged* next virtual segment is polled and process continuous recursively. This method of blockage or disconnection check has several advantages, the most important being no data overheads (message size is small) and network congestion avoidance due to polling of single virtual segment and light-weight transfer of data.

6. Power theft control

This smart meter has the capability to detect the power theft if used in conjunction with smart grid. GSM based technique is used for this purpose.

Each smart meter has a GSM module, which works on Micro SIM. SIM numbers can be utilized to uniquely identify each virtual region and smart meter. The diagram shows segmentation of SIM number. Virtual segment identifier can have possible 10^4 = 10,000 values, which allows for division of each physical region into maximum of 10,000 virtual regions. For smart meters 10^3 = 1000 possible permutations are available, which means each virtual region can have maximum of 1000 smart meters. A complete virtual region can only be tracked for energy theft, which leads to obvious conclusion that size of virtual segment should be small enough to identify a manually searchable area.

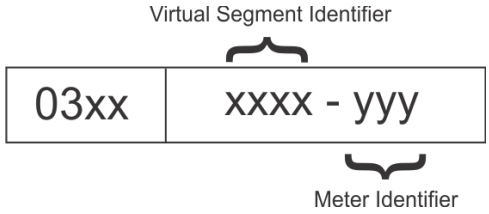

Fig.5. SIM number segmentation

Smart grid can identify the total amount of power supplied in a virtual region. Here virtual region is considered as the area in which power is supplied by a single distribution transformer (almost 25-35 homes). The server also calculates the total amount of power being utilized from all the smart meters connected to this particular distribution transformer. Then it calculates the difference between the power supplied and the power consumed. So here we get the extra power, which is generally considered in terms of line losses. In case of any power theft these line losses will be more than usual.

The server calculates the percentage of these losses from the total power supplied, if more than 5% then there is a doubt of power theft that needs to inspected and if the percent rises to 10 then there is a confirm power theft and the area is marked for physical inspection. The percent levels defined here are safe enough to avoid the confusion of I^2R

losses that occur in lines ahead of distribution transformer.

7. Results of prototype

The prototype made, was tested under small scale but practical conditions. The electronic equipment worked with perfect accuracy once they were well integrated and synchronized with each other. Practical voltage and current levels, that of utility were applied to the meter and the readings were obtained that were cross checked by some other techniques (few of which are mentioned above) and in the end percentage error of almost 1.23% was calculated. Smart Meter design fully supported the implementation of encryption, polling, data preservation and power theft calculation, which were the actual targets. The percentage error yielded can be further minimized by detailed research for commercial production. Actual network congestion can only be known once meter is put to use in real environment but the response time was short for individual meter. DSL internet connection was used for communication between distributed servers, the accuracy of data transfer was close to 100% due to inherited check and retransmission scheme of TCP (Transfer Control Protocols) on which HTTP (Hypertext Transfer Protocol) is based.

8. Conclusion

In countries where power theft is a common issue and each year utility has to suffer heavy line losses, the implementation of this concept will be indeed revolutionary. This technology will not only prove to be a milestone in reduction of line losses (including power theft) but will bring up the automation in power distribution system and reduce the human errors. It can help reduce shutdowns due to overloading of phases especially in summer. Its implementation on commercial scale will eliminate the concept of typical meter reader and will set up a better accountability procedure also cutting down the cost. Database systems will maintain the records, while automatic billing will benefit both the consumer and the utility. Industrial standard data preservation will ensures error free billing and collection of data for auto generation of annual/daily reports on energy production and consumption. It can also help estimate the future demand using current trends so government/utility can prepare for upcoming challenges. Thus a more secure and comprehensive system can be implemented to give fruitful results.

References

1. Gerwen, R.V., Jaarsma, S., Wilhite, K.R.: *Smart Metering.* Leonard-Energy Org., 2006.

2. Mahmood A., Aamir M., Anis M.I.: *Design and implementation of AMR smart grid system.* In: Proceedings of IEEE Electric Power and Energy Conference EPEC'2008, October 6-7, 2008, Vancouver-Canada; p.1-6.

3. Haney, A.B., Jamasb, T., Pollitt, M.G.: *Smart Metering and Electricity Demand*: *Technology, Economics and International Experience*. University of Cambridge, Infraday .TU-berlin, 2009.

4. McLaAughlin, S., Podkuiko, D., McDaniel, P.: *Energy theft in the advanced metering infrastructure.* In: Critical Information Infrastructures Security, 6027 (2010), Springer Berlin Heidelberg 2010, p.176-187.

5. Bennett C., Wicker S.B.: *Decreased Time Delay and Security Enhancement Recommendations for AMI Smart Meter Networks*. In: Proceedings of IEEE Conference on Innovation Smart Grid Technologies (ISGT) NIST '2010, Jan 19-21, 2010, Washington D.C, p.1-6.

6. McDanniel, P., McLaughlin: *Security and Privacy challenges in the smart grid.* In: Security & Privacy IEEE, VII (2009), No.3, May-June 2009, p.75-77.

7. Deconinck G., Decroix B., Leuven K.U.: *Smart Metering Tariff Schemes Combined with Distributed Energy Resources.* In: Proceedings of IEEE 4th International Conference on Critical Infrastructures CRIS' 2009, March 27-April 30, 2009, Virginia, p.1-8.

8. Weynand, G.: *Energy sector assessment for USAID/Pakistan* United States Agency For International Development, America, 2007.

9. Luan S., Teng J.H., Chan S.Y., Hwang L.C.: *Development of a smart power meter for AMI based on ZigBee communication* In: IEEE International Conference on Power Electronics and Drive Systems PEDS'2009, Nov 2-5, 2009, Taipei-Taiwan, p.661-665.

10. *Announcing the Advanced Encryption Standard (AES)* Federal Information Processing Standards Publication197,2001.
http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf