SECURE SMART GRID WIRELESS COMMUNICATION

By Shweta Satao

Abstract

Smart-grid metering and control systems hold enormous promise for improving efficiency, convenience, and sustainability. However, the complicated and heterogeneous system architecture has made securing the smart grid particularly challenging. Cyber security in the smart-grid metering and control system is an important and rapidly evolving area that has attracted attention from government, industry, and academia. It introduced the high-level architecture of a smart-grid metering and control system, detailed the system's security requirements, summarized the recent efforts from industry and academia, and highlighted several areas and directions for further research. Moreover, the design of security solutions should take into account the salient features of the smart grid as well as the underlying power system. so we need to focus on the communication-security aspect of a smart-grid metering and control system from the perspective of cryptographic techniques.

Keyword

Smart-grid, Cyber security, Cryptographic techniques

Objective

The objective is to shed some light on cyber security in the smart grid and to trigger the close collaborations among government, industry, and academia.

Introduction

Smart grids – add communication capabilities and intelligence to traditional grids. Smart Grid is the integration of advanced metering, communications, automation, and information technologies on the electric distribution system to provide an array of energy saving choices and integration of distributed generation while lowering operating costs and maintaining or improving service. A Smart Grid system could be the enabling technology to allow curtailment of electric usage at critical times, thus, reducing peak demand by not using the most expensive energy sources.

This electric grid delivers electricity from points of generation to consumers, and the electricity delivery network functions via two primary systems: the transmission system and the distribution system. The transmission system delivers electricity from power plants to distribution substations, while the distribution system delivers electricity from distribution substations to consumers.

Building the smart grid means adding computer and communications technology to the existing electricity grid. With an overlay of digital technology, the grid promises to operate more efficiently and reliably. It can also accommodate more solar and wind power, which are inconsistent sources of energy that can become more reliable with better controls. Much like computers and routers manage the flow of bits on the Internet, smart-grid technologies use information to optimize the flow of electricity. The term ‘Smart Grid’ does not have a precise definition and there are not exact specifications for the quantity or arrangement of components that make up the Smart Grid deployment, including the equipment, devices, software, processes and procedures required to make the Smart Grid operational in the various unique geographical and cultural locations. The Smart Grid can best be described in terms of the following functionalities:

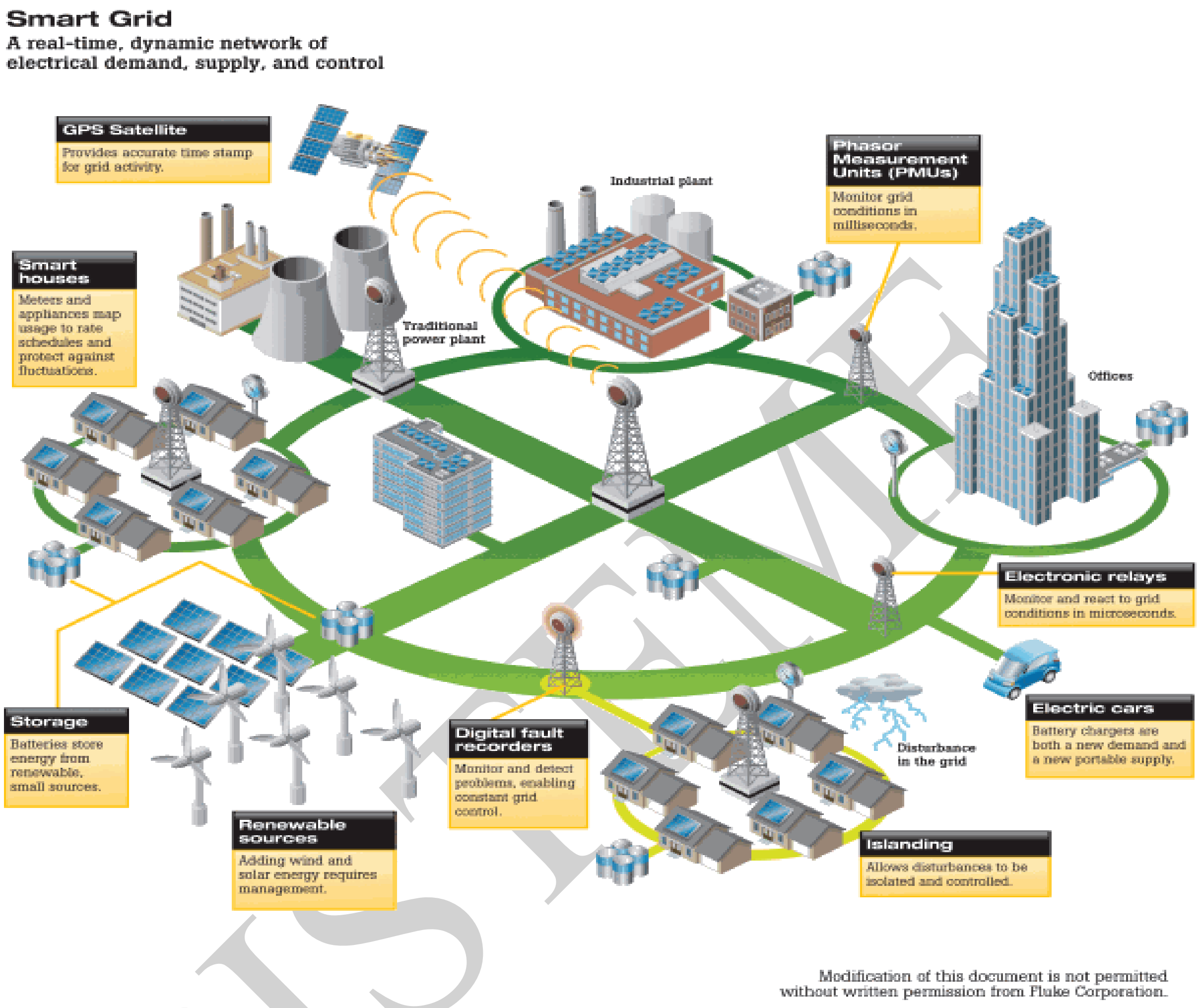
- The ability to develop, store, send and receive digital information concerning electricity use, costs, prices, time of use, nature of use, and storage, to and from the electric utility system.
- The ability to program any end-use device such as appliances and heating, ventilating and air conditioning (HVAC) systems to respond to communications automatically.

- The ability to sense and localize disruptions or changes in power flows on the grid and communicate such information instantaneously and automatically for purposes of enabling automatic protective responses to sustain reliability and security of grid operations.

Architecture of Smart Grid

A smart grid is not a single upgrade to the electric transmission and distribution systems but a complete overhaul with 21st century infrastructure, metering and communications technologies. Smart grid technologies take advantage of much advancement used today, including geographical information systems and wireless communication as shown in fig.1.1. Each part of the smart grid brings its own system and societal benefits with the goal of improving how electricity is delivered and used.

The interactivity allowed with the smart grid also will help consumers make decisions about when they use energy to save money. By making the choice to use electricity during times of the day when others are not, consumers can take advantage of hours with cheaper energy costs, and avoid hours with higher energy costs.


Smart Grid
A real-time, dynamic network of electrical demand, supply, and control
GPS Satellite
Provides accurate time stamp for grid activity.
Smart houses
Meters and appliances map usage to rate schedules and protect against fluctuations.
Traditional power plant
Industrial plant
Phasor Measurement Units (PMUs)
Monitor grid conditions in milliseconds.
Offices
Electronic relays
Monitor and react to grid conditions in microseconds.
Electric cars
Battery chargers are both a new demand and a new portable supply.
Disturbance in the grid
Islanding
Allows disturbances to be isolated and controlled.
Digital fault recorders
Monitor and detect problems, enabling constant grid control.
Renewable sources
Adding wind and solar energy requires management.
Storage
Batteries store energy from renewable, small sources.

Modification of this document is not permitted without written permission from Fluke Corporation.

Fig.1.1 Architecture of Smart Grid

Consumers who chose not to change their usage patterns and continue using electricity during high-cost hours could see their energy costs increase. Consumers also will benefit from increased reliability through a smarter grid. Because a smart grid has the ability to self-heal, momentary outages may occur less frequently and outages related to powerful storms can be significantly reduced.

Smart Grid Wireless Communication

As shown in fig.1.2 the smart grid Communication Infrastructure includes four main components:

- advanced metering infrastructure
- advanced distribution operations
- advanced transmission operations
- advanced asset management.

With these technology improvements, the electrical needs of Ohioans can be met with greater efficiency and reliability and will allow more widespread use of renewable energy to help offset carbon emissions. Of these four, the advanced metering infrastructure will most directly include consumers. The advanced metering infrastructure will enable direct two-way communication between a utility and the customer that will provide a variety of information, such as real-time pricing and usage information over certain time periods. The advanced meters will enable customers to respond to real time electricity prices and allow better management, monitoring and control of energy use in their homes.

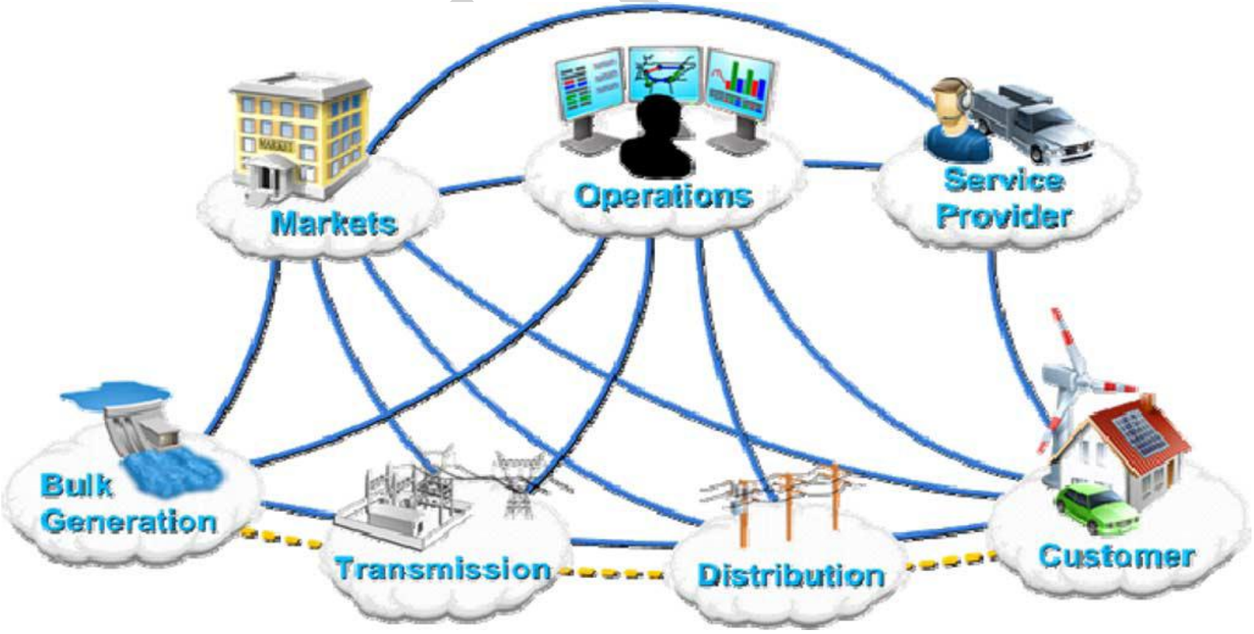


Fig.1.2 Architecture of communication infrastructure

Another common term associated with advanced metering is smart meters. These meters allow real-time pricing tied to customers' electric use, but also have the capability of net metering. Net metering lets customers sell excess electricity back to the utility for a payment, provided they are generating their own power, for example, by using a rooftop solar installation.

The smart grid will allow consumers to better control their consumption which can result in lower energy costs. As more consumers take control of their consumption and costs, improved electric reliability and environmental sustainability will bring more savings to the electricity system. These savings can further reduce electric costs. Electric utilities also will receive operational savings that, in some cases, can make up more than half of the smart meter investment that should be used to help defray the costs passed onto consumers. These are significant and include savings for meter reading, call centers and outage management. Advanced meters also will help utilities and competitive suppliers offer many voluntary rate options that customers can choose to lower their electric costs. The meters will be able to tell consumers how energy is used, what it costs them and what kind of impact that usage has on the environment. To take advantage of lower electricity costs, consumers will need to make adjustments to their electric use or set preferences that will tell the utility to automatically make changes based on those settings. In the near future, consumers will be able to remotely communicate with appliances, thermostats and electronics which will encourage energy efficient decisions that will save money.

Need for Secure Wireless Communication

High-speed, fully integrated, two-way communication technologies that make the smart grid a dynamic, interactive "mega-infrastructure" for real-time information and power exchange also enables cyber security.

Cyber Security: the new communication mechanism should consider

- Security : Network security is a priority and not a add on for smart grids
- Protection of all SG Components: Protecting control centers alone - not enough.
- Secured Remote access to devices.
- QoS requirement from security system
- Safety (line worker public and equipment)
- Reliability and availability

Literature Review

1) Fault-Tolerant and Scalable Key Management for Smart Grid (2011)
Author: Dapeng Wu and Chi Zho

In this paper, we study the problem of secure key management for smart grid. Since existing key management schemes are not suitable for deployment in smart grid, in this paper, we propose a novel key management scheme which combines symmetric key technique and elliptic curve public key technique. The symmetric key scheme is based on the Needham-Schroeder authentication protocol. We show that the known threats including the man-in-the-middle attack and the replay attack can be effectively eliminated under the proposed scheme. The advantages of the new key management scheme include strong security, scalability, fault-tolerance, accessibility and efficiency.

It is known that the ideal case to ensure this once-only semantics is to use a purely random bit sequence as a nonce. The practical compromise is to use a pseudo-random bit sequence for a nonce. However, it is virtually impossible to require a low-power receiver to verify a nonce for the fulfillment of this semantics against all used nonce's in real-time in a large smart grid network. In this paper, we will demonstrate that it is feasible to ensure this once-only semantics at a receiver by combining timestamp and nonce using a pseudo-random bit sequence at a message originator. Since the message originator can simply generate a pseudo-random number with a sufficient number of bits, a nonce collision between two instances is highly unlikely at the message source; for this reason, we focus on ensuring the once-only semantics on the message receiver's side. Next, we present our proposed key management for smart grid.

In this paper, we have studied the requirements on key management for smart grid. A key management scheme is proposed for its use in smart grid and it meets these requirements. The security of the proposed scheme is built on the foundation of a public key infrastructure and the secure Needham-Schroeder authentication protocol. We show that the known threats including the man-in-the-middle attack and the replay attack can be effectively eliminated under the proposed scheme. We also address the issue of additional vulnerabilities on session keys and communication keys via techniques including a strict one-time use rule and on-the fly key generation. The advantages of the new key management scheme include strong security, scalability, fault-tolerance, accessibility and efficiency.

Advantages:

- The advantages of the new key management scheme include strong security, scalability, fault-tolerance, accessibility and efficiency.
- The key management at trust anchors is significantly simplified since there is no need to maintain shared symmetric keys.

Disadvantages:

- For cross realm secure access, data aggregator sends a request to a local trust anchor for a session key for communicating to a remote data aggregator, and the trust anchor in the remote realm will instead issue the actual session key.

2)EPPA: An Efficient and Privacy-Preserving Aggregation Scheme for Secure Smart Grid Communications (2011)
Author: Rongxing Lu, Xiaohui Liang Xiaodong Lin, Xuemin (Sherman) Shen

Smart meters are important components of smart grid. They are two-way communication devices deployed at consumers premise, records power consumption periodically. With smart meters, smart grid is able to collect real-time information about grid operations and status at an operation center, through a reliable communications network deployed in parallel to the power transmission and distribution grid, as shown in Fig. 1. The operation center may be implemented in a distributed way and span different geographic regions. It is responsible for dynamically adjusting power supply to meet demand, and detecting and responding to weaknesses or failures in the power system in real time. Smart grid also automates reliable power distribution by engaging and empowering customers in utility management. It exposes customers' detailed real time electricity use information (through smart meters) to utility companies, which may then change electricity price accordingly or even adjust customers' usage by pre-installed load control switches in order to help flatten demand peaks. Customers are allowed to access their own real-time use information through smart grid services. In order to lower their own energy costs and enjoy uninterrupted activities, they will be willing to use energy-efficient appliances and tend to shift power use from peak times to non-peak times.

In this paper, we have proposed an efficient and privacy preserving aggregation scheme (EPPA) for secure smart grid communications. It realizes a multi-dimensional data aggregation approach based on the holomorphic Paillier cryptosystem. Compared with the traditional one-dimensional data aggregation methods, EPPA can significantly reduce computational cost and significantly improve communication efficiency, satisfying the real-time high-frequency data collection requirements in smart grid communications. We have also provided security analysis to demonstrate its security strength and privacy-preserving ability, and performance analysis to show the efficiency improvement. For the future work, we will study the possible behavior by internal attackers and extend the EPPA scheme to effectively resist such attacks.

Advantages:

- Existing data aggregation schemes regards power use information as one-dimensional information. With smart meters being used, it is however multi-dimensional in nature, for example, including the amount of energy consumed, at what time and for what purpose the consumption was, and so on.
- We further notice that power usage information is often small in size, smaller than the plain text space of the encryption algorithm used.

Disadvantages:

- The communication efficiency of the GW-to-OA communication is still a challenging issue.
- How to aggregate multidimensional data remains to be a challenging issue.

Issues in Smart Grid Wireless Communication

Major reason for this smart grid security research is because of the complexity of the smart grid, the importance of the smart grid as a super-critical infrastructure, and the fact that many reports of potential attacks on the grid have been disseminated in the media. This section should help put some these issues in perspective. However, the primary purpose of this current section is to discuss threats and vulnerabilities, and general security problems. Subsequent section will address controls to mitigate those risks and countermeasures, using best practices; and where best practices are not adequate then we will suggest research topics that need to be addressed in the future to help solve those problems.

Availability

Availability refers to ensuring timely and reliable access to information, which is the primary security goal of a smart-grid metering and control system. Malicious attacks targeting availability can be considered as denial-of-service attacks, which intend to delay, block, or even corrupt the communication in the system. In particular, due to the extensive adoption of wireless communication technologies in the smart grid, a jamming attack that fills the wireless medium with noise signals has become the most typical form of physical-layer attack. The jamming attack is able to defer the transmission of messages and to distort the transmitted data signal. As a result, the legitimate receiver cannot recover messages out of the damaged data packets. Jamming attacks are more relevant and serious in the smart grid than other than other networking systems, because the smart grid involves essential resources for people’s everyday lives. On the other hand, many man-in-the-middle attacks can be launched only when the full or partial communication channels can be jammed. Examples include jamming then inserting false location information and jamming then delaying the transmission. Because the network traffic in the smart grid is generally time-critical, it is crucial to evaluate the impact of denial-of-service attacks and to design efficient and effective countermeasures to such attacks.

Integrity

Integrity refers to preventing or detecting the modification or destruction of information by unauthorized persons or systems. Malicious attacks targeting the integrity of a smart grid attempt to stealthily manipulate critical data such as meter readings, billing information, or control commands. Based on the assumption that an attacker has compromised one or several smart meters and is able to access the current power-system configuration information, such attacks can successfully inject arbitrary bogus data into the monitoring centre, and at the same time, pass the data-integrity checking used in current state-estimate processes. Integrity protection can be achieved by authentication, certification, and attestation. More specifically, the smart devices and substation must authenticate each other's identity to thwart impersonation. Data certification of a message prevents modification of data during transmission. Data authentication with non-repudiation goes beyond certification by preventing the sender from claiming that it did not send the data. Substations use attestation to confirm that the memory contents (code and data) on a smart device have not been modified. The security services related to integrity are usually implemented using public-key cryptography, which requires a trusted third party that hosts a key-management service.

Confidentiality

Confidentiality refers to protecting personal privacy and proprietary information from unauthorized access. Malicious attacks targeting confidentiality aim at obtaining desirable information (e.g., power usage, customer's account information) through eavesdropping on communication channels in a smart-grid metering and control system. Although such attacks have negligible effects on the operation of the system, the transmission of fine-grained consumption data by smart meters has raised concerns about privacy. It has shown that the consumption data collected by smart meters reflects the use of all electric appliances by inhabitants in a household over time, and it allows criminals to make inferences about the behaviors, activities, or preferences of those inhabitants. Those privacy issues need to be addressed appropriately to reduce customers' fears about potential leakages of their information. Some best practices relating to privacy have been proposed for the design of smart grids.

Authentication

Device authentication*:* The identity and legality of the smart meters and associated consumers should be verified before joining the interconnected smart meter network and receiving proper utility service.

Advanced Metering Infrastructure (AMI) Security Issue

Advanced Metering Infrastructure (AMI) refers to systems that measure, collect and analyze energy usage, from advanced devices such as electricity meters, gas meters, and/or water meters, through various communication media on request or on a pre-defined schedule. This infrastructure includes hardware, software, communications, customer associated systems and meter data management (MDM) software.

AMI components

AMI systems are viewed as consisting of the following components:

• Smart Meter:

The smart meter is the source of metrological data as well as other energy-related information. These smart meters can provide interval data for customer loads as well as distributed generation.

• Customer Gateway:

The customer gateway acts as an interface between the AMI network and customer systems and appliances within the customer facilities, such as a Home Area Network (HAN) or Building Management System (BMS). It may or may notco-locate with the smart meter.

• AMI Communications Network – This network provides a path for information to flow from the meter to the AMI head end.

AMI Security Threats

The following types of security threats are possible on AMI of Smart Grid:

• **Eavesdropping:** It is unauthorized real-time interception of a private communication.

• **Traffic Analysis:** It is the process of intercepting and examining messages in order to deduce information from patterns in communication.

• **EM/RF Interception:** Electro -Magnetic/ Radio Frequency interception to perform unauthorized interception of private communication.

• **Repudiation:** People, including public authorities, may modify the AMI data and thus refuse to acknowledge an action that took place.

• **Masquerade:** It is a type of attack where the attacker pretends to be an authorized user of a system in order to gain access to it or to gain greater privileges than they are authorized for.

• **Authorization Violation:** People may violate the authorization of AMI system to perform unauthorized actions.

• **Man-in-the-Middle:** It is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection when in fact the entire conversation is controlled by the attacker.

• **Integrity Violations:** Integrity is violated when someone accidentally or with malicious intent modifies the AMI interaction data.

• **Theft:** Physical theft of the AMI components could lead to unauthorized actions being performed.

• **Replay:** It is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed.

• **Virus/Worms:** A computer virus is a computer program that can copy itself and infect a computer. A computer worm is a self-replicating computer program. It uses a network to send copies of itself to other nodes (computers on the network) and it may do so without any user intervention.

• **Trojan Horse:** It is a term used to describe malware that appears, to the user, to perform a desirable function but, in fact, facilitates unauthorized access to the user's computer system.

- **Trapdoor:** An undocumented entry point into a computer program, which is generally inserted by a programmer to allow discreet access to the program.
- **Resource Exhaustion:** Hackers may use up all available facilities so no real work can be accomplished and thus AMI system resources become unavailable to the intended users.
- **Integrity Violations:** Integrity is violated when someone accidentally or with malicious intent modifies the AMI data and thus prevents intended users from using the AMI system resources.
- **Stolen/Altered:** The AMI data could be stolen or altered and that could lead to denial of action that took place or claim of an action that did not take place.
- **Repudiation:** People, including public authorities, may refuse to acknowledge an action that took place.
- **Cheating Customer:** The customer at an endpoint would attack to achieve the goal of reduced cost of electric and/or natural gas use. They would use information freely available from the AMI meter vendor or a standard associated with AMI meters to reset the meter and reprogram it to report false information. If the information is not freely available, the attacker would reverse-engineer a meter to develop a way to modify it.

Conclusion

Smart Grid provides intelligent, advanced power control for the next century. Many new technologies involve for supporting sensing, controlling, human interfaces. Charging electricity cost is fundamental infrastructure can be implemented similar to stock market in smart grid. Security and privacy are critical to the development of real-time communication strategy in smart grid. As the electricity usage information is frequently exchanged between the customers, the CCs, and the utility companies, to prevent the security attacks and the privacy violations is critical. This report summarized security, trust, and privacy issues in a comprehensive smart grid system. Presented the security and privacy challenges of smart grid system design and proposed dynamic secrets based solution for smart grid wireless communication. Throughput of system is useful for Application that needs low data rate. Some of its applications are: A Design of Greenhouse Monitoring & Control System Based on ZigBee Wireless Sensor Network, Smart Home etc.

References

[1] A Dynamic Secret-Based Encryption Scheme for Smart Grid Wireless Communication Ting Liu, *Member, IEEE*, YangLiu, YashanMao, Yao Sun, XiaohongGuan, *Fellow, IEEE*,mWeibo Gong, *Fellow, IEEE*, and Sheng Xiao

[2] Efficient Authentication and Key Management Mechanisms for Smart Grid Communications Hasen Nicanfar, Student Member, IEEE, Paria Jokar, Student Member, IEEE, Konstantin Beznosov, Member, IEEE and Victor C. M. Leung, Fellow, IEEE IEEE Systems Journal.2013

[3] EPPA: An Efficient and Privacy-Preserving Aggregation Scheme for Secure Smart Grid Communications Rongxing Lu, *Member, IEEE,* Xiaohui Liang, *Student Member, IEEE,* Xu Li, *Member, IEEE,* Xiaodong Lin, *Member, IEEE,* and Xuemin (Sherman) Shen, *Fellow, IEEE*
IEEE Transactions On Parallel And Distributed Systems,2013

[4] Fault-Tolerant and Scalable Key Management for Smart Grid Dapeng Wu and Chi Zhou , IEEE,2011

[5] PaRQ: A Privacy-Preserving Range Query Scheme Over Encrypted Metering Data for Smart GridMI WEN1,2 (Member, IEEE), RONGXING LU3 (Member, IEEE), KUAN ZHANG2,Jingsheng Lei1, Xiaohui Liang2 (Student Member, Ieee), AndXuemin Shen2 (Fellow, Ieee)IEEE Transactions On Emerging Topics In Computing current version 20 September 2013.

[6] A Trust-Management Toolkit for Smart-Grid Protection Systems
Jose E. Fadul, Kenneth M. Hopkinson, *Senior Member, IEEE,* Todd R. Andel, *Senior Member, IEEE,* and Christopher A. Sheffield IEEE Transactions On Power Delivery, Vol. 29, No. 4, August 2014

[8]Practical Secure Communication for Integrating Wireless Sensor Networks Into the Internet of Things Fagen Li and Pan Xiong IEEE SENSORS JOURNAL, VOL. 13, NO. 10, OCTOBER 2013

[9]Security for Smart Distribution Grid by Using Wireless Communication S.K.Saranya1, Dr.R.Karthikeyan. (2014)

[10] Ghansah, Isaac, 2009. *Smart Grid Cyber Security Potential Threats, Vulnerabilities And Risks* California Energy Commission, PIER Energy-Related Environmental Research Program. CEC-500-2012-047.

[11] IEEE Transactions On Smart Grid, Vol. 2, No. 4, December 2011
A Lightweight Message Authentication Scheme for Smart Grid Communications Mostafa M. Fouda, *Member, IEEE,* Zubair Md. Fadlullah, *Member, IEEE,* Nei Kato, *Senior Member, IEEE,* Rongxing Lu, *Member, IEEE,* and Xuemin (Sherman) Shen, *Fellow, IEEE.*

Bio