Research Journal of Applied Sciences, Engineering and Technology 9(10): 895-901, 2015
DOI:10.19026/rjaset.9.2640
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: December 14, 2014 Accepted: January 27, 2015 Published: April 05, 2015

Research Article

Design of a Secure Smart Grid Architecture Model using Damgard Jurik Cryptosystem

K. Seethal, Divya M Menon and N. Radhika
Department of Computer Science and Engineering, Amrita Vishwa Vidyapeetham, Coimbatore, India

Abstract: Smart grid is a paradigm shift from the traditional Power grid which promises to make the electric grid both energy efficient and Fault tolerant. Trade-off between Energy savings and Security is a critical issue in Smart grid architecture. Smart grid architecture requires a high level secure data exchanges between sensors like Phasor Measurement Units and Advanced Metering Infrastructures like Smart Meters. In this study a Secure Smart grid Architecture model is proposed for the Smart grid network. Initially DamgardJurik encryption algorithm is applied on the data from the Phasor Measurement Units and a digital signature is then attached to the encrypted text to provide further authentication. The digitally signed data is collected in Data centre where it is decrypted. The proposed architecture has been implemented in both software and hardware. The effectiveness of the system is verified by introducing an intruder in hardware implementation.

Keywords: DamgardJurik scheme, digital signature, Phasor Measurement Unit (PMU), smart grid

INTRODUCTION

Smart grid has evolved as a powerful replacement for the traditional electrical power grid in the coming years. As the need for Electricity increases so is the need for efficient Power grids. Furthermore the design of our traditional power grids is not able to meet the increasing demands of suppliers. Hence we need a smarter solution and that is Smart grid. The need for an autonomous, self healing, reliable electric grid has paved the way for Smartgrid (Rahimi and Ipakchi, 2010). Bidirectional Communication between Power generation suppliers and end users, deployment of efficient sensors throughout the network makes the grid smarter.

Power requirement by the end users and efficient energy distribution throughout the Smart grid is to be managed by Advanced Metering Infrastructure (AMI), without human intervention. Another main component is the smart meter, which will help the customers to reduce the energy costs and will automatically turnoff devices when there is chance for outage.

Another inevitable part of Smart grid is the sensor network, which consists of a network of sensor nodes that have processing and routing capabilities of information. A sensor network monitors the performance of electronic equipments and generates billing based on information from smart meters (Yan *et al*., 2013).

Smart grid is the need of the century and hence security is a major concern for the grid. While using wireless transmission in Smart grid networks high level of security need to be established at all the three stages of Smart grid network i.e., Power Generation, Power Transmission and Power Distribution. Generation Phase in a Smart grid System does not have any significant change when compared to Power Grid. The major concern for security arises at the communication network deployed in Smart Grid. The Phasor Measurement Units (PMUs) are measuring equipments which functions as sensors in the Smart grid communication network. PMUs require a Coordinated Universal Time (UTC) which it receives from the Global Positioning Satellites. Calibrating the time discrepancies in PMUs is done by Distributed Time Service (DTS). Coordinated Universal Time (UTC) generates the voltage and current values. Data exchanges between the PMUs and PDC that is the central Data Centre require higher level of security. Thus this study proposes a Secure Smart Grid Architecture (SSGA) framework for Smart grid sensor networks. In particular, this study introduces security architecture between the distribution and transmission side of Smart grid while balancing the energy consumption. Further, detailed results are presented for security measures adopted between the sensors and the Data Centre. The major challenge is to ensure high security with low energy consumption.

The architecture of Smart grid system with three main modes of operations i.e., Power generation, Power Transmission and Power Distribution is illustrated in Fig. 1. This study concentrates on the security aspects between the Transmission and Distribution side. Here we have proposed a Secure Smart Grid Architecture

Corresponding Author: K. Seethal, Department of Computer Science and Engineering, Amrita Vishwa Vidyapeetham, Coimbatore, India

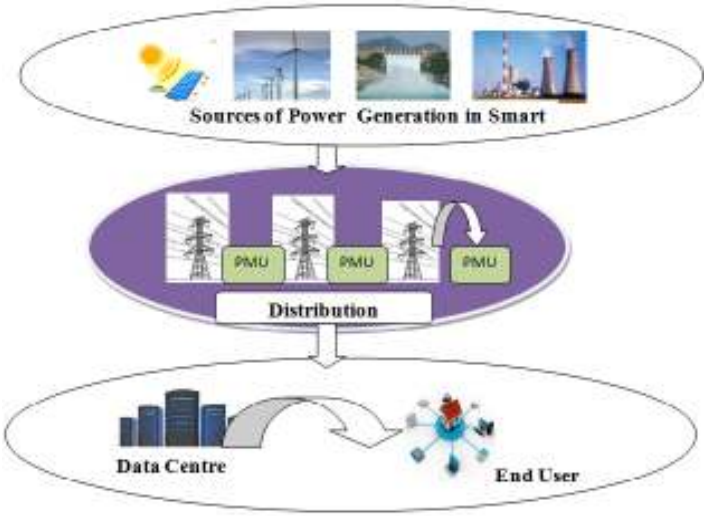

Fig. 1: Smart grid system

(SSGA) covering these two areas. The study is organized in the following three sections as: In the following Sections we have considered the related works in security of Smart grid networks. And we have described the mathematical background used in this model. And also formulated the Secure Smart grid Architecture (SSGA) model in Materials and Methods. In Results and Discussions we have demonstrated the results of both software and hardware implementation. In last Section, we have concluded the paper and provided directions for future research.

Smart grid is equipped with new technologies day by day so there arises for security and privacy concerns. It is so vulnerable and more prone to attacks (Chen *et al*., 2012). So our concern is to provide security for data between transmission and distribution side (Wei *et al*., 2009). Fengjun Li, Bo Lu and Peng Liu proposed (Li *et al*., 2010) a secure data aggregation model using Paillier cryptosystem (Paillier and Pointcheval, 1999) in Smart girds. They have articulated the secure aggregation using a virtual tree based aggregation of data. Ye Yan proposed a security protocol which deals with the Advanced Metering Infrastructure in Smart grid networks. They have proposed an Integrated Authentication and Confidentiality (IAC) protocol which integrates both authentication and confidentiality for collecting data and messages in a secured way. Wang and Yi (2011) have analyzed two problems by creating a wireless mesh network and security framework under this architecture. Within the network an intrusion detection security firewall is built and the network communication architecture is analyzed. Nicanfar *et al*. (1999) articulated a mechanism that utilizes the advances in network in network coding to maintain data privacy in smart gird through which they could ensure schemes for encryption and traffic routing. We need a secure Smart grid system which provides confidentiality and integrity of data. Therefore we have implemented Secure Smart grid Architecture (SSGA) which integrates both encryption and digital signature to assure security in the Smart grid system between transmission and distribution side. We used DamgardJurik cryptosystem (Damgård and Jurik, 2001) which provides additive property of homomorphic encryption function.

MATERIALS AND METHODS

Here we discuss the mathematical background of algorithms used in SSGA model. The main focus is on DamgardJurik scheme (Damgård and Jurik, 2001) for encrypting the phasor values. In our Smart grid system we need to aggregate all the Phasor Measurement Unit (PMU) values and hence our focus is on homomorphic encryption. This algorithm uses the property of additive homomorphism. After applying encryption we are applying RSA Digital Signature Algorithm to the data for authenticity.

DamgardJurik encryption scheme:

Definition: Let (M, o) be the message space. DamgardJurik scheme on M is a quadruple (K_g, E_p, D_c, A) which satisfies the following conditions.

Steps involved in key generation: For an input message DamgardJurik scheme K_g will generate a key pair {k1, k2} where k1→ (n, g) and k2→d:

- Randomly select two prime numbers p and r which are independent
- Obtain the values for n and λ, where n = pr and
- λ = lcm (p-1, r-1)
- Choose $g = (1+n)^j \times \mod n^{(s+1)}$, for all $g \in Z^*_{n^{(s+1)}}$
- Choose b using Chinese remainder theorem where it should satisfies the conditions b mod n $\in Z^*_n$ and b = 0 mod λ

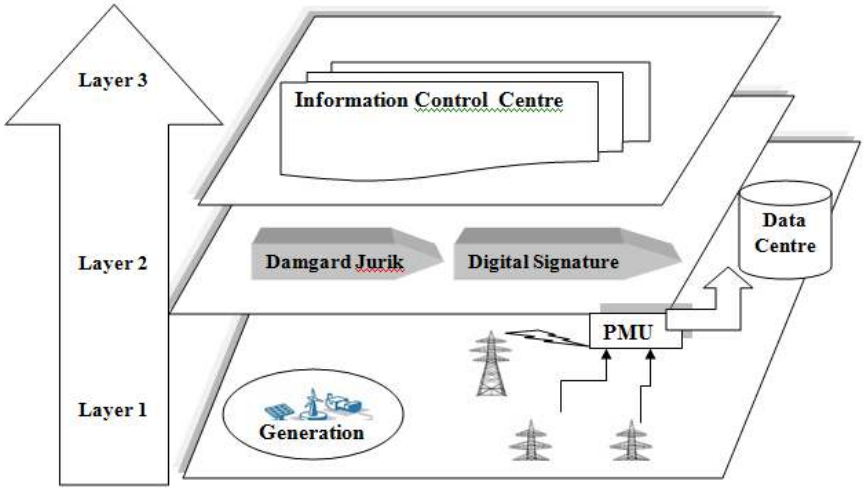

Fig. 2: Layered architecture of secure smart grid architecture

Steps involved in encryption: Choose a random number t, where $t \in Z *_n^{(s+1)}$
Derive the cipher text c, where, $c = g^m . t^{n\,s} \bmod n^{(s+1)}$

Steps involved in decryption: Compute $c^b \bmod n^{(s+1)}$ to obtain plain text.

Digital signature: Digital signature is an authentication for a digital message or document. RSA digital signature validates the PMU.

Sending process: Create a hash value of the message.
Use private key pair (n, d) to generate the signature.
S = Md mod n.
Sends S to the receiver.

Signature verification: The receiver uses public key pair (n, e) to obtain the hash value
R = Se mod n
Generate the hash value from the sender's message
Checks for both hash value
If both values are identical then data will be valid.

PROPOSED FRAMEWORK FOR SSGA

Typically any Smart grid application requires a secure network model for data transmission. The component of this Secure Smart Grid Architecture (SSGA) framework includes a Smart grid Generation Unit, Smart grid Distribution Centre and Transmission Centre. This architecture proposes a new level of security between transmission and distribution of Smart grid system. Therefore we focus on a multi security system to provide secure data transmission.

Figure 2 depicts a layered visualization of Secure Smart grid Architecture model (SSGA). Layer 1 is the Physicallayer which represents the physical components involved in SSGA. Layer 2 is the Secure Communication Layer which provides secure data transmission between the physical components through security algorithms. Layer 3 represents the Application Layer which manages the information in the data centre for user specific application.

Here we consider a Secure Smart grid Architecture model in which there are a number of PMUs attached to the transmission station. PMUs collect all the Phasor Measurement values and will transmit it to the Distribution Controller i.e., Data centre at the Distribution side. Our model encrypts all the PMU values before sending to the Data centre using DamgardJurik Encryption Algorithm. For providing further authenticity the encrypted data is again digitally signed using a RSA Digital Signature Algorithm.

Every PMU holds a database for storing voltage and current values Each Pmu will be having values in the format Pname*V*V_a*I*I_a*F# which it periodically transmits to Data centre. P_{name} defines the PMU name. V, I, V_a, I_a represents the voltage, current values and their angles, respectively. F denotes the frequency. Here every PMU data is separated using #.

Procedure for SSGA software implementation:

1. Read values from serial port.
2. Check for # value.
3. While # do
   Read the PMU Name
   Choose the DB table corresponding to PMU name
   Insert I and V values to the Database
4. End While
5. For all PMU value in DB table do
   Apply DamgardJurik Encryption Algorithm
6. End for
7. Apply RSA Digital Signature Algorithm for the cipher text
8. end

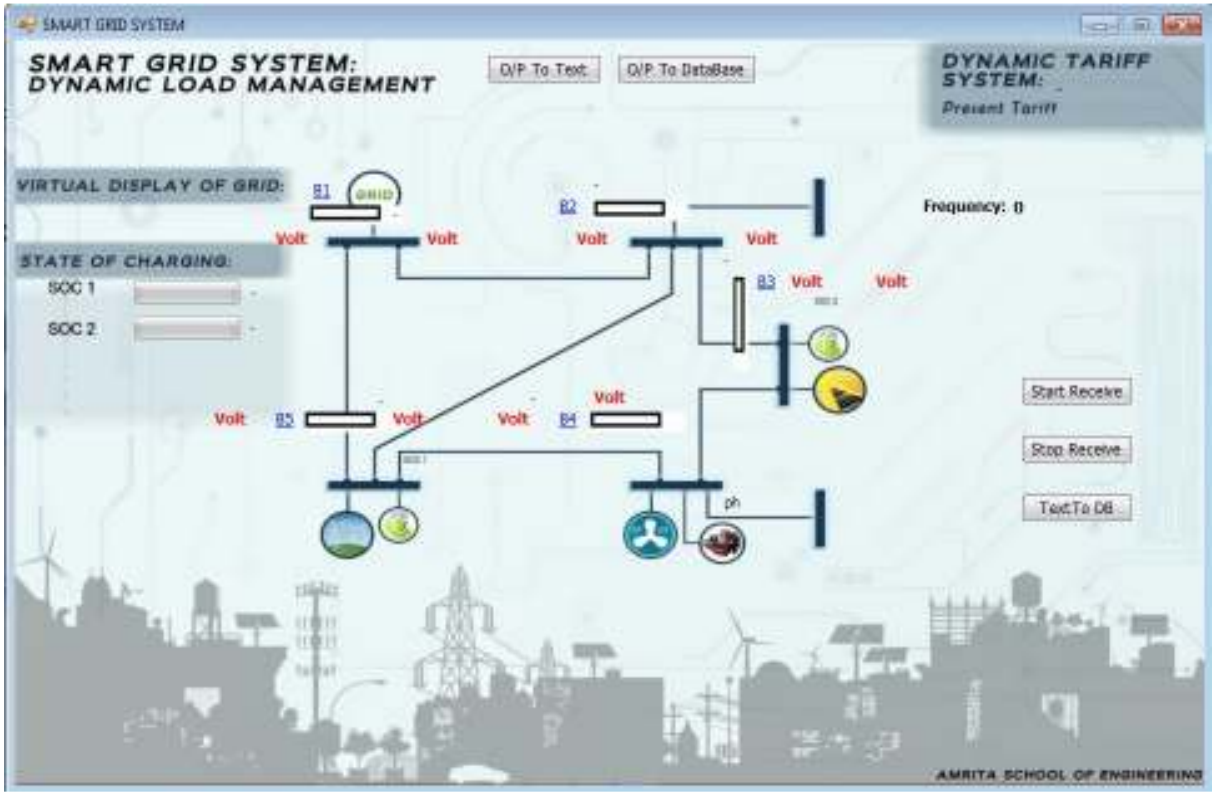

Fig. 3: GUI of secure smart grid architecture

Fig. 4: GUI of web application of secure smart grid architecture

RESULTS AND DISCUSSION

A raw electric system has been made more users friendly by providing a user interface and efficient ways to access data from different PMUs**.** Figure 3 shows the GUI of Secure Smart Grid Architecture. In the architectural GUI we have placed bus buttons which are attached to databases. Whenever values are transmitted from the Smart grid system it will be stored in the corresponding database. It identifies the name of the PMU from the data format and data to the corresponding database is to be entered. From the GUI itself one will be able to get the database value.

In our SSGA two options for data storage is implemented both in database and in website. A database application and a web application is created to store these PMU values.

The Web Application is shown in Fig. 4 where the voltage and current values are stored in web. The Web Application allows the values to be stored in web. Administrators can monitor the performance of the Smart grid by constantly monitoring the PMU Values.

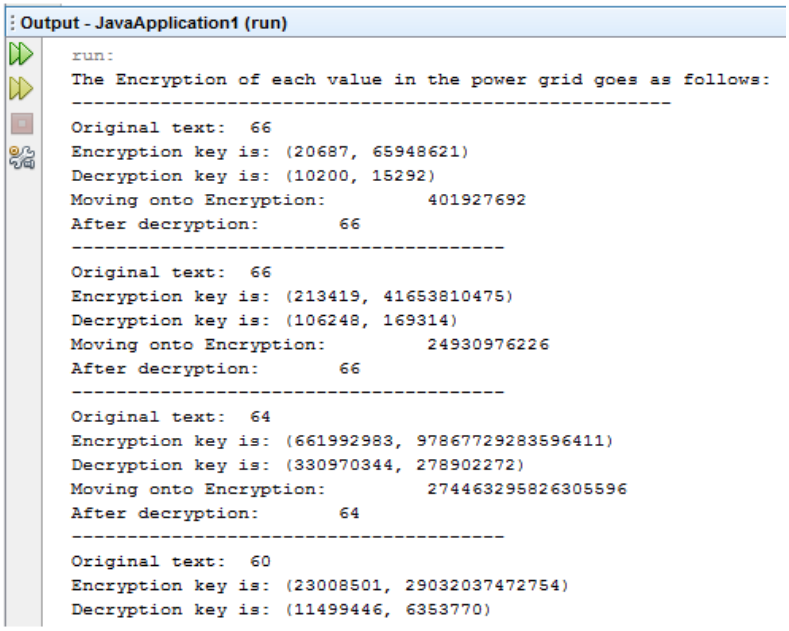

Fig. 5: Implementation of DamgardJurik Encryption

At the Data centre these values are decrypted and the frequency value which controls the Smart grid system is returned to the PMU. The control variable from the datacenter is also stored in this application for performance analysis of the Smart grid System. Since it is decrypted using homomorphic function cipher text can be used for other operations without revealing the actual plain text. DamgardJurik scheme uses additive property of homomorphic function.

The SSGA framework and its methodology are implemented using DamgardJurik encryption algorithm and digital signature algorithm. DamgardJurik algorithm is an additive homomorphic encryption algorithm which ensures the privacy of encrypted data. This scheme works well on encrypted data while maintaining the confidentiality of data. The first step of our approach is to encrypt the phasor values using DamgardJurik scheme. Figure 5 shows the stored values in the PMUs are encrypted using DamgardJurik Encryption Algorithm.

The sender uses a one way hash function to calculate the message digest and uses its own private key to sign the document. The receiver verifies the signed document with the sender's public key. Since the public exponent in the RSA algorithm is smaller than the private exponent, faster signature verification is done. Figure 6 shows the verification of digital signature at the data centre.

Implementation of any encryption algorithms always gains significance when we provide hardware implementation for the algorithm. Speed is a major drawback when running time critical software implementation. An alternative is hardware implementation of encryption algorithms, since provides speed along with secrecy of the encryption.

In our Secure Smart Grid Architecture (SSGA) framework we are collecting all the Phasor Measurement Unit values attached to the transmission system. PMU is a phasor measurement unit attached to Smart grid system which measures voltage and current values periodically. These PMU values are encrypted using DamgardJurik encryption algorithm. For a higher level of security we are applying digital signature algorithm for the encrypted values. A number of PMUs are connected to each other. Each Pmu will be having values in the format P_{name}*V*V_a*I*I_a*F# which it periodically transmits to Data centre. P_{name} defines the PMU name. V, I, V_a, I_a represents the voltage,899current values and their angles respectively. F denotes the frequency. Encryption is done for these values at the sender side (i.e., in PMU) and they are digitally signed before transmitting to the Data Centre.

At the receiving side these values are decrypted and the frequency value is used for controlling the Smart grid system. Depending on frequency values transmitted from each PMU a control variable is transmitted from the data centre back to PMU.

dsPIC30F4011 a high-Performance, 16-Bit Digital Signal Controller is used for our hardware implementation of the PMU which operates at speed 29.49MHz. This microcontroller is programmed for encrypting the data using DamgardJurik encryption algorithm and the data is transmitted to PIC16F877A. Figure 7 shows the hardware schematic where the 16 bit microcontroller encrypts the data and transmit it to the datacenter. Zigbee module is used for the wireless transmission between the PMUs and Data centre. We have introduced an intruder PC which checks the security of the SSGA model.

Fig. 6: Digital signature verification

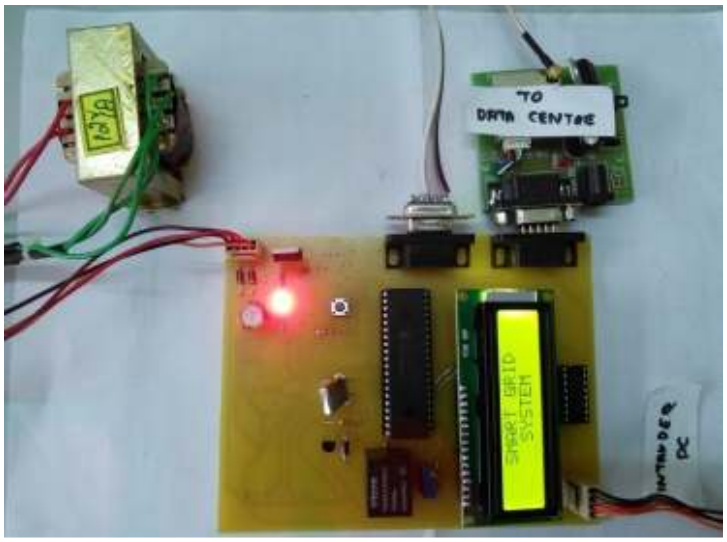

Fig. 7: Hardware schematic for single PMU

CONCLUSION

Security has become a major concern in Smart grid networks. In this study a Secure Smart Grid Architecture model (SSGA) was proposed for Smart grid networks. The security framework for this architecture is expected to satisfy the security requirements between the transmission and distribution side in the Smart grid network. We have applied DamgardJurik encryption algorithm for providing data security. To further provide additional security the encrypted data is again digitally signed using RSA Digital Signature and finally transmitted to the Data centre where it's decrypted. We have carried out both software and hardware implementations of this model. The reliability of the implementation has been checked with an intruder. In our future work, we will employ Cloud storage for the Data. In the long term we will also develop a more holistic security model covering the generation and distribution as well.

REFERENCES

Chen, P.Y., S.M. Cheng and K.C. Chen, 2012. Smart attacks in smart grid communication networks. IEEE Communi. Magaz., 50(8): 24-29.

Damgård, I. and M. Jurik, 2001. A Generalisation, a Simplification and Some Applications of Paillier's Probabilistic Public-Key System. Public Key Cryptography, pp: 119-136.

Li, F., B. Luo and P. Liu, 2010. Secure information aggregation for smart grids using homomorphic encryption. Proceeding of 1st IEEE International Conference on Smart Grid Communications (SmartGridComm), pp: 327-332.

Nicanfar, H., P. Talebifard, A. Alasaad and V.C.M. Leung, 2013. Enhanced network coding to maintain privacy in smart grid communication. IEEE T. Emerg. Topics Comput., 1(2): 286-296.

Paillier, P. and D. Pointcheval, 1999. Efficient public-key cryptosystems provably secure against active adversaries. In: Lam, K.Y., E. Okamoto and C. Xing (Eds.): ASIACRYPT'99, LNCS 1716, Springer-Verlag Berlin Heidelberg, pp: 165-179.

Rahimi, F. and A. Ipakchi, 2010. Demand response as a market resource under the smart grid paradigm. IEEE T. Smart Grid, 1(1): 82-88.

Wang, X. and P. Yi, 2011. Security framework for wireless communications in smart distribution grid. IEEE T. Smart Grid, 2(4): 702-706.

Wei, X., Z. Yu-Hui and Z. Jie-Lin, 2009. Energy-efficient distribution in smart grid in sustainable power generation and supply. Proceeding of International Conference on SUPERGEN'09, pp: 1-6.

Yan, Y., R.Q. Hu, S.K. Das and H. Sharif, 2013. An efficient security protocol for advanced metering infrastructure in smart grid. IEEE Network, 27(4): 64-71.