Available online at www.sciencedirect.com
ScienceDirect
Procedia Technology 21 (2015) 125 – 131
Procedia Technology

SMART GRID Technologies, August 6-8, 2015

Design of a Secure Architecture for Last Mile Communication in Smart Grid Systems

Divya M. Menon[a] *, N.Radhika[a]

[a] *Department of Computer Science and Engineering, Amrita Vishwa Vidyapeetham, Ettimadai, Coimbatore – 641112.*

Abstract

Ever increasing need of electricity has paved the need for Smart Grids. Smart Meters, digitalized networks and fault tolerant systems are the basic infrastructure which supports Smart Grid. Security in Smart Grid has become a major concern in the present scenario. In this paper we have proposed security architecture at the last mile distribution in Home Area Networks. A Secure communication architecture has been modeled which focuses on secure data transmission between the Smart Meters at home and Central Gateway at the utility centre. Hybrid Encryption algorithms and Digital Signature has been used to provide data integrity. The strength of the model has been verified with the help of an attacker and the model is found to resist attacks.The Encryption time and Decryption time of the cyptostack is lower when compared with other encryption algorithms.

Peer-review under responsibility of Amrita School of Engineering, Amrita Vishwa Vidyapeetham University

Keywords: Smart grid ; Smart Meters (SM) ; Digital Signature;

1. Introduction

Today's lifestyle in modern society is highly dependent on electricity. Increasing need of electricity has paved the way for Smart grid. Smart Grid is a solution to a more sustainable, efficient, flexible and reliable power system. Intelligent metering and monitoring of Communication network is what makes the Smart Grid smarter [1]. Fig. 1 shows the architecture of smart grid system. Smart Meter functions as sensors in Smart Grid[2] .These Smart Meters are capable of monitoring and controlling power consumption by end users [3].Users are able to obtain significant information including next month's electricity bill estimate ,amount of power consumed till date etc[4] .

*Corresponding author. Tel.:+ 91 9495880085.
E-mail address: divya@jecc.ac.in

Peer-review under responsibility of Amrita School of Engineering, Amrita Vishwa Vidyapeetham University
doi:10.1016/j.protcy.2015.10.019

Smart Meters allows people to organize their daily routines based on the bill details and also provide information that helps them to lower their monthly power consumption bills[3].

Home Area Network contains a number of home appliances ranging from microwave oven to washing machine. A secure duplex Machine to Machine (M2M) communication is needed between these home appliances and Smart Meter for information regarding power consumption and network monitoring [5]. IEEE 802.15.4 ZigBee is the best protocol used for Machine to Machine (M2M) communication within a home [6]. ZigBee has low power consumption when compared to its counterparts WiFi and has a communication range between ten to hundred metres [6].Smart Meter gathers the information from the smart appliances in the home and then conveys the residents information regarding usage of electricity. Smart Meters in Home Area Network are capable of signalling price changes and defective household equipments to the residents[1]. These Smart Meters in turn transmit the data to the Central Gateway at the utility centre. The proposed framework provides security for messages transmitted between Smart Meter and Central Gateway.

An important aspect of Smart Meter is the security of the information collected by Smart Meter. The data collected by the Smart Meter reveals a lot about the behavior of a family. Extracting household information will result in a lot of strategic issues since the data may be used by both good and bad people[7]. Figure1illustrates the Smart Grid scenario. Here we have a Central Gateway which collects information from different residential Customers. Smart Meter communication to base stations should enforce high security since the personal information of every house hold is vital. Significant concern regarding security of information in Smart Grid has been evolved in recent years[8].In this paper we have used a cryptographic stack which contains both symmetric and asymmetric algorithms to implement the proposed architecture. This paper proposes a Secure communication architecture between each Smart Meter in the Home Area Network and the Central gateway at the Utility Centre.

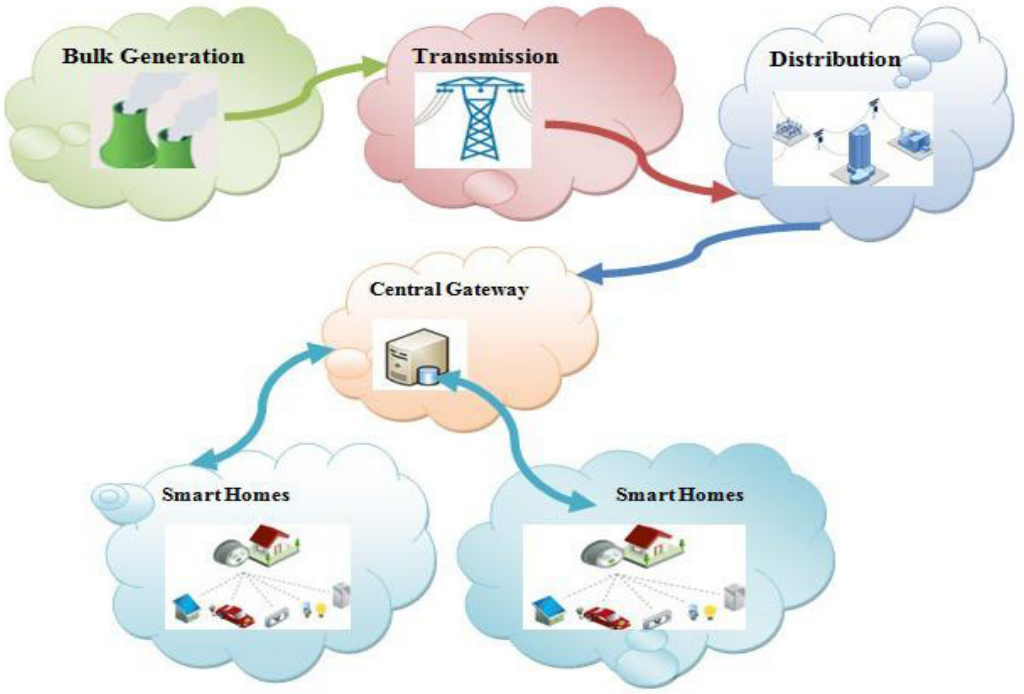

Fig. 1. Smart Grid System

2. Communication Architecture in Smart Grid

Smart Meters are electronic meters embedded with Micro Control Unit(MCU) which are capable of collecting information from household appliances. Smart Meters operate in a real time duplex mode without human

intervention. Smart Meter collects the information from household equipments and pass this to the Central Gateway in Home Area Network. A further important security consideration is the misuse of data from Smart Meters . Prediction of personal information can be done by hackers by analyzing the data obtained from Smart Meters [12]. The data from Smart Meters contain personal behaviour of every household which may be of interest to burglars and anti social elements. The Central Gateway at the utility centre will sent the predicted tariff to the Smart Meter on a daily basis [12]. So there is a two way communication between the Smart Meter and the Utility centre. We therefore need a secure architectural consideration for effective communication between Smart Meters and Central Gateway to protect this critical information.

Utility centre will broadcast the predicted electricity tariff to the Smart Meters in the Home Area Network. Every Smart Meter schedules its activities based on the predicted tariff. Here we propose a secure cipher suit for effective Communication between Central Gateway and Smart Meter. Fixed number of Smart Meters will be attached to the Central Gateway in a Home Area Network .Communication between Smart Meters and Central Gateway need to be synchronized so that every Smart Meter gets a fair chance to exchange information. Consider the scenario in which there are Five Smart Meters and each Smart Meter is attached to a Central Gateway. Central gateway collects information from Smart Meter which is attached to each household. Initially every Smart Meter register its unique ID with the Central Gateway using its Equipment number provided by the utility centre.Central gateway provides a positive acknowledgement for Smart Meters whose unique Id is registered in the Gateway Database. On receiving positive acknowledgement a secure communication is established. Situation may arise when one or more Smart Meters wishes to communicate with the Central Gateway. The problem of session allotment for each Smart Meter can be resolved with the help of a timestamp values .Each Smart meter is set with an initial timestamp value of zero which it periodically increments .Timestamp TS is calculated as a function of time and previous timestamp value. Smart Meters who wishes to communicate initially passes its timestamp value along with the request message.

The Central Gateway compares the timestamp values obtained from Smart Meters and responds with a positive acknowledgement to the Smart Meter having the lowest timestamp value. Primary approach on setting up a Home Area Network is to allocate time slot for each Smart Meter . Once a positive acknowledgement is received from the Central Gateway we need to establish a secure communication to transfer data from the Smart Meter. Fig. 2 shows the diagram of communication between smart meter and Gateway.

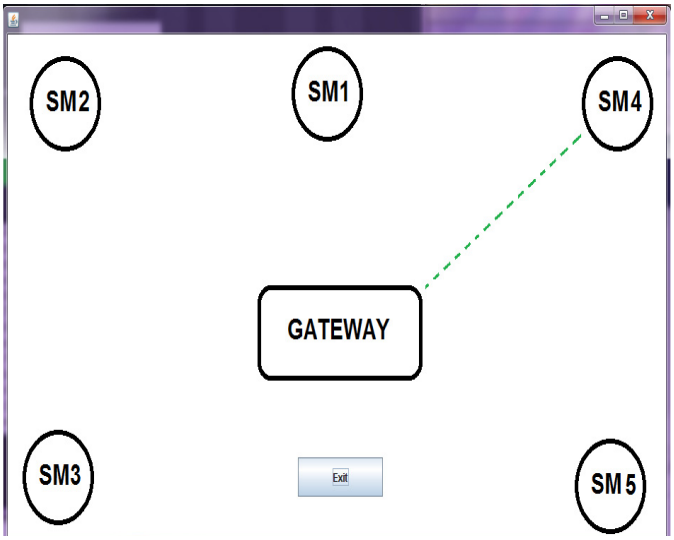

Fig. 2. Communication between Smart Meter and Gateway

3. Proposed Framework For Secure Communication Architecture

To develop a cryptographic stack, three algorithms have been used in this architecture model. Firstly, Blowfish algorithm by Bruce Schneieris used to encrypt the message. Blowfish algorithm is a 64 bit block cipher which has a key length of variable size ranging from 32 to 448 bits[9].Blowfish follows a fiestal network of 16 rounds[9]. Secondly MD5 algorithm is used to obtain a message digest[10].Finally RSA is used for Digital Signature Verification[11].RSA uses two keys public and private key for encryption and decryption process.

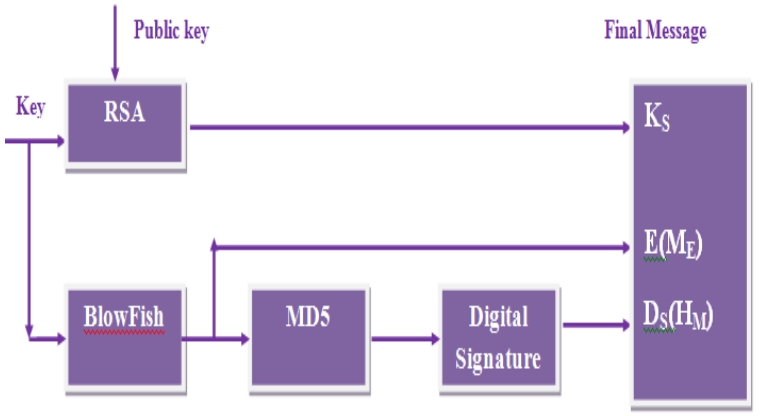

Fig. 3. Cipher Suit for Encryption

In this paper, Blowfish algorithm is used for faster encryption and for securing the key, asymmetric encryption with RSA is used. Symmetric Encryption consumes only less power and asymmetric encryption provides greater authentication for each Smart Meter. Combination of Blowfish with RSA has been used to benefit the advantages of both Symmetric and Asymmetric encryption. The objective of this paper is to establish a Secure communication architecture between each Smart Meter and the Central Gateway. A higher level of security in the communication architecture has been achieved by incorporating Digital Signature along with hybrid encryption. The design of a secure communication is made possible only with the help of an efficient encryption scheme. Implementation of an encryption scheme requires an important consideration ie. Trade off between energy constraints and the cryptographic algorithms [2].To deal with this we propose a cryptographic stack which contains symmetric and asymmetric encryption along with Digital Signature.Fig. 3 represents the cipher suit for Encryption.

4. Implementation

Initially, a secret key is used to encrypt the message using Blowfish Algorithm. The Secret Key of Blowfish is encrypted with RSA and transmitted along the message. To further enhance the strength of encryption, a one way hash function using MD5 is added to provide data integrity. Finally a RSA Digital Signature is generated for the message digest which will be verified at the receiver end. The final message transmitted from each Smart Meter contains a combination of Encrypted Message, Encrypted Key and a Digital signature .To further illustrate the procedure, the security model is implemented in Java using 5 Smart Meters and a Central Gateway. The Database is maintained by the Central Gateway. At the central gateway decryption using private key of RSA will generate the Blowfish Key which in turn can be used to decrypt the encrypted message. Receiver can verify the integrity of data using the RSA Signature Verification.

Procedure for Secure Encryption

1. Setup a connection between chosen Smart Meter and Central Gateway.
2. For all messages from Smart Meter do
3. Choose a Secret Key of variable length 32- 448 bits.
4. Initially apply RSA to encrypt the Secret Key ,KS
5. Apply Blowfish encryption to obtain cipher text for Message,M from Smart Meter,E(ME) represents the encrypted message .
6. Generate 512 bit Message Digest using MD5 algorithm for the Encrypted Message.
   HM = MD5(E(ME))
7. Apply RSA Digital Signature to HM to generate Digital Signature DS(HM).
8. For all message do
   Generate KS, E(ME) , DS(HM)
9. End for
10. Send CM = KS + E(ME) + DS(HM)
11. End for
12. Disconnect the session.
13. End

The final message transmitted from each Smart Meter is decrypted and digital signature is verified . The Monitor monitors the network and whenever a Smart Meter with an unknown Id sends a message to gateway it detects the presence and informs the gateway that attacker and has been detected and the intrusion of any attacker will be detected by the monitor. Fig. 4 shows the Monitor detecting an Attacker.

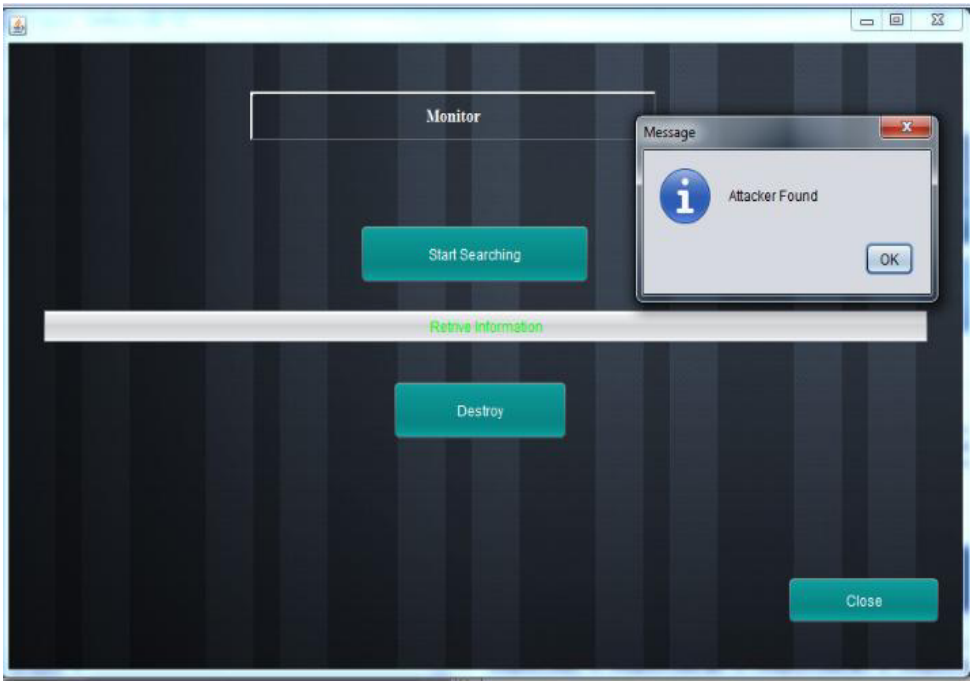

Fig. 4. Monitor Detecting an Attacker

Procedure for Secure Decryption

1. For all messages reaching Central Gateway do
2. Decrypt the Secret Key KS using RSA.
3. Apply Blowfish decryption to obtain plain text for Message, E(ME) using the secret key , KS from step 2.
4. For all message E(ME) do
5. Generate Message Digest (HM)
6. Using RSA's public key generate hash value.
7. Compare Hash values obtained from step 4 and step 5.
8. End for
9. Disconnect the session.
10. End

The performance of the crypto stack has been compared with RSA, Blowfish and AES. Fig. 5 shows the comparative performance of Encryption and decryption time of algorithms. It is found that the encryption and decryption time for the proposed cipher suit is lower than these algorithms. Hence this cipher suit can be used for communication between Central Gateway at the utility Centre and Smart Meter at Home Area Network.

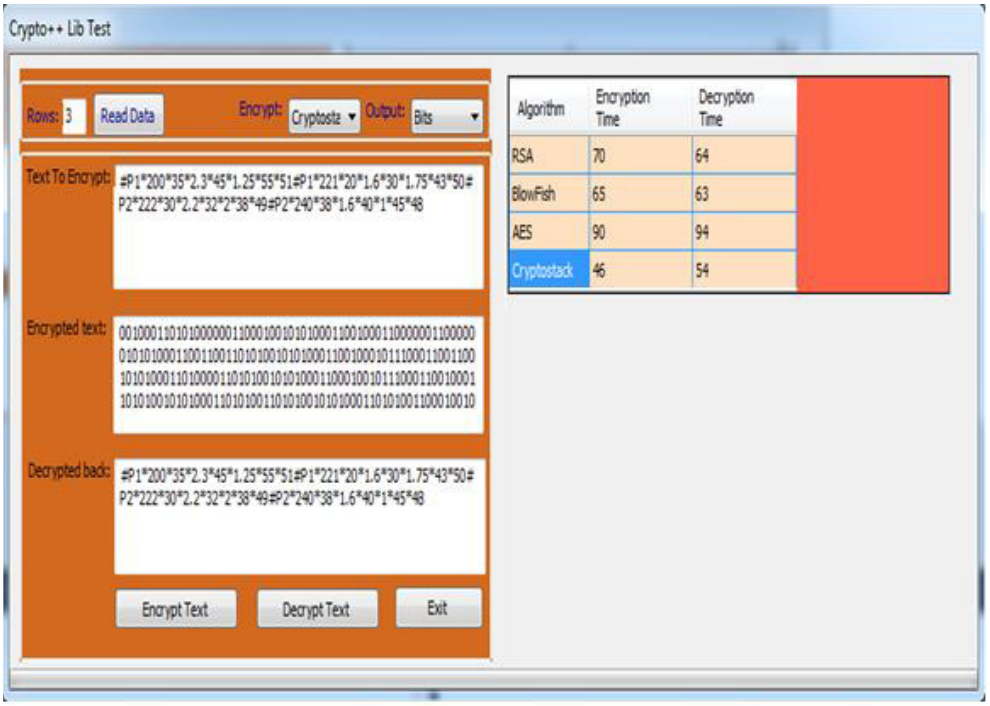

Fig. 5. Comparative Performance of Algorithms

5. Conclusion

As Smart Grid continues to evolve in the coming years, security plays a major role in its deployment. Intelligent electronic devices (IED) in the Smart Grid need to be secure for effective development of Smart Grid infrastructure. In this paper we have proposed Secure Communication architecture between Smart Meters and Central Gateway using crypto stack. Here we have combined the benefits of symmetric as well as asymmetric algorithms to develop an encryption process. To further strengthen the process we have attached a Digital Signature along with the

message. An attacker was introduced to demonstrate the strength of authentication scheme used in this paper. Monitor used in this architecture will be able to detect the attacker .Smart Grid requires integration of wired communication along with wireless communication at the last mile which need to be considered in future.

References

[1] Jixuan Zheng; Gao, D.W.; Li Lin, Smart Meters in Smart Grid: An Overview, Green Technologies Conference, 2013 IEEE , vol., no., p.57,64, 4-5 April 2013.

[2] Meikang Qiu,Hai Su, Min Chen, Zhong Ming and Laurence T. Yang ,Balance of Security Strength andEnergy for a PMU Monitoring System in Smart grid, IEEE Communications Magazine , May 2012.

[3] K. Seethal, Divya M Menon and N. Radhika, Design of a Secure Smart Grid Architecture Model using Damgard Jurik Cryptosystem ,Research Journal of Applied Sciences, Engineering and Technology , vol 9,no.10, p 895-901, 2015.

[4] S.C. Chan, K.M. Tsui, H.C. Wu, Yunhe Hou, Yik-Chung Wu, and Felix F. Wu, Load/price forecasting and managing demand Rsponse for Smart grid, IEEE Signal Processing Magazine [68] ,September 2012.

[5] T. M. Chen, Smart grids, Smart Cities Need Better Networks, Editor's Note, IEEE Network, vol. 24, no. 2, p. 2-3,June 2010.

[6] Zubair Md. FaDLullah, Mostafa M. Fouda, and Nei Kato, Toward Intelligent Machine-to-Machine Communications in Smart grid, IEEE Communications Magazine , April 2011

[7] Adam Hahn and Manimaran Govindarasu, Cyber Attack Exposure Evaluation Framework for the Smart grid, IEEE Trans. Smart grid, Vol. 2, No. 4, December 2011.

[8] Jauch, E.T., Implementing Smart Grid challenges of integrating distribution DG, Transmission and Distribution Conference and Exposition (T&D), 2012 IEEE PES ,May 2012.

[9]Vinaya.V, Sumathi.P, Implementation of Effective Third Party Auditing for Data Security in Cloud, International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, May 2013.

[10] Zhao Yong-Xia; Zhen Ge, , Multimedia and Information Technology (MMIT), 2010 Second International Conference on , vol.2, p..271,273, 24-25 April 2010.

[11] Somani, U.,Lakhani, K.; Mundra, M., Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing, Parallel Distributed and Grid Computing (PDGC), 2010 1st International Conference on , vol., no., p..211,216, 28-30 Oct. 2010.

[12] Pin-Yu Chen,Shin-Ming Cheng, and Kwang-Cheng Chen, Smart Attacks in Smart grid Communication Networks, IEEE Communications Magazine , August 2012.