ISSN No. 0976-5697

Volume 8, No. 5, May – June 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Review on Smart Grid Attacks and their Countermeasure using Cryptography Algorithms

Sumandeep Kaur
Research Scholar
Department of Computer Engineering
Punjabi University, Patiala, Punjab, India

Supreet Kaur
Assistant Professor
Department of Computer Engineering
Punjabi University, Patiala, Punjab, India

***Abstract*:** There are various technologies that are being used in many fields. With the advancement of technology existing electrical grids are converting into smart electrical grids. A smart grid is an evolved grid system that manages electricity demands in a sustainable, reliable and economical manner built on advanced infrastructure and tuned to facilitate the integration of all operations. Smart grid has effective power management, secure communication and environment friendly. But smart grid has complex architecture because there are various vendors who are involved in this. So, the biggest problem is authentication, authorization and integrity. Second problem is how to provide security for communication lines from various types of attacks. In this paper, a survey is done on various cryptographic algorithms which are used for security in smart grid. On the basis of survey, various security issues are discussed in smart grid. It has been found that lightweight algorithm is more appropriate for smart meters for less memory usage and power consumption.

Keywords: smart grid, smart meter, attacks, security, cryptography.

I. INTRODUCTION

In last few years due to load unbalancing there is wastage of electricity and due to user affected. This is also cause of wastage of money. Power grids are changed into smart grid because smart grid provides two way communications between user and supplier. A traditional grids focus on only transmission, generation and distribution of electricity. It is also provide one way communication which is not effective. Smart meters are major component for smart grids. Smart grid involve various kind of sensors in smart meters which deliver user's real time electricity usage and manage and produce demand from central unit. Also smart meters provide balance between generation and consumption and effective power management

[1].A. Overview of Smart Grid Architecture

fig1. Shows the smart grid is an order in which three layers are involved. At the bottom layer Home area network (HAN), Industrial area network (IAN), Business area network (BAN) presented which are either wire or wireless connected with smart meter. Smart meter are responsible for provide users electricity usage information to grids. The middle layer include Neighborhood area network (NAN) which combine all the small geographic area smart meters and responsible for different distribution. The third upper layer contains SCADA (Supervisory control and data acquisition) master station. SCADA is the brain of smart grid. The electrical infrastructure is mostly depending on the SCADA system that is responsible for monitor and control all the function of grid. In the monitoring they check the load balancing on the transmission lines so that load unbalancing never occur. Second under the control according to demand they forecast future plan for electricity generation[2].

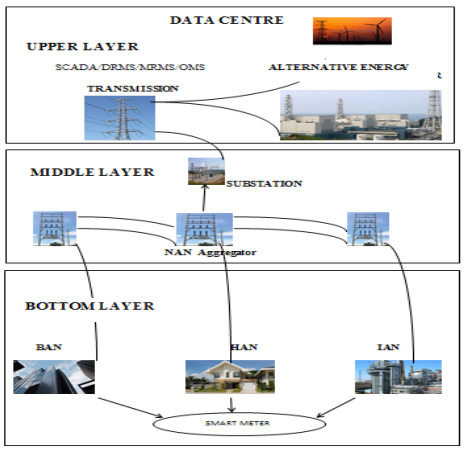

Figure 1: Smart Grid Architecture

All three layers communicate with each other. The main elements of SCADA master station are human Machine Interface, application server and communication front end, firewall etc. There are three major components that make up the grid: electrical transmission system which transfers energy from power plants to distribution substations located near to population center. In Distribution system it is the final stage of delivery network and refers to delivery of electricity from distribution substation to end consumers. All three layers communicate with each other. Other modules of smart grid are DRMS (Demand resource management system), OMS

B. Attacks on Smart Grid

(Outage management system) which enable effective management of faults and incidents power network. Demand resource management system also used to optimize and schedule resources at time of peak demand. This usually determines the best possible way to provide load balancing at peak generation.

Table 1: Comparative of Attacks on Smart Grid

S.no.	Active attacks	Passive attacks
1	In active attacks, the unauthorized parties are according to their demands can modify messages or misuse of the system resources when two parties are communicating.	In general, when two parties are communicated third party silently listens your message without damaging your system resources
2	Examples of active attacks are Masquerade attack, Dos, Session replay attack, message modification attack etc.	Examples of passive attacks are Eavesdropping ,traffic analysis etc.
3	In Masquerade attack, the intruder pretends to be a specific user of a system to achieve access or to achieve greater privileges than they are authorized for. A Denial of service attack aims to break up the availability of communication resources of system.	Eavesdropping is an attack to capture the unauthorized information which is confidential.
4	In Session replay,hackers takes an authorized user's log in information by taking the session ID and in message modification attack involve remodeling of the content of an original message for produce an unauthorized access.	In traffic analysis the unauthorized parties are monitoring of your electricity loads information for some physical attack.

C. Need of Security for Smart Grid

Due to different types of attacks some design goals are nominated for provide security to smart grid. These goals are:

- Confidential
- Authorization
- Integrity
- Non repudiation
- Authenticity

D. Overview of Cryptography Algorithm for Smart Grid

Smart grid has complex architecture and various stakeholders which makes authenticity and authorization a big challenge in smart grid security. To fulfill the design goals of smart grid various cryptographic algorithms are used to securecommuni-cation .Cryptography is the process of hiding information by encrypting the message. In cryptography some random key and encryption algorithms are applied on plaintext to produce cipher text. So it is the process to encrypt the plaintext to cipher text using secret key so that the message should be read by intended receiver with privacy. Cryptographic algorithm addresses the problems which are related to authentication, privacy and integrity and provide various aspect of security such as confidentiality and integrity for the information exchanged over network. Confidentiality means information should be secret that is provided by encryption algorithm.
Integrity means information is send by the intended receiver and no changes are made to the information when it is transferred over the channel. Integrity is provided by the authentication algorithm with key-hashed functions, block ciphers and more recently with the stream ciphers.
Cryptographic algorithms are of two types that is symmetric key cryptographic algorithm and asymmetric key cryptographic algorithm.

Cryptography algorithms are classified in two terms based on keys:
Symmetric Algorithms: In Symmetric algorithm same key is used for encryption and decryption purposes like AES, HIGHT, PRESENT*etc*. So, in symmetric algorithm key is also shared on the network with cipher text. This key is kept secret among sender and receiver so that no intruder can steal the data to be transferred by encrypted. Symmetric key cryptographic algorithm is further categorized into two parts named as Stream cipher and block cipher. Block ciphers are the ciphers which permutes N-bit blocks of plaintext with the secret key and output the N-bit blocks of cipher text. Stream cipher works serially by producing the pseudorandom bits, the key stream bits. The key stream is XOR with the plaintext to produce the cipher text.
Asymmetric Algorithms: Asymmetric algorithm is also called public key system that use two keys, public key is announced publically and private key that is secret key for user. In Asymmetric algorithm different keys used for encryption and decryption purposes like RSA, ECC etc.

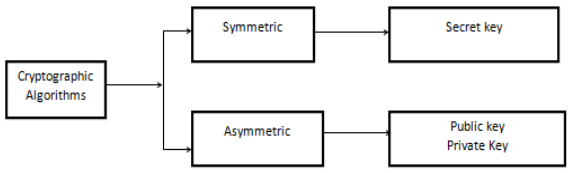

Figure 2: Classification of Cryptographic Algorithms

This Paper structured as section 2cover the literature survey part .In this various types of algorithm are surveyed which provide secure communication for smart grid.Section 3 cover conclusion that report reults of this paper.

II. LITERATURE SURVEY

In the literature survey discussed the symmetric and asymmetric algorithms used in smart grids for secure communication. Also, some new approaches are survey because of their good performance.

[4]This paper discuss about the security of two way communication between smart meter and neighborhood gateway. This also proposed a lightweight authentication scheme for smart grid to provide security and in this scheme Exclusive or operation is used for encryption. Langrage interpolation formula is used for authentication. This paper concludes that all algorithms require very less memory and provide good performance.

[5]In this paper secure anonymous key distribution scheme is proposed for smart grid. In this scheme a smart meter can anonymously access provided services using one private key without the help of trusted anchor during authentication. It also discussed about working of identity based signature and encryption scheme used for key distribution between smart meter and service provider in smart grid.

[6]This paper presents a secure data communication protocol for data collection because secure, efficient and scalable data collection becomes a big challenging task. DCs (Data Collectors) collect data and convey it securely from measurement devices to the power operators. Smart grid has complex architecture so authentication and authorization is required for communication. DNP (Distributed network protocol) is of main concern which is used in SCADA. This paper implements RSA algorithm to create and verify signature and parameter in their system to optimize the time.

[7]This explained the today's growth of deployments of smart grid systems that is a large quantity of energy usage and grid status data have been collected by smart meters. In smart grid data communication networks many authentication protocols have been proposed to control access on smart grid devices; but most of time, authentication protocols control readings from meters are mostly ignored. In this paper, they proposed a secure and efficient framework to enable secure data readings from the isolated smart grid devices based on a two-phase authentication protocol. The framework with the use of the smart reader as a bridge for isolated smart grid device connections make use of smart grid cloud, but considers the systems physical constraints. Security analysis shows that under most typical attacks our framework is efficient and secure; meanwhile it satisfies the hardware constraints of smart grid devices. Performance evaluation validates the efficiency of this framework.

[8]This mentions the existing security issues and designed a security situational awareness mechanism in smart grid based on the analysis of big data. To perform analysis in smart grid the Fuzzy cluster based analytical method; game theory and reinforcement learning are integrated. The simulation and experimental results show the advantages, one is high efficiency and other is low error security situational awareness rate.

[9]This paper contributes an efficient and lightweight attack detection procedure for a smart grid Neighborhood Area Network (NAN) which is combination of distributed and centralized intrusion detection. A NAN consist customers' appliances, smart meters and collectors. Power consumption of each application is measured and the collectors integrate the measures and moved to control center where analysis done. In their framework, Intrusion Detection System (IDS) agents, run at smart grid levels in distribution and in centralized fashion at collector side and on nodes of control center. Integration between a rule-based detection and a learning algorithm for training and classification is bring to detect intruders that required either injecting false measurements or exhausting the energy of the grid, or inject Denial of Service (DoS) attacks. Simulation results confirm that sophisticated attacks are detected with less energy consumption by current cyber detection mechanisms using intruder detection framework.

[10]This proposed an effective way of QTL ultra-lightweight algorithm with resource constraint. QTL algorithm works in Feistel network. The merits of QTL algorithm is changing the message blocks in an recursive way as it change half block of message as compare to traditional way. To decrease the energy consumption of hardware components in the security process key scheduling is never used.

[11]Explained the small micro electrical mechanical systems of wireless sensor networks are implemented and communicate data in environment. WSNs can be used for monitoring and control of smart grid assets. Based on communication network security is a major concern for researchers and developers. Less processing capabilities of wireless sensor networks makes more exposed to cyber-attacks. The countermeasures in oppose to cyber-attacks make easy and form ability to offer confidentiality, data readiness and integrity. The address concern design and development method for network communication need a procedure to design data oriented WSN architecture. WSN security is an inevitable part of smart grid cyber security. This paper serves the analysis of communication standards, issues of cyber security and solves the WSN based smart grid infrastructure.

[12]Security and privacy are concerned in the context of the smart grid. Existing security methods are developed for systems of traditional information technology. These traditional can be used for designing security measures for the smart grid. However, latest methods meet the essential requirements and features of the smart grid. Instead of the restriction opposes on developing detailed security solutions for the future smart grid, complexity of the architecture and practical knowledge lacks in security. They review on the existing literature on different security aspects of the smart grid and provide directions for further research.

[13]Firstly, explained the use of WSNs for SG applications and also contributes the security issues and security threat challenges. In spite of this, they proposed security mechanisms for WSN-based SG applications are discussed. Finally, simple and easy working of this attack detection framework directed to sink and gateway nodes to web interface purposed and cases study has been done for efficiency.

III. CONCLUSION

In this paper different cryptographic algorithms and approaches are surveyed and concluded that Smart grid is the modern generation of power grids and become a pivot point of attacks. Smart meters are used in smart grids for provide real time electricity information, have less memory and area so lightweight algorithms are preferred in smart grid. Numerous types of attackers down the overall system performance, therefore it is essential to set constraints for security of system. for this purpose this paper also describes cryptographic algorithms used for obtaining design goals of smart grid. Symmetric algorithm is used for encryption process and asymmetric algorithms are used for authentication purpose.

REFERENCES

1. G, W.: Challenges and opportunites in smart grids. IEEE 99 (january 2011)
2. N. Komninos, E.: Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures. IEEE (2013)
3. He, , Chen, , Bu, , Chan, , Zhang, , Guizani, : Secure Service Provision in smart grid communications. IEEE (2012)
4. Liu, Y., Gu, T., Jiang, T., Li, X.: A lightweight Authenticated communication for smart grid. IEEE (Feberaury 2015)
5. Tsai, J.-L., Lo, N.-w.: Secure Anonymous Key Distribution scheme for smart grid. IEEE (2015)
6. Suleyman Uludag, K.-S.: Secure and Scalable Data Collection With Time Minimization in the smart grid. IEEE (2015)
7. Sha, K., Alatrash, N., Wang, Z.: A secure and efficent frame work to read isolated smart grid devices. IEEE transaction on Smart Grid (February 2016)
8. Wu, J., Dong, M., Ota, K., Li, J., Wang, H.: Big Data Analysis Based Security Situation Awareness For Smart Grid. IEEE transction on Big Data (October 2016)
9. Sedjelmaci, H., Senouci, S.: Smart Grid security: a new approach to detect intruders in a smart grid neighhborhood area network. In : International Confernece on Wireless network and Mobile communication (2016)
10. Li , L., Liu, B., Hui, W.: QTL: A new ultra-lightweight block. Elsevier Journal of Microprocessors and Microsystems (2016)
11. Chhaya, L., Sharma, P., Bhagwatikar, G., Kumar, A.: Wireless sensor network based smart grid communication: Ciber attacks,Intrusion Detection System and Topology Control. Journal of Electronics (December 2016)
12. Joker, P., Arianpoo, N., Leung, V.: A survey on security issues in smart grids. Security and Communication Network (2012)
13. Tuna, G., Orenbas, H., Das, R., Kogias, D., Baykara, M., Gulez, K.: Information Security threats and an easy-to-Implement attack detection framework for wireless sensor Network-based smart Grid Applications. IOP conference on series: Materials Science and Engineering (2016)