Volume 5, Issue 8, August 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Key Management Scheme and Cryptography in Smart Grid Elements

Dr. Sajjad Hussain, Raja Omman Zafar
Department of E.E, Muhammad Ali Jinnah University
Islamabad, Pakistan

Abstract— Smart grid technology can improve environmental sustainability, the energy management efficiency. Due to these significant advantages, the traditional grid system has been replaced by a new, expanded use of advanced metering infrastructure (AMIS) intelligent network system. These smart grid systems are based on the current information and communications technology (ICT) for users and better public services utilities. However, the use of information and communication technology is to the smart grid system vulnerable to cyber-attacks such as spoofing, listening and attack man-in-the-middle. A big security problem is to make sure that the data transfer between smart meters and utilities. Encryption technology is often used for this purpose. The encryption is generally used as a magic silver bullet adds safety applications. In fact, a question of the encryption technique is a key component of most of the standards and technologies. However, by itself, it does not provide security encryption ensures the confidentiality of data exchange. To be effective, there must be a comprehensive process to ensure that the level of information security. In addition, encryption introduces its own challenges, such as key generation, distribution, management and interoperability.

In this article, we provide efficient encryption key management mechanisms and interoperability, end to end security between the intelligent network elements. In particular, we describe the symmetric and asymmetric encryption, X.509 certificates and how they are in a variety of technologies, including VPN and TLS for authentication. Use the administration of the symmetric encryption key to smart meters and interoperability, eliminate our method the security threat. In addition, our mechanism is practical because no additional verification of the smart meter hardware is required.

Keywords—Certification Authority, Intelligent Electronic Device, Home Area Network, Public Key Infrastructure, Power Line Communication, Smart meter Identification Number, Confidentiality, Integrity, Availability.

I. INTRODUCTION

Smart Grid is a joint power grid, increased power from supplier to consumer. It is expected to bring a number of benefits, many governments are now widespread. It is customers the benefits of smart energy demand provide describes how to careful handling of the time, the concept of price signals based settlement tools. To this point, the user can illustrate on the smart grid in certain activities, such as washing clothes, when electricity demand is low, reducing the bonus, and allows customers to carefully plan their energy consumption. Further advantages of the smart grid must be protected to improve the reliability, efficiency, economy and national security as an improved easier to control and monitor [7]. Smart Grid is based on the order that is based on the idea of two-way digital communication control device in the consumer's home. Although this concept is new endless communication between the two sides has never materialized to such an extent that. In the case of the smart grid the monitoring is done by implementing a smart metering systems network, including smart meters carried out in order to communicate with the central system. It tracks all flow mains. This does not mean that these machines are not in the normal use of the grid, but in the case, the flow of electricity smart grid monitoring many other details.

Even the use of the smart grid has huge economic benefits, critical security and privacy concerns. In particular, in the intelligent network system is Advanced Metering Infrastructure (AMI) for the collection, analysis and retention of data from smart meters and meters is responsible to provide the data. However, AMI is due to the widespread use of information and communication technologies (ICT) are vulnerable to cyber-attacks. Hackers can use malware to launch a massive attack on the AMI or destroy targets with smart meters in order to manipulate data. Therefore a key provide the appropriate level of security. AMI is particular to ensure that all exchange of data between the meter and the utility. These data are moved generally by a plurality of ways to achieve the goal. Although each connecting plane hop supports the safe use of the communication protocols that is sufficient to provide adequate data integrity and confidentiality must be guaranteed, because the damage cannot intermediate nodes are familiar with the relevant data protection. Thus, acute myocardial infarction, it is necessary, a communication unit, which requires the use of a secure communications channel between the level of encryption security technology application support end-to-end establish. Encryption technology in AMI deployment requires efficient and scalable way to manage encryption keys.

According to a recent study [6] to the Smart Grid key management mechanism should secure on public key cryptography

(PKC) and a public key infrastructure (PKI) to build, because they have lower costs encrypted symmetric key Management. Historical research [9, 8, 10] investigated the safety mechanism of protein kinase for the Smart Grid C-based. However, the traditional approach to the implementation of the PKI smart grid management to introduce huge issue digital certificates. The utility or other representatives of the utility to manage encryption keys must be issued and managed smart meters all certificates of millions. Therefore a traditional PKI solution is not scalable.

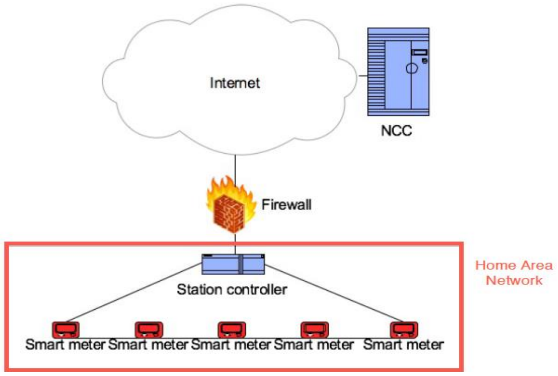

Fig 1: Scenario

II. SMART GRID ELEMENTS

The smart metering infrastructure consists of three main units: smart meters, a base station controller and a network control center. Smart metering and communication between the base station controller network communication from home is to, thanks to achieve a power line in order to use the availability of AC power cord. In the TCP / IP stack is selected as a high-level communication protocol for this scenario. The reason for this is that there is an increasing trend, the use of this technology [5], because they have a different common technology protocol PHY / MAC.

A. SMART METER

Intelligent Electronic Device (IED) is a technical term used in the power of the digital control unit. IED includes a sensor to provide the necessary data to send control commands. A smart meter (Figure 2) is an electronic device with two-way communication. It records in an hour or less [1] intervals consumed and periodically send to the public for the purpose of tracking and billing. In other words, there is a better output power monitors to collect data in a very short interval remote reporting. The most important advantage is that the real-time monitoring, including the ability during a power failure notification operation and monitoring of energy quality. The main technical problem is the communication on smart meters. The device is safe and reliable manner that the base station controller has caused many problems measure. Another problem is that in a different environment, in which the operation of rice. There are many solutions, including communication in the communication of the carrier flow line, mobile and WiMAX, satellite and mobile technologies. However, we will see how it is based on the use of funds, there is a variety of benefits, such as sales network and service tools, and this realizes a working communication carrier power line.

Fig 2: Smart Meter

B. POWER LINE COMMUNICATION

Power Line Communication (PLC) is a technique for carrying out the exchange of data routing. It can be transmitted to the high-voltage or low-voltage cables in the building. Each power line communication system transmits a modulated signal in the cable network. PLC technology is the most widely used local networking provided HomePlug Powerline Alliance called HomePlug AV [12] of the product. Other similar applications are LonWorks ™ bus technology [13] and G.hn [14, 18]. Since many companies have developed different specifications, there is a global standard. In ITU-T G.hn that the use of the high frequency power line communication standard was also known as IEEE1901 is known in order to standardize the working group network of power lines. The standard of the final version was approved in September 2010 for 30 years for the line support communication technology to smart grid power are considered.

C. ENCRYPTION AND KEY MANAGEMENT ISSUES

In many networking standards, all communications were the same encryption key. This means that if an attacker compromise with malicious intent single device, capable of spying on all communication between network nodes is he / she. Thus each device needs to have a unique key material; such a device does not affect the safety of other devices. Key management system should include the up-to-date and relevant key revocation key update process; an encryption key is the time duration or the amount of change of the encryption key data after predetermined [3]. This shall be limited to the same encryption key in which realize the safety data a positive impact on the data. However, if the key has been compromised or lost need to remove before serving. This is called the process of withdrawal of the completion key.

I. ASYMMETRIC CRYPTOGRAPHY

Asymmetric cryptography is sometimes referred to as public key cryptography, as some algorithms pair public / private key. Private Key is known only to its owner, while the public key is that we all know. Public-key encryption algorithm in such a way that this calculation is very simple to produce, from private, but in the case of sufficient key length reverse process key employment should be public. To public-key encryption initialization security dialogue party's use - to send a message encrypted with the public key of the recipient. As mentioned above, only the private key decrypts the encrypted message key and public-private key is known only because the owner (in this case the receiver), capable of a message to be read. This concept ensures a secure conversation on both sides with public keys, because the confidentiality of information.

II. SYMMETRIC CRYPTOGRAPHY

Unlike the public key encryption, symmetric encryption using only a decryption key for the encryption and secret information. There are two types of symmetric algorithms: encryption stream and block ciphers. The difference between the two is that the stream ciphers encrypt each number separately (typically bits) and the number of bit block cipher encryption blocks called. The block size depends on the use algorithm. Using symmetric encryption dialogue between the parties is very simple. The sender with an encryption key using the already negotiated a particular encryption algorithm message. After the arrival of the message, the receiver is adapted to use transmit the same key as the decryption process.

It is known to protect a symmetric key algorithm, at the cost of less than the asymmetric key scheme is calculated. They are also more efficient because they require less computing time. However, symmetric key algorithm has a shorter life because it needs less time to open the key with brute force techniques Key exchange is problematic, because the security of the key exchange before delivery requires via secure channels [4].

III. EXISTING TECHNOLOGY

Home-Plug AV connection with symmetric keys, Advanced Encryption Standard (AES) key algorithms [9] and a simple symmetrical encryption block protocol mode shift key (CBC) [11] - Home. If the network [19] Host connector for smart metering technology, operation and the ignition key in rice [2], which are printed in the production of intelligent instruments and 128 bits. If the device is connected to the HomePlug network, the person responsible for the installation in the ignition key. Then a new key distribution will begin. The aim is to obtain a base station control device and the other for the IED communication authentication key.

In summary, home audio and video plug-in adequate security and low IT requirements. This is the best, no doubt for our scenario for modern technology. Moreover, it is not Powerline to meet the needs of its G.Hn and dragon Communications environment various technical design of communication media. Due to this fact, we Plug AV to better meet the requirements. The main reason for this decision is that the standard is the next better technical solutions, and can be easily changed to meet the other requirements.

III. NEW KEY MANAGEMNET SCHEME

Now we have the affected family identified –Home-Plug AV, it may be a better way to solve the key issues of the exchange key security, we can design a new key exchange system. As a basis for the new program, we use the same algorithm as the standard family, AV connector and some design changes to reduce these risks.

A. Key distribution and authentication

Step 1:

I→C: E {{N, Y}m , SID }

If the maintenance personnel to install a new member of the FDI, it sends a message to the control station includes random number N and joined the request of the ignition key encryption y. In this case, the key is not printed on the packaging, but stored in a tamper-resistant chip. This is because we do not want anyone; the key can know the counter access. Unique identification number SID smart meter is also connected to the encrypted message.

Step 2:

C→N: E {{N, Y}m , SID }

When the station controller receives a request, a message to the NCC sends by TLS channel.

Step 3:

N→C: E {M}

If the NCC receives a message from the controller determines, for each SID key serial number for use in the intelligent network approved saved, and frees its data set Y. Then he sends a message to the controller includes a base right key data again only sent over the secure TLS channel. SCC also follows the smart meter is associated with a particular client.

Step 4:

C→I: E {N, KN, KY} m

When the ignition key held controller that can decode received the original request from the smart meter. The message is decrypted station controller sends another message to the smart meter a N random challenge, a new network key and the key device. The message is encrypted by the key indicators.

Step 5:

I→C: E {N} KN

Smart meters by random query encrypt N by KN recognition. CN then used two base station controllers and other certification IED communication.

B. Key update and revocation

Step 1:

C→I: E {Y, N, KN'} KY

The station controller sends a new network key and random nonce encrypted by KY to the IED.

Step 2:

I→C: E {N} KN'

Receipt is confirmed by returning N encrypted by the new KY.

Step 3:

C→I1: E {Y1, N, KN'} KY1

C→I2: E {Y2, N, KN'} KY2

…

C→In: E {Yn, N, KN'} Kyn

Controller sends a new CN. "Each IED key revocation involves the same steps for the case of an Update button.

The new key exchange method combines symmetric and asymmetric encryption, limited to satisfy one side on the other side of the two requirements for security and IT. It provides a powerful and relatively simple solution to this problem, on which side of the smart metering technology today.

IV. CONCLUSION

Smart grid technology has great potential. However, more advanced technology becomes more susceptible to it. Already identified Chip exchange of encryption key security grid as one of the weaknesses in the system. This is not found between stress means for calculating the current use of smart metering gateway overlooking the proliferation of their safety and functional requirements today due to the limited processing power of the optimal solution. We were taking home AV, G.hn and lonely work comparative study, of which the first two allow the use of symmetric cryptography and system are disclosed when calculated for the working restrictions the best choice. We have found that the cap AV technology from home encryption G.hn can offer under design requirements, and it may reduce prices in order to generate the key. Undoubtedly an AV socket family is used to define the most appropriate scene contemporary technology. However, this is limited because it. Only able to their functions in the power line communication environment in other G.Hn and / or orphan works would be more appropriate environments. The new key-exchange program provides a powerful, is relatively easy to provide solutions to the problem of smart metering technology. This is mainly because it is not based on a single unit, it can be very sensitive. In addition, it also provides better accountability. In short, as long as it used symmetric encryption stress meter rule to calculate chip you can secure the best choice for network post smart meters. But the proposed changes in this labor certification system, for example, something the current threat can be mitigated. However, due to the nature of the art, the use of encryption, not all safety problems effectively reduce. Therefore, we must always keep in mind that additional measures should be provided by other security measures.

ACKNOWLEDGMENT

In the name of Allah, the Most Gracious and the Most Merciful. Alhamdulillah, all praises to Allah for the strengths and His blessing in completing this thesis. Special appreciation goes to my supervisor, Dr Sajjad hussain, for his supervision and constant support. His invaluable help of constructive comments and suggestions throughout the experimental and thesis works have contributed to the success of this research. Not forgotten, my appreciation to my co-supervisor, Prof Dr. Naveed Bin Raees for his support and knowledge regarding this topic.

REFERENCES

[1] Federal Energy Regulatory Commission. Assessment of Demand Response & Advanced Metering. [Online] December 2008; Available from: http://www.ferc.gov/legal/staff-reports/12-08-demandresponse.pdf

[2] Fuloria Shailendra, Anderson Ross, Alvarez Fernando, McGrath Kevin. Key Management for Substations: Symmetric Keys, Public Keys or No Keys? [Online] March 2011; Available from: www.cl.cam.ac.uk/~rja14/Papers/IEEE-PSCE-1.pdf

[3] The Smart Grid Interoperability Panel. NISTIR 7628 Guidelines for Smart Grid Cyber Security. [Online] August 2010; Available from: http://www.egov.vic.gov.au/focus-on-countries/north-and-southamerica-and-the-caribbean/united-states/trends-and-issues-unitedstates/ information-and-communications-technology-unitedstates/cyber-security-united-states/nistir-7628-guidelines-for-smartgrid-cyber-security.html

[4] Gregory Peter. CISSP Guide to Security Essentials; 2009

[5] Greeson Jennifer. Cisco Outlines Strategy for Highly Secure, Smart Grid Infrastructure. [Online] 2009; Available from: http://newsroom.cisco.com/dlls/2009/prod_051809.html

[6] S.W. Smith, Cryptographic Scalability Chanllenges in the Smart Grid, In Proceedings of the IEEE PES Conference on Innovative Smart Grid Technologies, 2012.

[7] Battaglini, Lilliestam J, Bals C, Haas A. The SuperSmart Grid. [Online] June 2008; Available from: http://www.germanwatch.org/klima/ssg08.pdf

[8] M.M. Fouda, Z.M. Fadlullah, N. Kato, L. Rongxing and S. Xuemin,Towards a light-weight message authentication mechanism tailored for Smart Grid communications, In Proceedings of IEEE Conference on the Computer Communications Workshops, 2011.

[9] H. Nicanfar, A tailored authentication and key management for smart grid, IEEE System Journal, 2013.

[10] C. Bekara, T. Luckenbach and K. Bekara, A Privacy Preserving and Secure Authentication Protocol for the Advanced Metering Infrastructure with Non-Repudiation Service, In Proceefings of ENERGY 2012, 2012.

[11] Morris Dworkin. NIST. Recommendation for Block ipher Block of Operation. [Online] 2001; Available from: http://csrc.nist.gov/publications/nistpubs/800-38a/sp800- 38a.pdf

[12] HomePlug Power Alliance. HomePlug Power Alliance Official Website. [Online] Available from: www.homeplug.org

[13] Lonworks™. Lonworks Official Website. [Online] Available from: http://www.echelon.com/communities/energycontrol/developers/lonworks/

[14] Copper Gate. G.hn. [Online] Available from: http://www.coppergate.com/solutions/g.hn/

[15] Oksman Vladimir, Gali Stefano. G.hn: The New ITU-T Home Networking Standard; October 2009

[16] Dvorak John, An introduction to G.hn security, [Online] Available from: http://blog.ds2.es/ds2blog/2009/09/introduction-ghnsecurity.html

[17] International Telecommunication Union. ITU-T X.1035, Available from: http://www.copper-gate.com/solutions/g.hn/

[18] Home Grid Forum. Home Grid Forum Official Website. [Online] Available from: http://www.homegridforum.org/

[19] Newman R, Gavette S, Yonge L, Anderson R. Protecting Domestic Power-line Communications. Symposium On Usable Privacy and Security (SOUPS). [Online] July 2006; Available from: http://www.cl.cam.ac.uk/~rja14/Papers/homeplug-soupspaper.pdf

