A Novel Technique for Smart Grid Wireless Communication

Mr. Mohan Khedkar[1] Prof. Vijay Shelake[2]

[2]Head of Department

[1,2]Department of Computer Engineering

[1]SES GOI Faculty of Engineering [2]TYCEM, University Of Mumbai, Mumbai

Abstract— Smart grid communication has recently received significant attentions to facilitate intelligent and distributed electric power transmission systems, but also introduces many security problems. In this paper the concept of dynamic secret is applied to design dynamic secret based authentication and encryption scheme for smart grid wireless communication. Between two parties of communication, the previous packets are coded as retransmission sequence, where retransmitted packet is marked as "1" and the other is marked as "0." During the communication, the retransmission sequence is generated at both sides to update the dynamic encryption key. Any missing or misjudging in retransmission sequence would prevent the adversary from achieving the keys. In addition with this we introduce a new protocol, Integrated Authentication and Confidentiality (IAC), to provide efficient secure AMI communications in smart grid. With the help of IAC, an AMI(Advanced Metering Infrastructure) system can provide trust services, data privacy, and integrity by mutual authentications whenever a new smart meter initiates and joins the smart grid AMI network.

Keywords: Authentication, Confidentiality, Dynamic secret, Encryption, Retransmission, Security, Smart Grid

I. INTRODUCTION

Recently, smart grid (SG) is the buzz word, which has attracted attentions from engineers and researchers in both electric power and communication sectors. The concept of SG has appeared in recent literature in different flavors. Some referred to it as intelligent grid whereas some called it the grid of the future. The objective of the SG concept remains more or less the same, namely to provide end users or consumers with power in a more stable and reliable manner. SG incorporates a two-way communication between the provider and consumers of electric power. The two-way communication indicates the ability of SG to enable the end users to express their power requirement demands to the utility provider. The electrical power industry is in the process of integrating its distribution system with communication networks and control techniques to form a bidirectional power and information flow infrastructure, commonly called a smart grid.[1] The smart grid (SG) is considered as a desirable infrastructure for energy efficient consumption and transmission, where the built-in information networks support two-way energy and information flow, facilitate significant penetration of renewable energy sources into the grid, and empower consumer with tools for optimized energy consumption.[2] The use of wireless technologies in the grid for applications such as system monitoring, metering, and data gathering goes back several decades, but they have the potential to be used to a much greater extent as utilities deploy the infrastructure for the smart grid.

Various types of attacks targeting industrial control systems (ICSs) and information technology systems (ITSs)

as well as different performance requirements of these traditional information systems determine a specific priority order for the security services implemented for smart grid wireless communication systems. The advanced wireless metering infrastructure (AWMI) refers to the systems that collect, measure, and analyze energy usage from networks that are connected to next-generation electricity meters, or so-called smart meters. Smart meters communicates with control central to send and receive electricity usage information, billing information etc..[1]Smart Meters is the source of metrological data as well as other energy related information. This smart meter provides internal data for customer loads as well as distributed generation.[8]Concurrent with this evolution in metering is the development of home area networks (HAN)composed of devices that communicate with one another and can communicate data to utilities (or other energy service providers) and can receive and respond to signals sent by these remote entities. An overarching vision of the Smart Grid holds that providing consumers with information about their energy usage will support an array of electricity pricing models and enable customers to better control their electricity use.
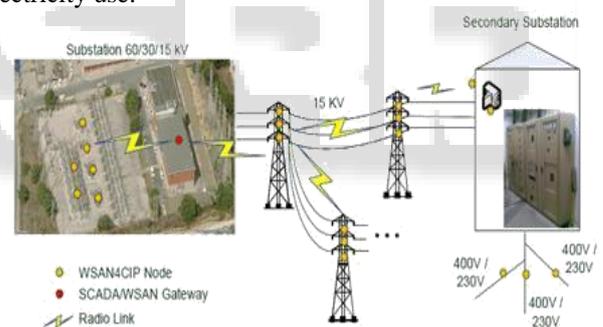

Fig. 1: Wireless Network for Electrical Distribution of Power Grid [6]

II. RELATED WORK

In the century since residential electrical service started to become a ubiquitous feature of life, the details of how households consume electricity have largely remained inside the home. Electromechanical meters have kept track of total electricity usage. These meters did not record or reveal who used electricity, when, or where, nor did they allow energy consumption to be noted in real-time. All of this is changing as digital "smart meters" become part of energy infrastructure. Smart meters, as components of the advanced metering infrastructure (AMI), serve a broader effort to construct a "Smart Grid" by integrating information technology into electricity generation, transmission, and distribution. According to the Federal Energy Regulatory Commission (FERC), as of September 2009, there were approximately eight million advanced meters installed nationwide; FERC expects that number to reach 80 to 141

million by 2019.5 In California, the three major investor-owned utilities (IOUs) are in the midst of deploying smart meters for electricity; they plan to deploy approximately 12 million electric meters by the end of 2012.[7]

Concurrent with metering is the development of home area networks (HAN) composed of devices that communicate with one another and can communicate data to utilities (or other energy service providers) and can receive and respond to signals sent by these remote entities. An overarching vision of the Smart Grid holds that providing consumers with information about their energy usage will support an array of electricity pricing models and enable customers to better control their electricity use (or authorize a third party to do so).[7]

One end of the design spectrum would rely largely on one-way transmissions of price and event information to customers; energy management systems within customers' homes or businesses would then control networked devices based on these signals and the customer's preferences. [7] At the other end of the spectrum is a Smart Grid that depends on two-way communications between home devices and utilities or other service providers. In this two-way architecture, a home area network (HAN) gateway enables not only communications between devices inside the home and service providers but also remote control of HAN devices . Other architectures are feasible, too.[7]

The California Public Utilities Commission has chosen to promote technologies and business models that embrace intensive two-way communications. The CPUC approved utilities' requests to include HAN gateways in their smart meter deployments. The CPUC reasoned that doing so would provide "the most cost effective way . .over the long term" of realizing the benefits of "enabling price signals, load control and near real time data for residential electric customers." Given the combined size of the major California IOUs' deployments and California's advanced state of Smart Grid activity relative to other states, these decisions are likely to influence other states. Federal policy could provide additional support to this influence. [7]

III. METHODOLOGY

One possible solution for security issues is to apply standard security techniques which provides authentication, encryption–decryption , data integrity. For example: Public key encryption, symmetric key encryption etc. There are certain limitation of these standard techniques which are solved in *Dynamic Secret Based Encryption Scheme*. The Limitations are as follows:[2]

1) Low-Cost: The cost is the first priority of the users and suppliers. In order to be cost effective, the computational power, memory and storage of the smart devices are limited. It leads to severe restriction on modern security techniques, such as:complicated cryptographic algorithms may exhaust all computation and storage resource of units;third party applications, such as private key generator, may visibly increase the cost of whole wireless system.

2) Low-bandwidth: The communication channels in lower distribution and consumption grids are designed to transmit short message, and require only low bandwidth. Integrity protection

mechanisms such as cipher-based message authentication code (CMAC) add typically 64 to 96 bits to every message. This leads to a high overhead in such a channel and might cause latency which is not affordable in many applications in SG. Distributed IDS can detect and classify malicious data and possible attacks by monitoring the communication traffics on many modules with doubled traffic flows, but might exhaust the bandwidth on these modules.

3) Easy-maintenance: The wireless networks in SG should be flexible and easy to manage. It would be unrealistic to hire hundreds of engineers to manage users' encryption keys and change battery.

4) Proposed Scheme:To overcome limitation and meet AMI security requirements we propose a Novel Technique for Smart Grid Wireless Communication. We use Dynamic Secret based Authentication and Encryption. These include three phases:

– Phase I: Generate DSE Key for SG Wireless Communication [2]

Dynamic secret was developed for securing wireless communication. The basic idea of dynamic secret is that the legitimate users dynamically generate a shared symmetric secret key utilizing the inevitable transmission errors and other random factors in wireless communication. In the fig we firstly introduce the basic algorithms of dynamic secret; and then present the DSE scheme.

A. Dynamic Secret:

The sender and receiver monitor the error retransmission in link layer to synchronously select a group of frames. These frames are hashed into dynamic secret to encrypt the data. This part is a brief introduction of dynamic secret.
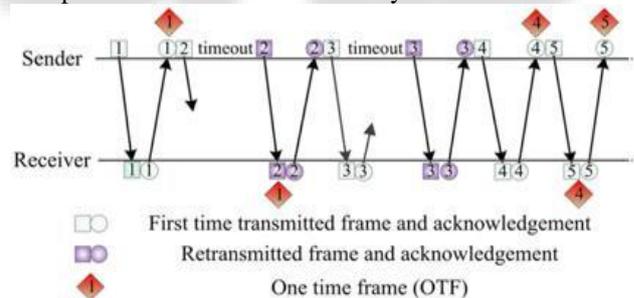

Fig. 2: SW protocol and OTF Identification

1) Retransmission Analysis/OTF Set Generation:

On the link layer's communication, error retransmission happens unavoidable and randomly at both side of the sender and the receiver. According to Stop-and-Wait (SW) protocol, the sender transmits a frame and waits for the corresponding acknowledgement before sending a new frame. If a frame is only transmitted once and its acknowledgement frame is received in time, this frame is named as one time frame (OTF). As shown in Fig.2, the packet 1 is confirmed as an OTF on the sender until the acknowledgement of packet 1 is received; it is confirmed on the receiver until the second packet is received. It will be added into OTF set . Both the transmitted frame (packet 2) and acknowledgement (packet 3) are retransmitted, thus they are not added into OTF set.

2) Dynamic Secret Generation:

Once the number of OTF set reaches the threshold, the sender and receiver agree on a uniformly random choice of universal-2 hash functions to compress into the dynamic secret DS(k) . Then, the is reset to empty. It is proved that DS(k) will fully retain the adversary's information loss.

3) Encryption/Decryption:

When a new dynamic secret is generated, it will be applied to update the encryption key at both sides of communication. This symmetric encryption key is used to encrypt the data at sender and decrypt the cipher at receiver. To reduce the computation consumption, the XOR function is used for encryption and decryption.

B. DSE Scheme for Smart Grid Wireless Communication:

Dynamic secret-based encryption (DSE) scheme is designed to secure the wireless communication between the smart devices and control center. The framework of DSE scheme is shown in Fig. 3, consisting of retransmission sequence generation (RSG), DS generation (DSG), and encrypt/decrypt.
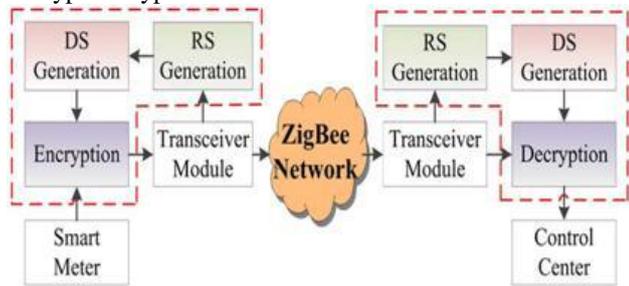

Fig. 3: Framework of DSE Scheme

1) DSE Algorithm:

– RSG: This module is applied to monitor the link layer error retransmission. The communication packets which have been retransmitted are marked as "1" and the non-retransmitted packets are marked as "0." The pervious packets are coded as0/1 sequence , named as retransmission sequence (RS).In DSE, RS is applied to replace the OTF set for dynamic secret generation due to the limitation of computation capability and storage resources.

– DSG: Once reaches the threshold L_RS (length of RS),it would be compressed to a DS in DSG module. Considering the limitation on computation power, the hash functions f_{hash} are recommended in DSG module.

$$DS(k)= f_{hash}(L\_RS)----------(1)$$

– Encrypt/Decrypt*:* The new dynamic secret DS(k) is applied to update the dynamic encryption key (DEK) by

$$DEK(k)=DS(k)\ EX\text{-}OR\ DEK(k\text{-}1)--------------(2)$$

DEK(k) is generated at both sides of communication synchronously. The sender applies it to encrypt the DATA and the receiver applies it to decrypt the CIPHER. XOR function, as one of the most light-weight and easy-implementation algorithm, is applied to update the DEK and encrypt/decrypt the data on both sides. If DEK is shorter than the data, DEK(k)is replicated and padded circularly to generate DEK*(k) whose length is equal to the raw data or cipher text.

– Phase II: Initialization Process and Authentication [1]

Fig.4. illustrates the initialization process for each new smart meter as a supplicant. Before joining the AMI network, each new smart meter must be verified by the remote authentication server located at the local management office as alegal device and terminal customer. The neighboring authenticated smart meters can play as authenticators in the initialization process and relay the authentication process messages between the supplicant and the authentication server. Both the supplicant and the authentication server have an identical key K, which was pre-installed, not concealed to anyone else including the authenticator. Both the mutual authentication identities and the consequent data encryption/decryption between supplicant and authentication server are based on k.If the supplicant's identity is authenticated as a valid device, the corresponding credential of the supplicant is established between the authentication server and the supplicant. Then, the authentication server will generate an initial vector (IV) and a key k. The IV and k will be encrypted by K, denoted as EK(IV‖k) as shown in Fig.4. So the supplicant can decrypt and get its IV and k. Meanwhile, the authentication servers ends k to the authenticator encrypted with their own K¢denoted as EK¢(IV‖k) since the authenticator was authenticated already with K¢. So the authenticator knows k. With itsk, the supplicant and authenticator can individually generatekn–1,n, which is the symmetric key for message authentication code generation and validation between one-hop neighboring nodes n and n − 1 on the data forwarding path. As such, afour-way handshake procedure is established to fulfill another mutual authentication between the supplicant and authenticator. After successful mutual authentication, the key kn–1,natboth the supplicant and authenticator sides is validated and made ready for subsequent message authentication code generation and validation purposes. After the initialization process, the proposed IAC protocol also includes a hop-by-hop data aggregation and forwarding scheme that transmits meter reading and control messages between smart meters and afeeder (collecting node).
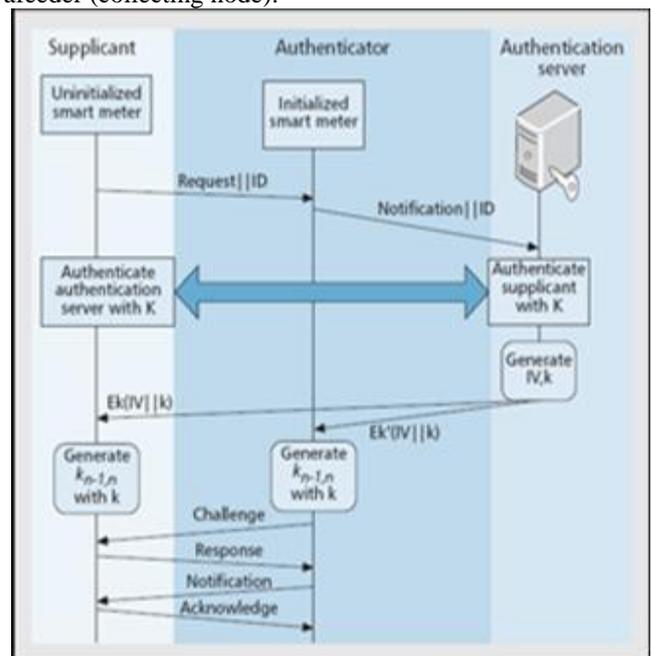

Fig. 4: Initialization Process and Authentication

– Phase III: Data and Control Message Encryption and Communication

Smart Meter collects/receives data/control messages and forwards to control center using encryption/decryption. Since it use DSE each time new key is generated and secured communication takes place.

IV. CONCLUSION

An Efficient Security scheme: Authentication and Encryption for Wireless Smart Grid Communication is designed to secure the wireless communication of SG. To reduce its complexity, the retransmission sequence is proposed to update dynamic encryption key, replacing the OTF set; and MD2 is selected as the hash algorithm. A demo system is developed to investigate the performance of DSE scheme. The newly added node is authenticated by the neighboring authenticated node. It provides mutual authentication between a remote server located in the local management office and a neighboring smart meter as the authenticator to obtain proper cryptography keys for consequent secure data communications. Therefore, readings from smart meters and management messages from central SCADA and/or local management offices can employ encryption and message authentication mechanisms tailored for the security requirements and system constraints. The numerous experiments reveal that: 1) the DSE scheme can protect the users against eavesdropping by updating the dynamic encryption key with retransmission sequence in communication, even the attackers know the details of DSE scheme and obtain the encryption key at some time; 2) it is a light-weight encryption method with only simple operations, such as MD2 and XOR; 3) it is self-contained, that is, it is dynamically generated during the normal communication without additional traffic and control command; 4) it has good compatibility, which could be integrated with many wireless techniques and applications, such as ZigBee.

REFERENCES

[1] Ye Yan Hu, R.Q. ; Das, S.K. ; Sharif, H. ; Yi Qian , "An Efficient Security Protocol for Advanced Metering Infrastructure in Smart Grid", Network IEEE,vol.27,2013.

[2] Ting Liu, Member, IEEE, YangLiu, YashanMao, Yao Sun, XiaohongGuan, Fellow, IEEE, Weibo Gong, Fellow, IEEE, and Sheng XiaoA, "Dynamic Secret-Based Encryption Scheme for Smart Grid Wireless Communication", IEEE 2013.

[3] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," IEEE Security Privacy, vol. 7, pp. 75–77, 2009.

[4] M. M. Fouda, Z. M. Fadlullah, N. Kato, L. Rongxing, and S. Xuemin, "A lightweight message authentication scheme for smart grid communications," IEEE Trans. Smart Grid, vol. 2, pp. 675–685, 2011.

[5] R. Metke and R. L. Ekl, "Security technology for smart grid networks," IEEE Trans. Smart Grid, vol. 1, pp. 99–107, 2010.

[6] AWireless Sensors Suite for Smart Grid Applications. António Grilo1, Helena Sarmento1, Mário Nunes1, José Gonçalves2, Paulo Pereira1, Augusto Casaca1.pdf.

[7] "PRIVACY IN THE SMART GRID: AN INFORMATION FLOW ANALYSIS" Prepared forCIEE By:University of California, Berkeley, Deirdre K. Mulligan, Longhao Wang, Aaron J. Burstein, March, 2011.

[8] "Smart Grid Cyber Security and Potential Threats, Vulnerabilities and Risk", University of California, May 2012.

[9] "The smart grid: An introduction," in DOE's Office of Electricity Delivery and Energy Reliability 2008.

[10] Y. Ye, Q. Yi, and H. Sharif, "A secure data aggregation and dispatch scheme for home area networks in smart grid," in Proc. 2011 IEEEGlobal Telecommun. Conf., pp. 1–6.

[11] Cisco,, "Security for the smart grid," 2009, White Paper[Online].Available:http://www.cisco.com /web/strategy/docs/energy/white_paper _c11_539161.pdf.

[12] W. Xudong and Y. Ping, "Security framework for wireless communications in smart distribution grid," IEEE Trans. Smart Grid, vol. 2, pp. 809–818, 2011.