ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com

Hybrid Security Approach for Smart Grid Infrastructure

Preethi S., U. Sushritha, SwethaShri V. and Dr. Jawahar A

Department of Electronics and Communication Engineering, SSN College of Engineering, Anna University, Chennai, India.

ARTICLE INFO

Article history:
Received 20 January 2015
Accepted 02 April 2015
Published 20 May 2015

Keywords:
Smart Grids
Secure communication
Hybrid Cryptosystem

ABSTRACT

A smart grid is an advanced grid system that manages electricity demand in a sustainable, reliable and economic manner. Smart grid is evolving as an intelligent architecture that will lead to fully automated and self-healing architecture in the future. A proper communication infrastructure is required to provide a real time automated platform for efficient power distribution wherein the security threats must be addressed. The objective of this paper is to provide an appropriate secure communication network between the customer and the energy service provider. In this paper, we have analyzed various cryptographic systems that will be suitable for the huge volume of data associated with smart grids.For such voluminous data, we conclude that hybrid cryptographic algorithms are more apt as they provide less encryption times with secure simultaneous transfer of data.

To Cite This Article: Preethi S., U. Sushritha, SwethaShri V. and Dr. Jawahar A., Hybrid Security Approach for Smart Grid Infrastructure. ***Aust. J. Basic & Appl. Sci.,*** *9(16): 91-96, 2015*

INTRODUCTION

The power grid which is in use now is aging with respect to infrastructure and technology. Smart grid technology is one of revolution which proves to be an asset in the near future. Modernization with Smart Grids will help in less consumption of the energy sources available and will make sure that the same will be available for prolonged years. These technologies enable energy companies to seamlessly control the power demand and allow for an efficient and reliable power delivery at reduced cost. Via digital two-way communications between consumers and electric power companies, the smart grid system provides the most efficient electric network operations based on the received consumer's information. But there are certain severe shortcomings in the hardware and software which will come out as a threat to this massive network. We see an urgent need in a complete overhaul of both hardware and software control platforms for the power grid and power devices in particular [8]. Need for such software design as to prevent the vulnerabilities are of great security concern now. We propose a strong solution for the safety, security and advantageous implementation of the Smart Grid technology.

A. Related Work:

In this section, we briefly highlight some of the work done with the details regarding the architecture and security area of the smart grid network.

FadiAloulaet. Al, 2012 in this paper, they have surveyed the vulnerabilities in smart grid networks, the types of attacks and attackers, the challenges present in designing new security solutions, and the current and needed solutions.

Metke.A.R and Ekl.R.L, 2010, discussed key security technologies for a smart grid system including public key infrastructures and trusted computing for various smart grid communication networks in their paper "Security Technology for Smart Grid Networks". They thoroughly presented the security requirements that are essential for the proper operation of the future grid.

Elias Bou-Harbet. Al. 2013, investigated applicable communication mechanisms that could be adopted in smart grid distribution networks. To tackle the cyber security of such infrastructures, we have pinpointed their security objectives and threats. They have further elaborated on their practical feasibility in terms of their technical implementation, possible obstacles and core security issues.

Frank Mueller et. Al, discussed cyber security challenges for the future power grid highlighting areas of urgent need on the software side to establish security as a first-class paradigm in cyber-physical control systems.

J. Daemen and V. Rijmen, 1999, thoroughly described the entire process of Advanced Encryption Standard which helps us in understanding the step by step working of the algorithm. The paper also clearly

Corresponding Author: Preethi S., Department of Electronics and Communication Engineering, SSN College of Engineering, Anna University, Chennai, India.
Tel: 9003267723; E-mail: preethisathiya229@gmail.com

mentions about the overall structure of AES, and its salient features.

To the best of our knowledge, the work being presented in this article is unique in providing a significant information and practical solution for the security need along with the list of the threats that the smart grid network is vulnerable to, with the use of the hybrid cryptosystem technology, which is elaborately addressed for both the algorithms used.

B. Motivation:

History has proven that industrial control systems were in fact vulnerable to and victims of cyber-attacks. World energy demand is expected toincrease at an annual rate of 2.2 percent,doubling the global energydemand overall. The smart grid is an evolution of the electricalgrid to respond to these challenges. The importance of maintaining the standards of the Smart Grid technologyover time at an appropriate pace is at maximum. The cyber threat landscape is evolving so quickly that thelast few years have seen an exponential growth of threats. The security attacks are becoming highly sophisticated and these attackers are no longer amateurs, but highly skilled and organized professionals who are able to launch complex and coordinated attacks using sophisticated tools. It is therefore of utmost importance toaddress the cyber security aspect of the smart Grid, specifically the area concerned with thecommunication mechanisms that deal with thedistribution subpart.

The article is organised in the follow. We pinpoint the motivation and the related work in the area concerned for this article. We thoroughly elaborate about the Smart Grid architecture and the infrastructure. The details of the cryptosystem algorithms are discussed in the next two sections. The effective proposed solution is explained. Finally, we summarize and conclude this article.

II. Smart Grid:

Smart grid is evolving as an intelligent architecture with a complex system of computers and technologies that work on information based approach. It can also be referred to as the advancement of the current electric grid as it serves the purpose of bidirectional flow of information. The implementation of the smart grid would require advanced sensors and metering and the integration of distributed generation resources. With the help of smart grids, consumers can decide with diverse choices on when and how much electricity must be used and at which particular interval of time. The above goals cannot be realized unless there is proper communication technology that will gather, assemble and synthesize data provided by the smart meters. In simple words smart grid can be described as network of networks with lots of sensors and is self monitoring. It can also self reconfigure providing a distributed electricity generation with active control type, pervasive control ability, low environmental pollution, and remote check testing along with high overall efficiency. It will lead to a fullyautomated, self-healing system which is predictive rather than reactive along with interaction with customers in the future.

The smart grid network consists of the generation, transmission, distribution, customers, markets, operations and service providers. In the smart grid, power flows from the generation across the transmission systems to the end users and pricing and other regular information flows back to the energy service provider with the help of a cloud network which connects the power station, utility, HAN(Home Area Network), smart meter and the devices[Fig(1).]. There are several links between the transmitting side and the receiving side. A proper communication infrastructure is required to connect these links and provide a real time platform for efficient continuous monitoring of the entire system as a whole. Issues like long range connectivity and cyber security also need to be taken care of. The paper proposes a solution to deal with the security threats that the network is prone to.

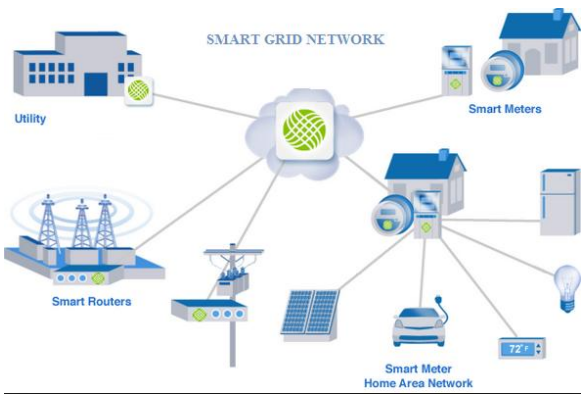

Fig. 1: Diagram showing the Overall Smart Grid Network.

An important characteristic of the smart grid is that it dynamically reconfigures multidirectional energy flow, and manages a cloud-based network of connected systems that need to communicate with eachother and with central control systems. This is advantageous to the customer as it helps them in the better management of their electricity consumption and helps in avoiding energy crisis in the future. Smart grids are however vulnerable to several malicious attacks. The main points of attack by intruders are the end user points as well as the central hub that is responsible for the management of the smart grid network. In the smart grid, operators will expect to have complete transparency and visibility to monitor, analyze, and control energy systems. They will need to know how much energy is being generated and how much is being consumed, where it is coming from and where it is going. They will also need to communicate with the various systems within the network to be able to control them to ensure optimum efficiency. Decisions must be made based on real-time data generated by the system constantly instead of past values of data. Smart grids also require a high degree of interoperability between a large numbers of intelligent devices. Interoperability is the ability of two or more systems or components to exchange information and to use the information that has been exchanged. Interoperability includes operability and controllability.

A. Infrastructure:

The major issue in smart grid infrastructure is how to provide an appropriate communication network between the customer and the energy service provider and to identify possible threats at the equipment level and the link level and to provide an appropriate solution to mitigate this issue. In establishing an appropriate communication infrastructure and to complete the data transfer towards the utility, WiMAX topologies can be implemented. IEEE 802.16 WiMAX is the better option. The frame format of WiMaX with which the data must be sent is as show in the Fig (2). WiMaX is similar to Wi-Fi but operates at higher speeds over greater distances and for a larger number of customers. Another benefit of WiMAX over Wi-Fi is that, it can provide full duplex operation between the end users. Two forms of wireless services are possible with WiMAX namely non-line of sight and line of sight. Non-line of sight option is similar to that of Wi-Fi where a small antenna on the smart meter connects to the WiMAX tower by using frequency range similar to that of Wi-Fi (2GHz-11GHz). In line of sight service, a fixed dish antenna points straight to the WiMAX tower may be from a roof top and the frequency range goes up to 66 GHz.

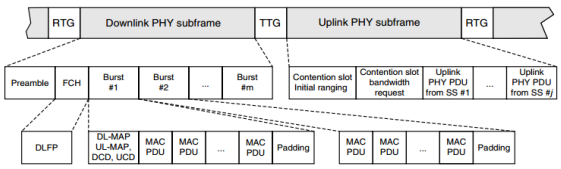

Fig. 2: IEEE 802.16 WiMAX frame format.

III. ***Threats:***

Some of the following vulnerabilities are the most serious in smart grids:

1) The massive amounts of data that are collected by smart meters are transported to the utility service providers. The data may contain information about when the service is being used by the customer and when it is vacant.

2) The smart grids contain a number of intelligent devices and may act as attack entry points into the network.

3) Physical security: Unlike the traditional power system, smart grid network includes many components that are out of the utility's premises thereby increasing the number of insecure locations.

4) Whenoutdated equipments are still in service, it acts as a weak security point and arealso incompatible.

5) Using various standards in smart grids is inherently vulnerable to many IP-based network attacks such as IP spoofing, Tear Drop, Denial of Service, and others.

6) Presence of many stakeholders might give raise to a very dangerous kind of attack.

The above mentioned vulnerabilities can be easily exploited by the attackers and cause different levels of damage to the network.

1) The attackers use various malware devices and them to the smart grids or replace them with sensitive information thus attacking the network.

2) When the database is not properly configured at the base, a skilled worker can gain access to the database and use his skill to exploit the system.

3) Injecting false information (Replay Attack): An attacker can send packets to inject false informationin the network, such as wrong meter data, false prices, fake emergency event, etc. Fake information canhave huge financial impact on the electricity markets.

4) Sensitive information can be obtained by monitoring network traffic which is known as eaves dropping.

IV. *Advanced Encryption Standard:*

Cryptography also called cryptology is the technique of hiding information for security purposes. Advanced encryption standard (AES) is the symmetric key algorithm that is used in the hybrid cryptographic system. Since it's a symmetric key algorithm, it provides a single key for both the encryption and decryption process. It is a strong cipher based algorithm that protects classified information. It provides not just security, but also balances good performance and efficiency.

Rijndael algorithm is the one that has been chosen for the encryption process. It is different from the official specification of AES where the block size remains fixed (128bits) while the key size varies as 128, 192 and 256. In Rijndael, both the block and the key sizes can vary. AES has three block ciphers, which are AES-128, AES-192 and AES-256. AES-128 would be a good enough implementation for use in the smart grid network, as the other two are more complex and they are preferred only for higher level of secure data.

A. Operation:

AES requires several rounds of operation to obtain the encrypted data. AES-128 requires only 10 rounds as compared to the other two requiring 12 or 14 rounds. Each round comprises of definite steps. The steps include substitution, transposition and mixing of the input plaintext. The round transformation is composed of four steps. They are byte sub, shift row, mix column and add round key. The AES encrypted information is available at the end of these four steps, which can be assumed to be strongly secure.

The algorithm is so strong that it will take a billion years in order to break the 128-bit key based algorithm and will require as much as trillions of Terabytes of memory space just to store the information gathered through the process. It will take even more for the 192 and 256 bit keys. Practically, there are no methods to completely break the algorithm.Attacks on the algorithm have been successful only in a very restricted environment. One of the attacks on AES is called as side-channel attack. It may not exactly attack the algorithm by itself, but attack only the implementations thereby resulting in a security breach. Several such attacks have come out in the recent times. A paper published recently proposed a method that was able to attack one such implementation of AES in just 60 milliseconds. Even though the probability of attacking such strong algorithms remains less, they cannot be used to protect sensitive information. This can be made more efficient by introducing a hybrid cryptosystem. The hybrid cryptosystem is a combination of two algorithms: one symmetric and the other asymmetric. ElGamal is a strong asymmetric key algorithm.

V. *Elgamal Algorithm:*

Public key cryptography, or as known as asymmetric cryptography, is a type of cryptographic algorithm which requires two different keys, a private one and another one which is public. The public key is used for the encryption of the message or to verify a digital signature; whereas the private key is for the purpose of decryption of the cipher text or to generate a digital signature. Different keys are required to perform these opposite functions, each the inverse of the other and hence called asymmetric encryption system as contrasted with conventional symmetric cryptography which relies on the same key to perform both. The two main basic cryptographic schemes for public key cryptography are RSA and ElGamal. The ElGamal system is a public-key cryptosystem that takes the lesser storage space when compared to RSA. The security of ElGamal depends on the difficulty of computing discrete logs in a large prime modulus, whereas the security of RSA depends on the difficulty of factoring large integers.Let p be a prime and α and β be nonzero integers and suppose

$$\beta \equiv \alpha^{n} \bmod p \quad (1)$$

The problem of finding n in eqn.(1) is called the discrete logarithm problem.

ElGamal consists of both encryption and signature algorithms. ElGamal encryption is used in the free GNU privacy Guard software, recent versions of PGP, and other cryptosystems. The encryption algorithm is similar in nature to the Diffie-Hellman key agreement protocol. The system parameters consist of a prime p and an integer g, whose powers modulo p generate a large number of elements, as in Diffie-Hellman. ElGamal decryption (without knowing the private key) is equivalent to solving Computational Diffie-Hellman. The ElGamal Algorithm provides an alternative to the RSA for public key encryption. The ElGamal signature algorithm is similar to the encryption algorithm in that the public key and private key have the same form; however, encryption is not the same as signature verification, nor is decryption the same as signature creation as in RSA. ElGamal uses randomization, an advantage which provides many different possible cipher texts with near certainty each time it is encrypted for the same message. For high voluminous amount of data as required for smart grid data transfer, ElGamal encryption is faster.

Also ElGamal is a multiplicatively homomorphic cryptosystem. RSA system without modifications is not semantically secure whereas with slight modification, ElGamal can be made

semantically secure. Though adding good padding (OAEP) will make RSA semantically secure, the homomorphic property is lost. Even if the hacker tries to compute a discrete log in the large prime modulus, the computation is too difficult to be practical, especially when the prime number chosen is greater than 200 digits. It is easy to compute modular exponentiation but, it is hard to compute the inverse operation of the modular exponentiation, i.e. discrete log. Using this properly it will be able to set up a secure channel between two parties and used for two way communication. The major application of Elgamal is establishing a secure channel for key sharing and encrypting messages for high possibility of security. The main feature which decreases the possibility of attack is the use of a random factor k for encryption.

A potential disadvantage of the ElGamal system is that message expansion by a factor of two takes place during encryption. This is particularly not helpful when considering high volumes of data as in smart grids. However, such message expansion is negligible if the cryptosystem is used only for exchange of secret keys and not the actual information itself.

VI. *Proposed Solution:*

We computed the complexity of RSA and ElGamal for the modulus function used in the encryption and decryption process. Using the extended Euclidean algorithm for the inverse modulo in the decryption process, the complexity of the two was found out as shown in table I. This shows the efficiency of the hybrid system with AES and ElGamal. Therefore, large amounts of data associated with smart grids are encrypted by using a hybrid cryptosystem of Advanced Encryption standard (AES) and ElGamal. The Advanced Encryption standard is used to encrypt the raw data itself, while ElGamal is used to encrypt the 128-bit key used in AES.

Table I: Complexity of the algorithms.

ALGORITHM	PROCESS	FORMULA	COMPLEXITY
RSA	ENCRYPTION DECRYPTION	$C = M^e \bmod N$ $MP = C^d \bmod N$	$O(\log(N)^3)$
ELGAMAL (With Euclidean)	ENCRYPTION DECRYPTION	$C = M*k \bmod N$ $MP = C*k^{-1} \bmod N$	$O(\log(N)^2)$

Fig (3). shows the execution time comparison for a hybrid system of AES and ElGamal, AES and RSA, and AES and ElGamal using extended Euclidean algorithm. The system of AES and ElGamal with extended Euclidean algorithm has the best execution time and is therefore, faster. This hybrid cryptography leads to an advanced level of security and is better than a single standalone algorithm in protecting the information from attacks.

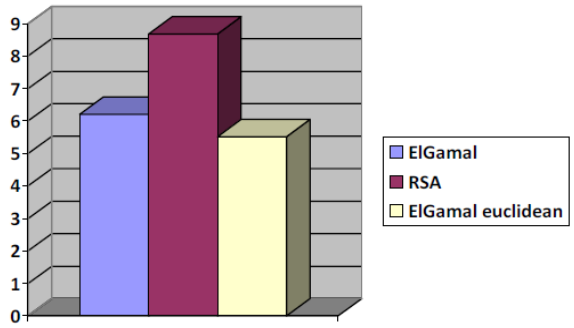

Fig. 3: Execution time comparison for the hybrid systems of AES and ElGamal, AES and RSA, and AES and ElGamal using Euclidean algorithm.

VII. *Conclusion:*

The smart grid infrastructure requires additional features to secure the information from various threats, for a sound and efficient system. In this paper, two algorithms, AES and ElGamal are explained in detail in different sections. The complexity for choosing the best algorithm to be used in the hybrid system has been computed and tabulated. The two algorithm are combined to get a hybrid cryptosystem that can be used in a smart grid network to encrypt and to ensure safe transmission of the data from the end user to the energy service provider and vice versa.

REFERENCES

Aloula, A.R. Al-Alia, Rami Al-Dalkya, Mamoun Al-Mardinia,Wassim El-Hajjba, 2012. "Smart Grid Security: Threats, Vulnerabilities and Solutions", International Journal of Smart Grid and Clean Energy, 1(1).

"Cisco backs Grid Net's WiMax smart meter play", Greentelecomlive.com.

Daemen, J. and V. Rijmen, 1999. "AES Proposal: Rijndael", *AES Algorithm Submission*.

Elias Bou-Harb, Claude Fachkha, Makan Pourzandi, Mourad Debbabi, and Chadi Assi, Concordia University, "Communication Security for Smart Grid Distribution Networks".

Energy Security white paper, "Building a Smarter Smart Grid: Counteracting Cyber-Threats in Energy Distribution".

Frank Mueller, Subhashish Bhattacharya, Christopher Zimmer, "Cyber Security for Power Grids" .

Intel's white paper, "Smart Grid Cyber Security".

Metke, A.R. and R.L. Ekl, 2010. "Security Technology forSmart Grid Networks," *IEEE Trans. Smart Grid*, 1(1): 99–107.

Ruofei Ma, Hsiao-Hwa Chen, Yu-Ren Huang, and Weixiao Meng, IEEE, "Smart Grid Communication: Its Challenges and Opportunities".