ISSN:0975-9646

NTP Based Smart Energy Meter

Chetana Dapse

Information Technology, MET, BKC, IOE, Nashik, India.
Savitribai Phule University of Pune.

***Abstract*— The fast advancing mobile communication technology and the decrease in costs make it possible to incorporate mobile technology into MSEB automation systems. The traditional approach for collection of energy consumption data is that the representatives of MSEB monthly comes and visit every residential and corporate and manually reads the consumption data from the meter. The data is recorded on a piece of paper along with a snap shot of the meter and finally submitted to the local MSEB office. There after the officials reads the snap shot and readings of the meter and then feed it to the local software for bill generation. Finally the bills are dispatched. Human resources are wasted and many other problems do occur.In this propose system, energy meter collects the consumed energy reading from residential and corporate zones, encrypt it and send it directly to the central Server. Every Energy consumption meter will be attached to a microcontroller unit that will scan the meter reading after every one month, encrypt the data to be send and then it will transmitted wirelessly to the local server along with the meter number. This data will be processed by the server and generates the bill automatically. Once the bill is generated an SMS alert will be send to the customer's mobile number and it will be also mailed on the customer's registered email ID.**

***Keywords*— (NTP)Network Time Protocol, (SGM)Smart Grid Meter, (TVES)Time Varying Encryption System, (SEM)Smart Energy Meter.**

I. INTRODUCTION

Saving energy, dropping costs, and growing consistency are return of smart grid Energy Meter, but only if the security of the system is definite. . To make sure correct operation, infrastructure must be secure. A novel crypto graphic mechanism appropriate for smart grid environments, namely the time-varying encryption organization, is proposed here. In the Ethernet network, the millisecond level time synchronization among client clocks and the server clock can be reached if they follow the Network Time Protocol (NTP). The time tags and some internal parameters for time synchronization are used for generating the encrypted ciphertext at the broadcast port. The same sets of time tags and internal parameters are used for recovering the information at the receiving port. Since the time tags and parameters are updated every second, the hacker move toward of code-breaking with brute force will fail. In this project there is observe the problem of synchronizing the time-of-day clock in one node of an computerization network system with a reference clock. The accent of this is on switched, highly loaded networks, where random delays introduce excessive management noise. PC clocks are accurate sufficient when connected within a network, but a new condition is for them to be synchronized, which means that they should show the same time at the same instant. The most well-known time-synchronization method is the network time protocol projected by Mills and Internet engineering task force group. A complete solution of the high-precision time-synchronization problem must diminish the randomness associated with the RTOS. The methods discussed in this article can help establish the frequency and time offset of a local time-of-day clock. The next challenge is to create a local time-of-day clock and relate the synchronization information to it.

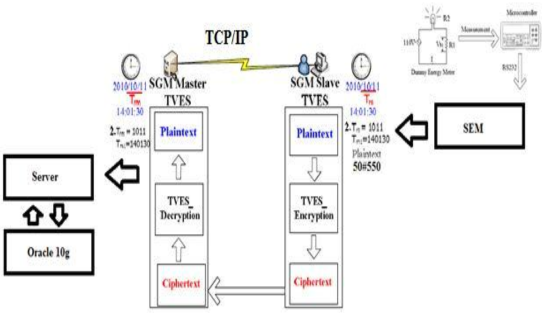
The quickly advancing mobile communication data and the diminish in costs make it possible to include mobile technology into MSEB mechanization systems. We suggest a system that collects the intense energy from residential and group zones and launch it directly to the central Server. The traditional approach for collection of energy consumption data is that the representatives of MSEB monthly comes and visit every housing and commercial and manually reads the utilization data from the meter. The data is recorded on a piece of paper along with a snap shot of the meter and lastly submitted to the local MSEB office. There after the officials reads the snap shot and readings of the meter and then feed it to the local software for bill calculations. Finally the bills are dispatched. We as a consumer then make the payment for the received bill. Such a hectic process is this. Man made mistakes can be countless. Human resources wasted and many other problems do take place. We at last consideration of building a system that will do the above process mechanically. Every Energy using up meter will be fond of to a microcontroller unit that will scan the meter reading after every one month. The meter reading will transmitted wirelessly to the local server along with the meter number. This data will be processed by the server and generates the bill repeatedly. Once the bill is generated an SMS attentive will be send to the owner's mobile number and it will be also mailed on the owners registered email ID.

II. PROBLEM STATEMENT

Network Time Protocol Based Time-Varying Encryption System for Smart Grid Meter

Economy energy, dropping expenses, and mounting consistency are recompense of smart grid, but only if the safety of the classification is assured. To make sure exact function, interactions must be protected. A novel crypto graphic mechanism suitable for smart grid environments, specifically the time-varying encryption system, is projected in this paper. In the Ethernet network, the millisecond level time harmonization among client clocks and the server clock can be reached if they follow the Network Time Protocol (NTP).

III. PROJECT METHODOLOGY



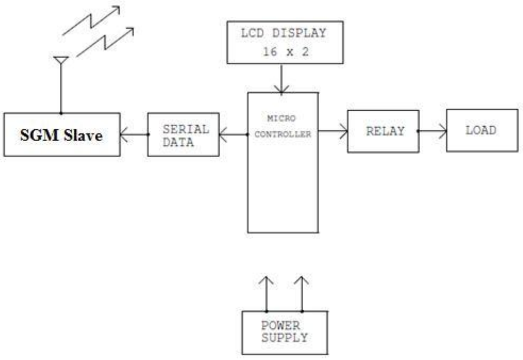
The above figure shows the proposed architecture. The architecture basically contains the following modules

1) *Smart Energy Meter*
2) *SGM Slave*
3) *SGM Master*
4) *Server*

A. *Smart Energy Meter*

The SEM is basically a hardware unit that demonstrates the working of the Energy meter. It is made up of electronic components which are controlled by a microcontroller unit. The SEM monitors the consumption and accordingly generates a unit based counter that represents the Meter reading. On request the Microcontroller serializes the data in a serial fashion to the SGM Slave. The data is send in a packet like structure that contains the user consumer number and the current consumption reading.

BLOCK DIAGRAM



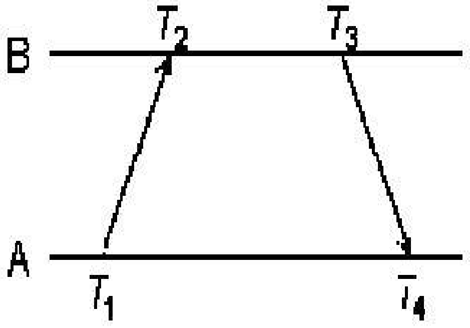
B. *SGM Slave*

SGM means Smart Grid Meter. This is a software based program that is connected to the SEM serially using RS232. The software is purely in java that collects the packet send by the SEM. The SGM applies the NTP protocol to secure the packets. The encrypted data is further send to the SGM Master using TCP/IP.

C. *NTP*

The NTP provides sufficient synchronization capabilities for many current factory automation applications. In a common distributed network environment, synchronized network time is a fundamental part of ensuring efficiency, reliability, security, and quality in a diverse array of applications. The NTP protocols basically encrypt the data based on the TVES system.

To better understand the issues, consider the ultimate case where the server and client implement clocks that can be read with exquisite accuracy. The object is to measure the time offset of a server (B) relative to the client (A).



NTP obtains time and compensates the explanatory drawing.

As shown in Figure, the NTP on-wire specification uses what is called here the reference timestamps *T*1, *T*2, *T*3and *T*4. *T*1 is the time of the request packet transmission. *T*2 is the time of the request packet reception. *T*3 is the time of the response packet transmission. *T*4 is the time of the response packet reception. *T*1 and *T*4 are struck by peer A from its clock, while *T*2 and *T*3 are struck by peer B from its clock. The object of the protocol is to determine the time offset of B relative to A and the roundtrip delay A-B-A:

$$\textbf{Offset} = [(T2\text{-}T1) + (T3\text{-}T4)] / 2 \quad (1)$$

$$\textbf{Delay} = (T4\text{-}T1)\text{-}(T3\text{-}T2) \quad (2)$$

After acquisition of the Offset, the client (A) Clock is added to the compensation. This allows the server and client clock times to move ahead simultaneously.

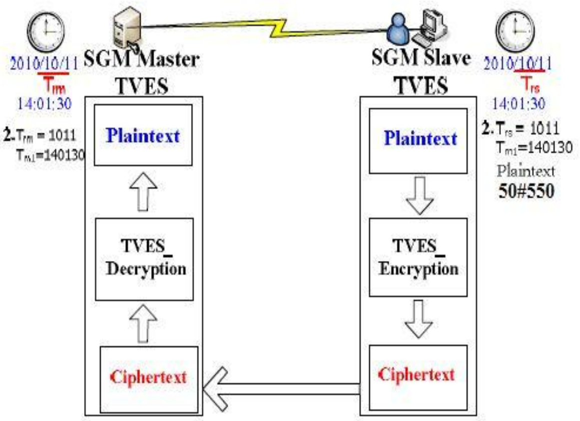
D. *TVES (TIME VARYING ENCRYPTION SYSTEM)*

The TVES Modules play an important role of securing the transmission data. The TVES on receiving data from the SEM, read the time and applies NTP here to synchronize the time factor between the SGM Master and Slave. The time factor has a tolerance of T^10.

In the below given figure the Tm1 is the key time that is used for encryption. The reading data is encrypted and further send to the TCP/IP Network for sending it to the SGM Master. The SMG Master on receiving read the data and synchronizes I clock using NTP by the same tolerance of T^10. A series of time will be created and the SGM Master uses the series for decrypting the data.

E. *Server*

The server reads the data from the SGM Master and updates the data in the database. After successful updating the server send SMS to the user notifying that the bill has been generated.

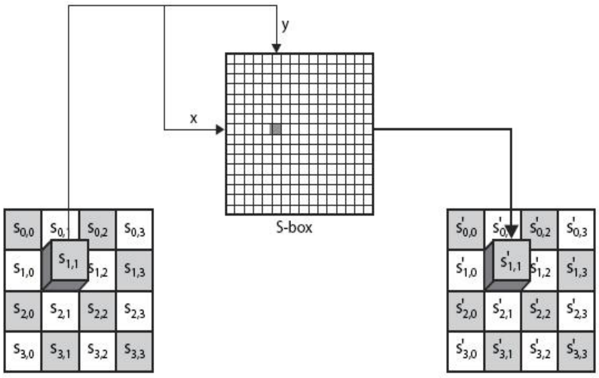


IV. AES ALGORITHM

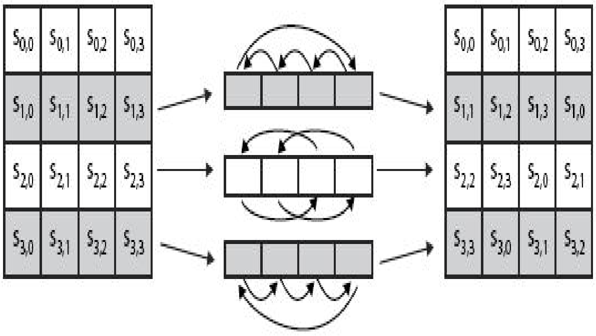
AES is an iterated symmetric block cipher, which means that:AES works by repeating the same defined step multiple times. AES is a secret key encryption algorithm. AES operate on a fixed number of bytes

AES as well as most encryption algorithms is reversible. This resources that almost the identical stepladder are performed to entire both encryption and decryption in invalidate order. The AES algorithm operates on bytes, which makes it simpler to realize and clarify. This key is delayed into being sub key, a sub keys for each procedure around. This progression is called KEY EXPANSION, which is described at the end of this manuscript. As mentioned previous to AES is an iterated block cipher. All that funds is that the same operations are performed many times on a fixed number of bytes. These operations can easily be out of order losing to the subsequent functions:

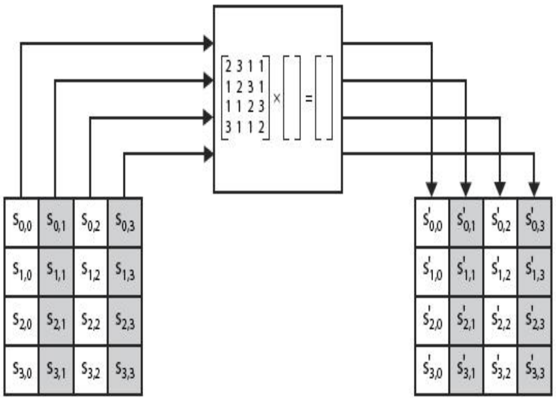
1.BYTE SUB


y
x
S-box
$s_{0,0}$ $s_{0,1}$ $s_{0,2}$ $s_{0,3}$
$s_{1,0}$ $s_{1,1}$ $s_{1,2}$ $s_{1,3}$
$s_{2,0}$ $s_{2,1}$ $s_{2,2}$ $s_{2,3}$
$s_{3,0}$ $s_{3,1}$ $s_{3,2}$ $s_{3,3}$
$s'_{0,0}$ $s'_{0,1}$ $s'_{0,2}$ $s'_{0,3}$
$s'_{1,0}$ $s'_{1,1}$ $s'_{1,2}$ $s'_{1,3}$
$s'_{2,0}$ $s'_{2,1}$ $s'_{2,2}$ $s'_{2,3}$
$s'_{3,0}$ $s'_{3,1}$ $s'_{3,2}$ $s'_{3,3}$

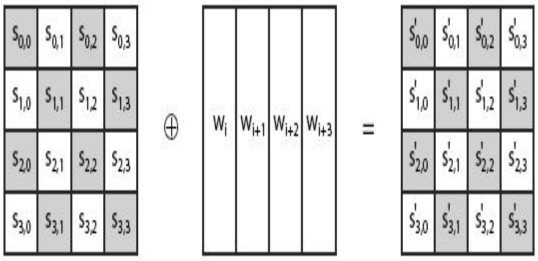
2.SHIFT ROW


$s_{0,0}$ $s_{0,1}$ $s_{0,2}$ $s_{0,3}$
$s_{1,0}$ $s_{1,1}$ $s_{1,2}$ $s_{1,3}$
$s_{2,0}$ $s_{2,1}$ $s_{2,2}$ $s_{2,3}$
$s_{3,0}$ $s_{3,1}$ $s_{3,2}$ $s_{3,3}$
$s_{0,0}$ $s_{0,1}$ $s_{0,2}$ $s_{0,3}$
$s_{1,1}$ $s_{1,2}$ $s_{1,3}$ $s_{1,0}$
$s_{2,2}$ $s_{2,3}$ $s_{2,0}$ $s_{2,1}$
$s_{3,3}$ $s_{3,0}$ $s_{3,1}$ $s_{3,2}$

3)MIX COLUMN:


2 3 1 1
1 2 3 1
1 1 2 3
3 1 1 2
x
=
$s_{0,0}$ $s_{0,1}$ $s_{0,2}$ $s_{0,3}$
$s_{1,0}$ $s_{1,1}$ $s_{1,2}$ $s_{1,3}$
$s_{2,0}$ $s_{2,1}$ $s_{2,2}$ $s_{2,3}$
$s_{3,0}$ $s_{3,1}$ $s_{3,2}$ $s_{3,3}$
$s'_{0,0}$ $s'_{0,1}$ $s'_{0,2}$ $s'_{0,3}$
$s'_{1,0}$ $s'_{1,1}$ $s'_{1,2}$ $s'_{1,3}$
$s'_{2,0}$ $s'_{2,1}$ $s'_{2,2}$ $s'_{2,3}$
$s'_{3,0}$ $s'_{3,1}$ $s'_{3,2}$ $s'_{3,3}$

4.ADD ROUND KEY:


$s_{0,0}$ $s_{0,1}$ $s_{0,2}$ $s_{0,3}$
$s_{1,0}$ $s_{1,1}$ $s_{1,2}$ $s_{1,3}$
$s_{2,0}$ $s_{2,1}$ $s_{2,2}$ $s_{2,3}$
$s_{3,0}$ $s_{3,1}$ $s_{3,2}$ $s_{3,3}$
⊕
W_i W_{i+1} W_{i+2} W_{i+3}
=
$s'_{0,0}$ $s'_{0,1}$ $s'_{0,2}$ $s'_{0,3}$
$s'_{1,0}$ $s'_{1,1}$ $s'_{1,2}$ $s'_{1,3}$
$s'_{2,0}$ $s'_{2,1}$ $s'_{2,2}$ $s'_{2,3}$
$s'_{3,0}$ $s'_{3,1}$ $s'_{3,2}$ $s'_{3,3}$

An iteration of the above steps is called a round. The amount of rounds of the algorithm depends on the key size.

The only exception being that in the last round the **Mix Column** step is not performed, to make the algorithm reversible during decryption.

V. Applications

1. E-MANUFACTURING
2. ELECTRONIC BILL PAYMENT SERVICES
3. FINANCIAL BANKING SERVICES

VI. Conclusion

In this paper, time tags are used as the parameters of the encryption method. The simplest Caesar cipher is adopted, since its simple computations are suitable for real-time applications. The encryption keys are time varying, and are updated every second. According to our decryption condition analysis, the probability of success of hacker attacks is very low. To demonstrate our ideas, the NTP and Electricity Consumption Meter are integrated together as the smart grid meter. Its results show that the safety of data transmission is improved greatly.

References

[1] International Telecommunication Union, *ITU-T G.810 Definition and terminology for synchronization networks*, 1996.

[2] M. A. Lombardi, *Operator's Manual: Frequency Measurement and Analysis Syste*, 1996 .

[3] International Telecommunication Union, *Handbook: Selection and Use of Pricise Frequency and Time System*, 1997.

[4] IEEE International Standard, *IEEE Standard 1588TM Precision clock synchronization protocol for networked measurement and control systems*, 2004.

[5] K. Correll, N. Barendt and M. Branicky, *Design Considerations for Software Only Implementations of the IEEE 1588 Precision Time Protocol*, VXI Technology, 2005.

[6]Sourceforge.(2007,Jun.).http://sourceforge.net/project/showfiles.php ?group _id=139814