Security Enhancement In Secure & Scalable Smart Grid

Mohit[*]*, NK Swarnkar*[**]

Abstract

Development of Sensors and Meters are increasingly rapidly toward a vision of smart grid to collect a secure and scalable data because data collection in today's era is a challenging task. In this paper we develop a data collection technique focusing on the security of smart grid. Using a MATLAB simulation and algorithm we develop a data collector and power operator. In this paper we are using cryptography with variable length mixed key generation. And for connecting data operator and power operator we are using a technique TCP/IP.

Keywords: Data collector, Time minimization, Cryptography, Power operator.

Introduction

In today's electrical era a smart gird is an important part. In smart grid there are number of electrical sensors and meters are connected for securing the smart grid [1]. In smart grid technique most challenging part is to collect data from every point of grid, data should be collected in a secure and efficient manner. To make it scalable, a hierarchical data collection framework is usually adopted for example, in advanced metering infrastructure [2]. So there is one power operator (PO) connected to multiple Data collectors (DCs) and data collectors are connected to multiple metering devices (MDs). One data collector can connect to multiple MDs and multiple MDs can connect to multiple DCs. Power operator do not have to maintain an expensive connection with each smart meter. The data or message should be deliver fast as possible to maintain security and to prevent from information leak.

There are many methods for data collection like Supervisory Control And Data Acquisition (SCADA). This system already collects data from different nodes and different sensors. Many changes in smart grid pose a new challenge for enhancing security and for increasing efficiency. Application of smart grid technique includes the monitoring of distributed energy resources, transmission, distribution, overhead lines, and state of charge monitoring and collection of information.

In this paper, we develop a protocol that collects data and enhances the security in smart grid in secure, scalable and efficient manner. We have used cryptography method with variable length mixed key generation algorithm for enhancing security with the help of TCP/IP. Fig 1 presents the data collection structure. In this paper PO is power operator that generate private key to and then keys are send it to DCs (Data Collector).

Here MDs are metering device that collect the data from smart grid. From figure we can say that each MD is connected to at least one DCs, but each DCs can connect to multiple MDs. In this we can say that PO is directly connected to each DCs.

[*]M.Tech Scholar, Department of Electrical Engineering, GVSET, Suresh Gyan Vihar University, Jaipur, India.
[**]Professor, Department of Electrical Engineering, GVSET, Suresh Gyan Vihar University, Jaipur, India.
Correspondence to: Mr. Nagendra Kumar Swarnkar, Department of Electrical Engineering, GVSET, Suresh Gyan Vihar University, Jaipur, India. ***E-mail Id:*** swarnkar.n123@gmail.com

© ADR Journals 2016. All Rights Reserved.

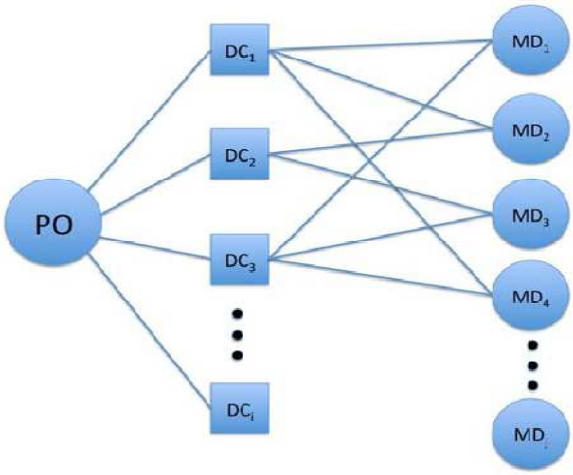

Fig 1.Hierarchical Data collection structure [1]

The PO and DCs are more powerful than MDs. The data is synchronized to PO with the help of DC. Due to massive number of MDs and their dispersion over a large area, it may not be appropriate to assume DCs can be completely trusted. In addition, one of the seven actors identified be the National Institute of Standards Technology (NIST) in the smart grid framework [3] is third service provider, which are to furnish value-added services. We assume honest-but-curious modes of DCs. Thus, the data collection tasks may be outsourced to third service provider [4]. Besides, the benefits of cloud computing [5] may be accrued for storage and processing of the data collected.

In other application [6], the connection between DCs and MDs are dynamic. So MDs are desired to encrypt their data in a way that DCs cannot access the data. In other we can say that MDs should encrypt there data through a private key to keep its data private from DCs. Due to limitation in computation capabilities, our encryption algorithm should be efficient.

In this paper we have proposed that

1. Under a simulation we proposed a secure and efficient data collection scheme in smart grid.
2. After this we develop a algoritm of power operator and data collector with cryptography with variable mixed key generation.
3. We have coupled POs and DCs with the help TCP/ IP (Transmission Control Protocol/ Internet Protocol).

The rest of this paper is organized as follows. Section II describes the related work on smart grid data collection scheme. We provide the system and protocol overview in section III. The result are analyzed in section IV and concluded in section V.

Related Work

There are many techniques for data collection there is tree based smart grid data collection technique, in this DC is responsible for collecting data from multiple MDs, but few can communicate with DC, other have to depend on other devices for relay the data. So there is communication protocol so that the data reported by each device is protected against honest-but-curious data collector and devices [7] to reduce the time they formulate an integer linear programming problem.

Data integrity and data collection have been studied on internet. However, most scheme, such as The Transport Layer Security (TLS) [8], assume the device has abundant memory and computation power to perform cryptography method. In smart grid technique there is a massive issue regarding to slow CPU and ongoing security protocol are thus not suitable for data collection [9].

Distributed network protocol (DNS) [10] is a standard communication protocol used in SCADA, the data collection subsystem of power grid. SCADA is within the security perimeter of the operator. A more recent standard for substation automation is IP based the International Electro-technical Commission (IEC) 61850 [11]. Yet IEC also is designed without security enhancement [12]. So the new security protocol for data collection and command delivery of smart grid needs to be developed.

Our proposed approach comprises security aspect of the smart grid data collection as well as the time minimization.

System and Protocol Overview

Operations and their Requirements

As mentioned our MDs send data to DCs, and PD generate private keys. Our communication architecture supports MDs to report data and PO to deliver commands in a timely and secure manner. So Table 1 describes each operation. In operation 1 (Op 1) firstly we open Simulink model of smart grid that was built in MATLAB. Running the model gives us the data of smart grid. This smart grid is an interconnected system of thermal and solar PV system. The data point in system are solar voltage, inverter voltage, inverter current, load voltage, load current, transmission voltage, and generating voltage. The data is collected from 0-200s. In operation 1 (Op 1) DC allows MDs to add, 2-4 MDs to the system.In operation 2 (Op 2) DCs contact to PO to generate private or public key. PO is self-independent architecture because it controls the whole system. In operation 3 (Op 3) PO sends private key to DCs. These keys can be read by only DCs, that means after this DC allows us to add metering device, remove metering device, encrypt data and decrypt data.In operation 1 (Op 1) when we give initial metering devices, according to our algorithm, our initial value is 0, when we give between 2 to 4 metering device, then it becomes 1. According to our algorithm, a private key is generated for each MDs that is added. Every MDs knows its private key.

	Operation	Security requirements
Op1	Open simulation of smart grid, PO and DCs, and adding MDs	Data should be authenticated and should be read only by PO
Op2	DCs contact to PO to generate Private Key	Same as Op1
Op3	PO send private keys to DCs	Same as Op1
Op4	DCs can add and remove MDs and data can be encrypted and decrypted.	The command should be authenticated properly.

Table 1.System operations and their Requirements

We develop a protocol to be secure from attacks like eavesdropping, impersonation, and message tampering, etc. We develop three types of insider in protocol like PO, DCs, and MDs. They all have their public and private key. Private Key and public key can be identified by authenticator (who can operate DC). If private key can be stolen easily than our protocol does not work at all. Then the system requires another form of authentication such as bio-metric and token based.

We should assume the PO is always trustworthy because it controls the whole system and it decides how to use the data collected. The DC, on the other hand, can read the data and can share to others if they could. As metering devices are located in the smart grid simulation, if they are in the same physical environment as PO, then the chance of leaking of private keys increases higher. When an attacker gets the private key of certain MD, it can report fake data to the PO on behalf of MD.

 ISSN: 2456-1401

System Parameters

Before any communication PO, DCs and MDs are equipped with a set of system parameters.

Long Term Keys

We assume that there are key server that generate a set of public and private key for each insider protocol. The public and private key are configured into a DC and MD before. PO on other hand, it keeps its own key pair and also remember the public and private keys of DCs and MDs. Therefore, our system is secure from attackers.

TCP/IP

We adopt the TCP/IP key exchange mechanism to develop shared key between two parties. It is the communication language or protocol of the internet. The internet protocol standard dictates the logistic of packets sent over networks; it tell packets where to go and how to get there. The transmission control protocol is responsible for ensuring the reliable transmission of data across internet-connected network. In this paper TCP/IP is used for connection between PO and DC. We have also used American Standard Code for Information Interchange (ASCII).

Cryptography

It is a method of storing and transmitting data in a particular form so that authenticate person can read or write the data. To prevent the data from third party or attacker's cryptography is usually used. PO has the cryptography algorithm and function of cryptography are installed in DC. In this paper we have used Variable Length Mixed Key Generation Cryptography.

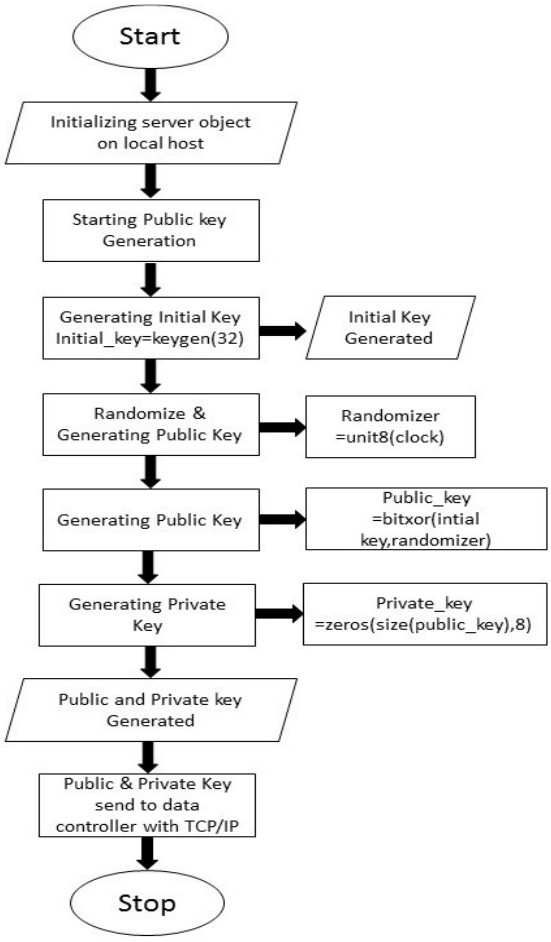

Fig 2.Flow Diagram of Power Operator Algorithm

Fig 2 is the flow chart of Power Operator algorithm. In this algorithm first PO initializes server object on local host thatmeans PO checks the local IP address and port number of object. After this PO starts the public key generation process. For public key generation first PO has to generate initial key and randomizer key. Randomizer keeps the PO operation in real time. So *publickey generation=bitxor (initial key, randomizer*). After generation of public key PO generate the private key. So *private key=zeros (size (public key), 8)*. After this PO send the public and private key to data controller.

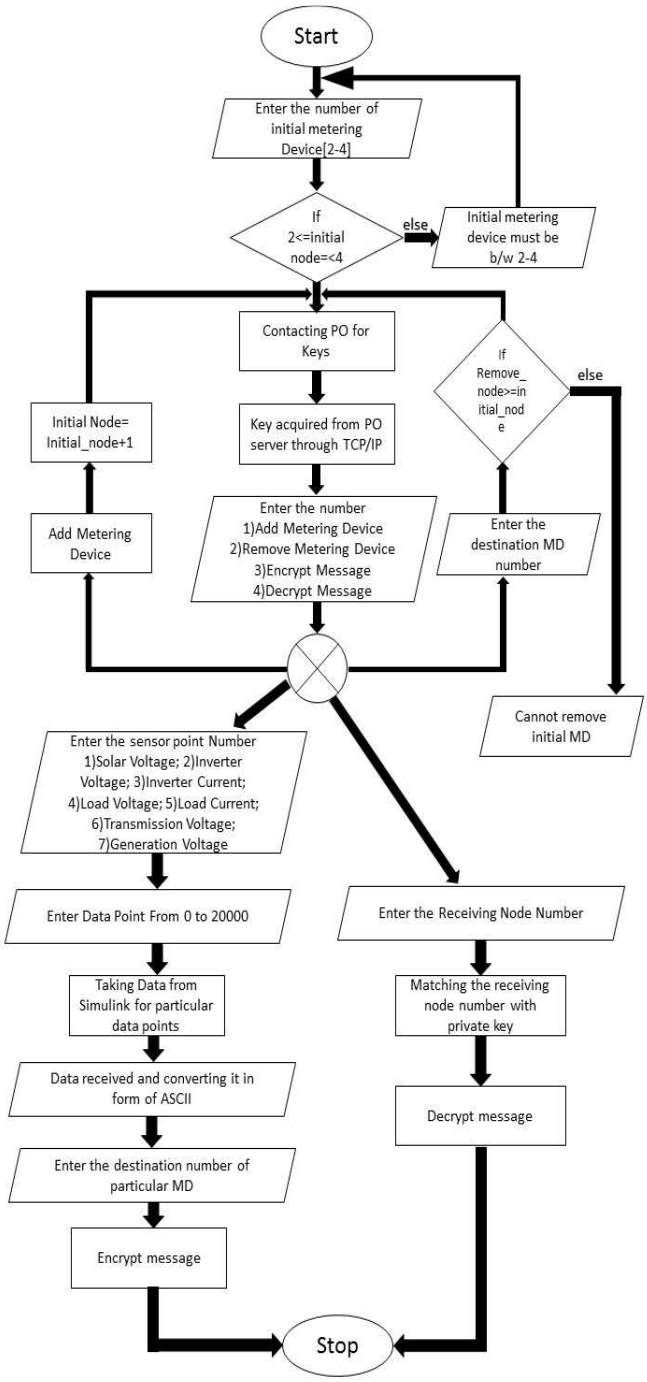

Fig 3.Flow diagram of Data controller

Fig 3 shows the flow diagram of DC. Firstly we ask user to enter the number of metering device. The number should be between 2 to 4. Afterword's DC contact PO to generate public and private key for each MDs. From DC we can add and remove MD. We can encrypt

 ISSN: 2456-1401

message and we can decrypt message. In adding metering device we can add another metering device in system. After adding new MD, DC contact to PO for generating public and private key for new MD. We can remove MD. For this we have to tell DC to which number of MD is to be removed. After this DC again contacts PO for generation of public and private key. For this DC we can take data from our simulation. Our simulation has seven sensor points i.e. solar voltage, inverter voltage, inverter current, load voltage, load current, transmission voltage, and generation voltage. These data can be taken over several time steps between 0-200s. The data came from simulation then converted into ASCII (American Standard Code for Information Interchange). Thus ASCII convert data to encrypted data. Then encrypted data can be seen by only authenticated person. To decrypt the particular message or data, firstly we have to give the receiving node number that the data which we have to decrypt. Then PO match the receiving number to public and private key, then PO decrypt the message.

Our simulation process in shown in Fig 4. The generation is made up of solar PV system and thermal power plant.

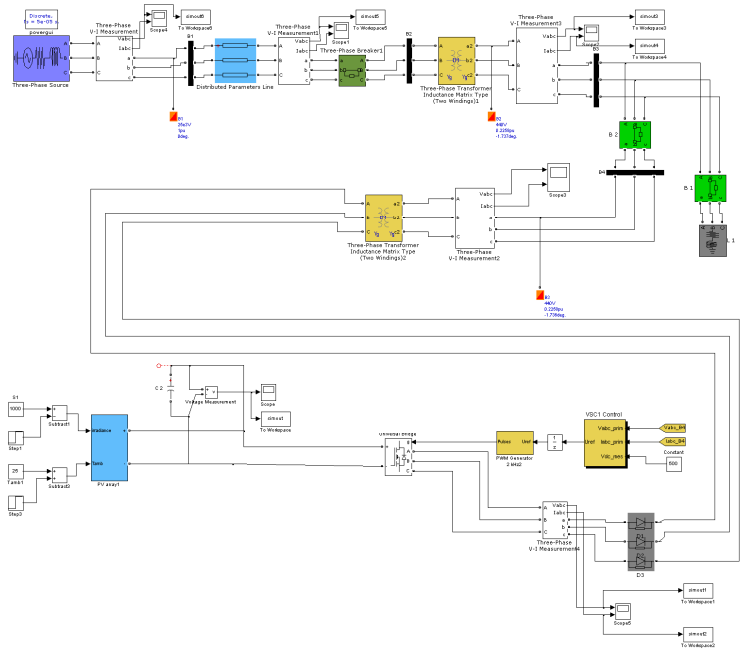

Fig 4.Simulation diagram

Result

There are some result from simulation problem

	Generation		Load (Kw)
	Voltage	Current	
Thermal	20,700 V	8.3 A	5Kw
Solar After Inversion	86 V	2.6 A	

Table 2.Inputs and Outputs of Simulation

This is the result from our simulation model. In this interconnecting thermal and solar system. In this system solar is assumed backup system. When our system fail then solar system works. Thus our simulation is working well and efficiently and giving data to PO and DC.

There are results from PO

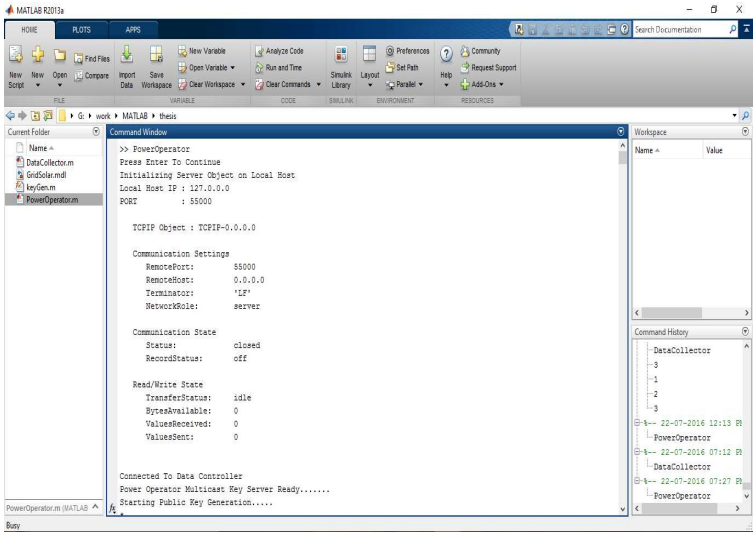

Fig 8.PO generating Public & Private Key

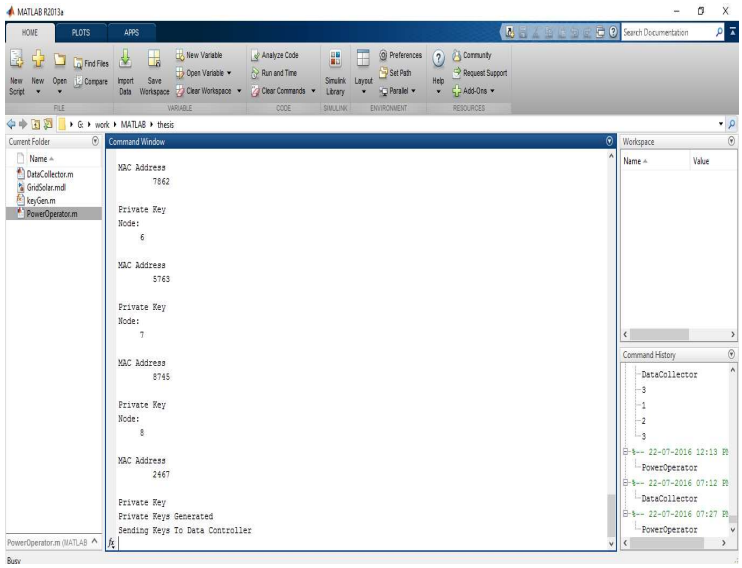

Fig 9.Public & private key send to DC

Here there are some result from DC. After key acquired form PO.

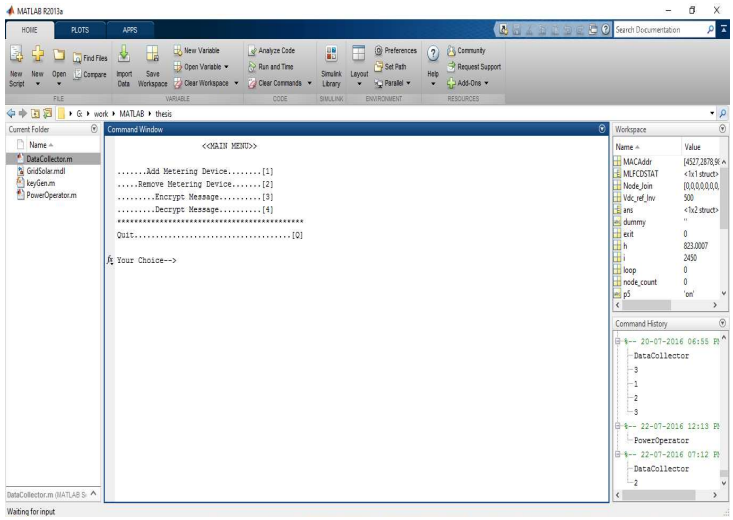

Fig 10.DC result

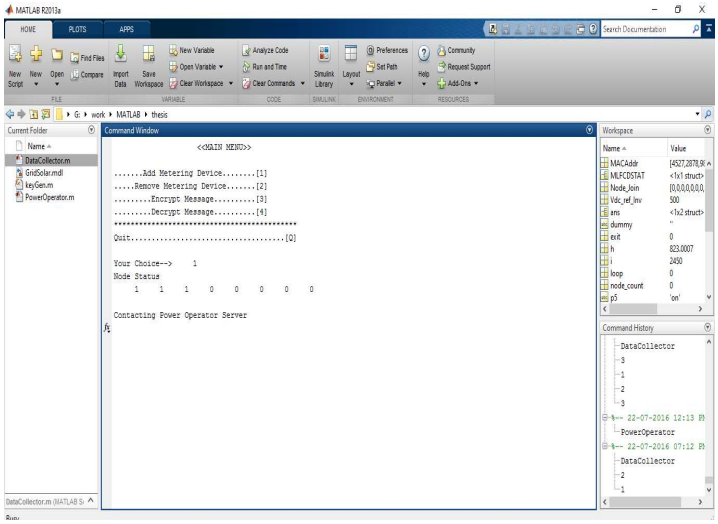

Fig 11.Adding new MD

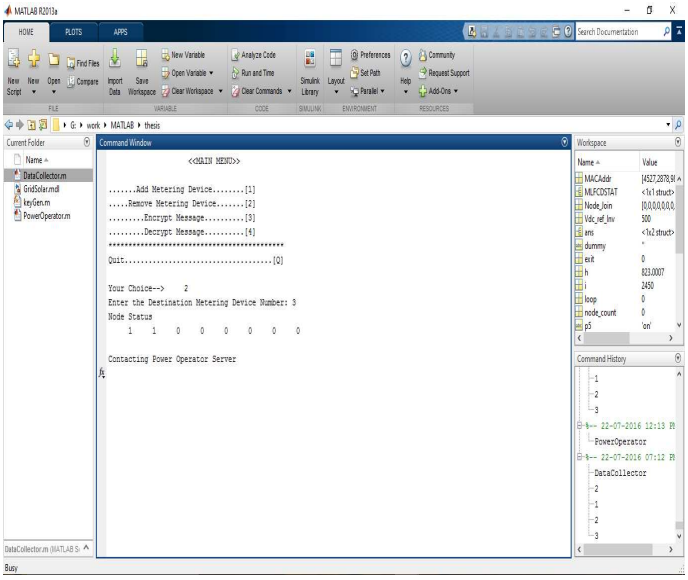

Fig 12.Removing exiting MD

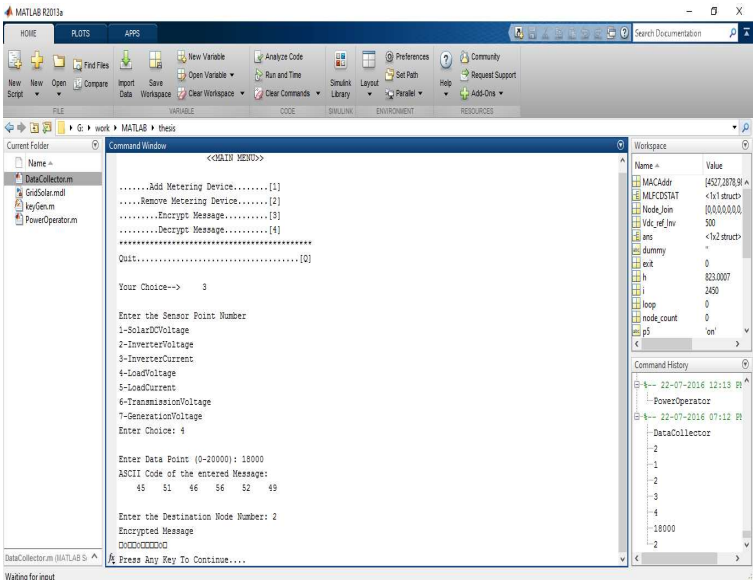

Fig 13.Encrypt Message

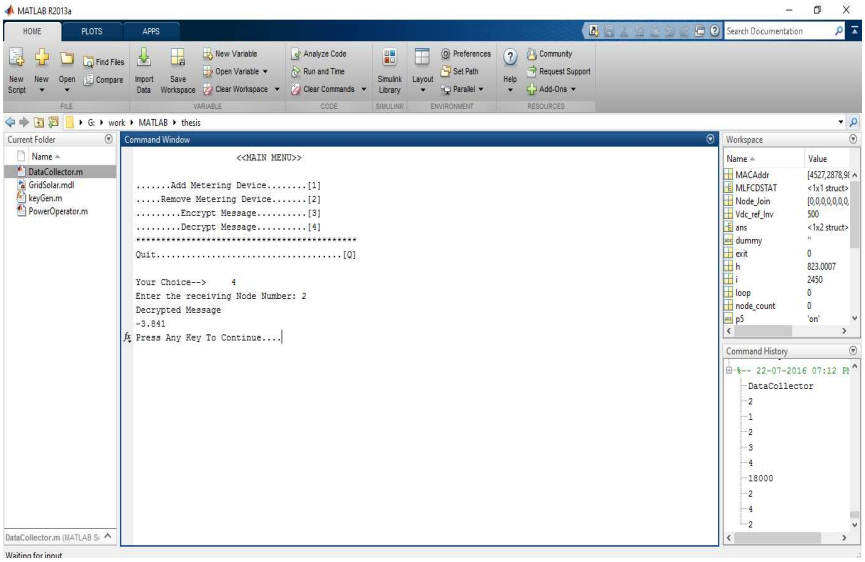

Fig 14.Decrypt message

These are the result from DC. In DC we have given four option that are adding MD, removing MD, encrypt message and decrypt message. In adding MD, DC add one initial node and then contact to PO for generating public and private key for that MD. In removing MD, DC ask for number of MD which have to remove. We can encrypt and decrypt the message came from simulation problem.

Conclusion

In this paper, we have developed a secure and scalable smart grid with security enhancement on real time minimization. We develop an efficient protocol to collect data from MDs or sensor point that are on simulation. We have developed PO and DC algorithm. Our simulation was conducted on real time minimization that conduct our algorithm well and efficiently. In future we can develop our protocol to bemore efficient by enhancing security by mobile computing security. In this protocol we can add security by wireless methods. In this system we can add password system for enhancing more security. PO and DC can only be operated when authenticator gives password to system. In this one MD can store one data point but in future one MD can store at least two or more data point.

References

[1]. Suleyman Uludag, King-Shan Lui, Wenyu Ren,"Secure and scalable data controller with time minimization in the smart grid," in IEEE 2015 .

[2]. N.Kayastha, D. Niyato, E. Hossain, and Z. Han,"Smart grid sensors data collection, communication and networking: A tutorian," wireless commun. Mobile Comput., Vol. 14, no. 11, pp. 1055-1087, 2012

[3]. NIST framework and roadmap for smart grid interoperability standards, release 3.0, smart grid interoperability panel (SGIP), NIST standards 1108R3, oct. 2013

[4]. X. Fang, S. Misra, G. Xue, and D. Yang,"Managing smart grid information in the cloud: opportunities, model, and application," IEEE Netw., Vol. 26, no. 4, pp. 32-38, Jul./Aug. 2012.

[5]. S. Bera, S. Misra, and J. Rodrigues,"Cloud computing application for smart grid: A survey," IEEE Trans. Parallel Distrib. Syst., Vol. 26, No. 5, May 2015.

[6]. R. Tabassum, K. Nahrstedt, E. Rogers, and K.-S. Lui,"SCAPACH: Scalable possword-changing protocol for smart grid device authentication," in Proc. 22nd Int. Conf. Comput. Netw., Nassau, the Bahamas, 2013, pp. 1-5

[7]. H. Jin, S. Uludag, K.-S. Lui, and K. Nahrstedt, "Secure data collection in constained tree-based smart grid environments," *2014 IEEE Int. Conf. on Smart Grid Comm., pp.308-313, Nov. 2014.*

[8]. *The Transport Layer Security (TLS) Protocol Version 1.2,* RFC standard 5246, 2008.

[9]. Y.-J. Kim, V. Kolesnikov, and M. Thottan, "Resilient end-to-end message protection for large-scale cyber-physical system communication," in *Proc. IEEE 3rd Int. Conf. Smart Grid Commun. Tainan, Taiwan, 2012, pp. 193-198.*

[10]. *DNP3 Secure Authentication Version 5,* IEEE Standad 1815-2012, 2011.

[11]. *IEC Power Utility Automation, Technical Committee 57 (TC57),* IEC Standard 61850, 2003.

[12]. W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and Challenges," *Comput. Netw., vol. 57, no. 5, pp. 1344-1371, 2013.*