Journal of Computer Sciences and Applications, 2015, Vol. 3, No. 3A, 27-39
Available online at http://pubs.sciepub.com/jcsa/3/3A/4

DOI:10.12691/jcsa-3-3A-4

A Survey on Cryptography Key Management Schemes for Smart Grid

Bashar Alohali*, Kashif Kifayat, Qi Shi, William Hurst

Department Name, Liverpool John Moore University, Liverpool, United Kingdom
*Corresponding author: B.A.Alohali@2012.ljmu.ac.uk

Received May 07, 2015; Revised July 08, 2015; Accepted July 16, 2015

Abstract A Smart grid is a modern electricity delivery system. It is an integration of energy systems and other necessary elements including traditional upgrades and new grid technologies with renewable generation and increased consumer storage. It uses information and communication technology (ICT) to operate, monitor and control data between the generation source and the end user. Smart grids have duplex power flow and communication to achieve high efficiency, reliability, environmental, economics, security and safety standards. However, along with unique facilities, smart grids face security challenges such as access control, connectivity, fault tolerance, privacy, and other security issues. Cyber-attacks, in the recent past, on critical infrastructure including smart grids have highlighted security as a major requirement for smart grids. Therefore, cryptography and key management are necessary for smart grids to become secure and realizable. Key management schemes are processes of key organizational frameworks, distribution, generation, refresh and key storage policies. Currently, several secure schemes, related to key management for smart grid have been proposed to achieve end-to-end secure communication. This paper presents a comprehensive survey and discussion on the current state of the key management of smart grids.

Keywords: *key management, smart grid, cryptography, smart meters, AMI, NAN, HAN*

Cite This Article: Bashar Alohali, Kashif Kifayat, Qi Shi, and William Hurst, "A Survey on Cryptography Key Management Schemes for Smart Grid." *Journal of Computer Sciences and Applications*, vol. 3, no. 3A (2015): 27-39. doi: 10.12691/jcsa-3-3A-4.

1. Introduction

The smart grid is an electricity system with bi-directional power flows and communications between the utility provider and end user. Processes are automated and use sensors to communicate and monitor. Intelligent computational devices provide security, efficiency and reliability in the electricity system grid. Smart grids are able to deal with a large number of customers, enabling a timely, secure and adaptable information flow, which is needed to provide power to the evolving digital economy.

One of the main advantages of the smart grid is a model system of monitors which fosters communication between the power utility and the end user. This communication life-cycle involves; sending generated electricity to the distribution centre/power storage where it can be dispersed depending on need. During the power transfer from distribution to user, the utility company has the ability to monitor the process using sensors. The information recorded can include current electricity residence and the amount of potential energy being sent. Using this information, utility companies manage the zones of high use, detect power failure, control and store unneeded power and provide a suitable service. The data collected during peak times can be used to ensure high demand is adequately met and provided for [1].

Typical smart grid components tend to include smart electronic hardware, which controls and manages the distribution and transmission grids. Automation applications, such as distribution management applications and energy management applications to provide real-time control over transmission and distribution, also comprise a significant part of the grid mechanisms [1]. Each component delivers information about their operations and tasks, which is forwarded to centralized systems for automation. This data is used to improve the reliability and efficiency of the system.

In 2009, US President, Barack Obama, announced an investment grant program totalling $3.4 billion for the development of smart grid networks in the USA [2]. As present grids need improvement, due to age and growing demand, there are many factors that encourage world governments to invest more in smart grids. Further more, traditional electricity suffers from many issues, such as limited control, down falls and black outs, manual monitoring and one-way communication [3]. The following are the expected benefits for utilities, consumers and society offered by the introduction of smart grids:

- *Reliability*—Smart grids are more reliable than the traditional grid infrastructure [4].
- *Business economics*—The introduction of future smart grids is expected to improve the economics for both utility companies and end users. For utility companies there will be opportunities for new energy

sources. Particularly, theft of service is reduced from efficient management of billing [5].

- *Efficiency*—By upgrading the traditional power grid, several new features are added to the power grid system to improve its efficiency. For example, improved efficiency in the smart grid is reductions in peak load and transmission congestion costs. Smart grids are able to intelligently integrate all the users to improve operator control and decrease the cost of generation [6].
- *Safety*—Decreasing accidents and providing a fault-tolerant system prevents voltage spikes caused by grid-related events [7].

Despite its numerous advantages, there are many security challenges and issues with smart grids. Access control, identity management, connectivity, privacy, cyber malicious attacks and other issues are challenges, which the smart grid must contend with. Recent cyber-attacks, such as Stuxnet, on critical infrastructures have highlighted security as a major requirement for smart grids [8]. Cryptographic issues, such as data encryption and key management, are important security considerations which must be addressed to guarantee safe and secure grid operations.

Key management is a process of controlling access to and validating keys in cryptographic systems. This involves key generation, keys distribution, key storage and key updates. Key management is one of the most important security requirements to achieve data confidentiality and integrity in smart grids. However, smart grids consist of multiple components and applications, which imply key management schemes are a challenge to implement. In addition, there are a significantly large number of components, such as power generators, smart applications, system integrators etc. with different security levels and security requirements.

Many key management solutions have been proposed to fulfil the security requirements of smart grids. This survey presented in this paper summarizes the current state of the art on the key management for smart grids. The advantages and limitations of each solution are highlighted. The aim of this paper is to assist researchers, and provide and introductory background knowledge and understanding of key management for smart grids. The rest of this paper is as follows. Section 2 presents the background research into Smart Grids. Section 3 presents the existing literature in Smart Grid Networks and the security challenges on such networks. Section 4 presents an overview of cryptographic key management and literature that propose security schemes for Smart Grid Networks. Section 5 dwells in detail on Key Management for the AMI in the Smart Grid. Section 6 presents the privacy issues in the Smart Grid and Section 7 concludes the survey.

2. Smart Grid Background Research

Existing traditional power grids provide a consistent one-way power distribution to end-users. However, they face issues that need to be addressed in the future. The two main problems include slow reaction time and lack of real time monitoring. Broader issues which need to be addressed include, depletion of primary energy resources, climate change, reliability issues, diversification of energy generation and unintelligent systems, to name a few [9].

Smart grids are intelligent, with the capability to control and monitoring different devices and grid components for the provision of optimal energy generation and usage [9]. In this section, we describe the architecture for Supervisory Control and Data Acquisition (SCADA) and explain how control systems play a key role in the development of the smart grid.

2.1. SCADA system

SCADA is just one example of a control system, which plays an important role in the smart grid. SCADA is distributed system used to control and monitor geographically dispersed resources spread over a huge area of several square miles. Centralized data acquisition and controls are critical to the system's operation. Typically, SCADA systems are used in distribution systems such as gas pipelines, water, oil and electrical grids [10]. The technology used in SCADA systems helps smart grids to reduce operational and maintenance costs, and ensure the reliability of power supply. Hence, without a secure SCADA system, it is impossible to deploy a smart grid system [11].

Following are the major components of a SCADA system:

- *Human Operator*—Every SCADA system is controlled and monitored by a human operator [12].
- *Human Machine Interface (HMI)*—the operator controls the system by analysing various types of inputs such as graphs, charts and schematics. Therefore, the HMI allows the operator to view the status of the process. There are many technologies such as web browsers [12] that can support HMI.
- *Master Terminal Unit (MTU)*—The MTU works as a master in the master/slave architecture. It manages the high-level operation of the process. This unit provides responses based on the data collected from another site to the operator via the HMI. The remote site then receives a control signal which is transmitted by the MTU [13]. In other words, the MTU sends control commands and collects updates from sensors in field devices to allow for high-level control.
- *Communications system*—The MTU and remote site communicate by means of wired or wireless systems, e.g., the Internet or satellites. They can use different network protocols, such as TCP/IP or field bus protocols [12].
- *Remote terminal unit (RTU)*—RTUs work like a slave in the master/slave architecture. Signals are sent to the device under control, and data are obtained from these devices and then transmitted to the MTU. RTU is also referred as a programmable logic controller (PLC) and the communication in the RTU is two-way [14]. The RTU can also be described as a microprocessor that controls sensors and actuators that interact with the real world. However, there are some limitations in RTUs such as memory and processing power, where the standard protocols are 16-bit microspores and 8 KB of RAM [12].

Figure 1 displays a high-level view of a SCADA system with its components.

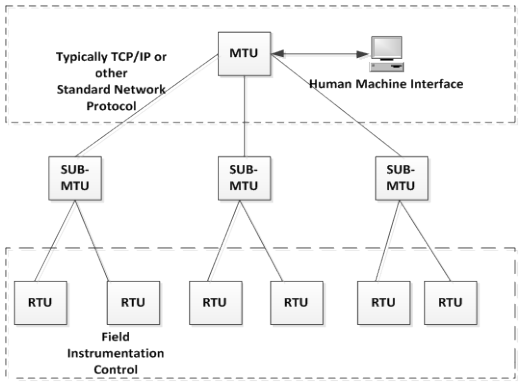

Figure 1. Components of a SCADA System

The data transported in the SCADA system can be sensitive; therefore, it must be protected from unauthorized access. Consequently, SCADA systems are paramount to the national security of the country because these systems control and manage the power, water, oil, gas, chemical, electric, telecommunications and a number of other foundations. Unauthorized access to these SCADA systems by malicious users may result in the retrieval of sensitive data and result in these systems becoming inoperable or exposed. Maintaining and securing the data in the SCADA systems are crucial to avoid any disruption to the normal lives of the people in the country. Investing in the security of the SCADA system will prevent future financial losses due to the system being hacked or broken as a result of security weaknesses [15].

2.2. Smart Meters and Smart House Appliances

The implementation of the smart grid brings with it the integration of smart house appliances for enhanced energy monitoring. Smart house appliances (smart and legacy) are expected to be able to communicate with smart meters via a home area network (HAN), which will assist in efficient energy intake and control to all home devices. One key appliance is the smart meter, which consists of a microcontroller that has memory, digital ports, timers, real-time and serial communication facilities [16]. A smart meter is an electricity meter that reads and records a user's power consumption and enables data collection for the remote monitoring interface known as an advanced metering infrastructure (AMI). Each device is able to record the power intake and transmit it to the utility server, connect or detach a customer source of energy and send out alarms in case of an error. Power utilities communicate with smart meters to control energy intake [17].

The AMI is a system, which gathers data, measures and analyses electricity using smart meters and service providers to offer two-way communication [18]. An AMI system involves different technologies and applications including smart meters, user gateways, home area network, wide-area communications infrastructure, and meter data management systems (MDMSs), Each are integrated to perform as one system [19]. The approach is used to collect, store, analyse, and measure electric usage data. In effect, a gateway between the consumer and electric supply is provided [20].

2.3. An Overview of Smart Grid Architecture

In this sub-section, smart grid architecture is introduced. A discussion is put forward on the functionalities of each layer and related communication technologies are highlighted.

In the smart grid architecture, there are four layers. This includes: a power system layer; a power control layer; a communication layer and an application layer. Figure 2 shows an overview of smart grid architecture.

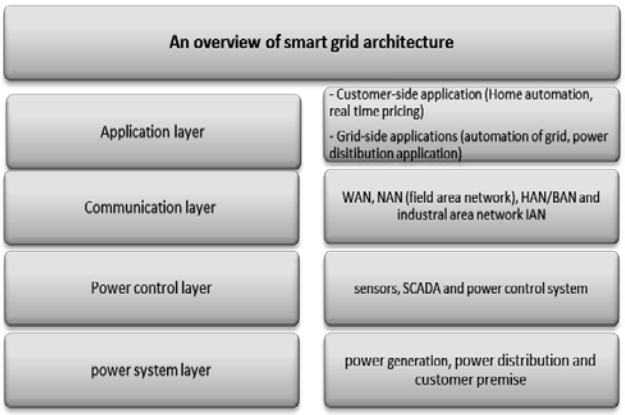

Figure 2. An overview of the smart grid architecture

The power system layer involves electricity generation, distribution and customer premise. The power control layer is comprised of sensors, control systems (such as SCADA) and the power control system. The communication layer consists of WAN, NAN (field area network), HAN/BAN. Finally, the application layer includes power transmission, customer application, and real-time pricing.

The application layer can generally be categorized into customer-side applications and grid-side applications. It provides smart grid applications for customers (such as information of energy usage or real-time pricing, critical peak pricing, automated controls for appliances and smart devices) and for utility provider (such as substation monitoring, fault detection, integrated volt-VAR control [80]).

The communication layer provides a network for the transport of data and information in a two-way, efficient, reliable and secure manner between the power systems and the data centre. As part of the communication layer, the HAN is initially a multi-supplier environment composed of smart appliances that need to be set-up together continuously using suitable standards such as ZigBee and HomePlug NANs are employed for covering large geographical areas and distributed field devices. Typically, NANs use Wi-MAX (Worldwide Interoperability for Microwave Access) or 3G/4G based for wide range communication. Table 1 presents a comparison of different communication protocols and standards.

The WAN performs as the core network. It consists of the backbone network and the backhaul network. In the WAN, the backbone network connects the utility backbone and substation to provide high capacity communication with minimal latency and commonly uses

optical fibres. To provide broadband connectivity to the NAN, the backhaul network is the link between the WAN and the NAN. In addition, it is connected distribution systems such as sensors, SCADA, remote terminal units (RTU) and mobile workforces. The main task of the WAN is to transport the smart grid's data to distant sites in an efficient and reliable way. Utility control centres have been operating WANs and manage the operations and processes in the grid for many application such as grid monitoring and SCADA [23].

Table 1. Different Communication Technologies in a Smart Grid

Technology	Application	Data Rates	Approx. Coverage
ZigBee	Used for HAN, home appliances and AMI	250 kbps	10 to 100 m
HomePlug	It is a power line uses for electricity wiring to communicate in HAN [21]	14 Mbps 200 Mbps	300 m
WiMAX	Demand response, AMI/wireless automatic meter reading (WAMR)	75 Mbps	50 Km
Cellular G3-PLC	SCADA and controlling for RTUsAMI, Demand response, monitoring for remote site [22].	240 kbps 33.4 kbps	50 Km 6 km
Satellite	AMI, WAN	450 Kbps	Depend on number of satellites and their beams

2.4. Efficiency and Reliability

The future smart grid requires meeting the increasing efficiency requirement using and advanced communication infrastructure. Information technologies enable smart grids to provide grid-wide remote monitoring and control capabilities, which go beyond the ability of the traditional infrastructure. Moreover, smart grids provide high-performance two-way communication with fast controls and enable fast automated control actions for voltage and power flow management [19]. Furthermore, there is a fault tolerance requirement as smart grid nodes are often deployed in inhospitable environments. To achieve increased efficiency, it is essential for smart grids to meet the need for fault-tolerance and that they have the ability to deliver the desired level of functionality in the occurrence of faults.

The reliability of power distribution systems and transmission systems are critically significant for utilities and customers. A distributing power generation facilities at various points within the power grid, and creating sub grids within larger grids, improves the overall reliability.

2.5. The Challenges of Big Data and Integration

The smart grid deals with data from a huge number of devices in the field and HAN. The data collected from smart appliances; smart meters are very important for utility companies to obtain information about their power system such as voltage levels, energy usage and so on. However, handling, and integrating such huge interconnected data for analysis is a really challenging and complex task that needs to be addressed in other to achieve trusted and reliable data. Smart grid will force power providers to process far more information than they are accustomed to handling [24]. Consequently, in the following section, a background survey of research into the challenges posed by the integration of big data and smart grid issues is presented.

3. Related Work

There have been many research and survey papers on smart grid networks [2,25-32]. This section presents a discussion on the literature survey conducted into the related research.

3.1. Smart Grid Networks

The authors of [2] focus on conduct of communication and reviews networking technologies, including communication/networking architectures, control and management of operations and QoS and optimization in the smart grid. The work in [25] reviews and classifies various routing protocols of smart grid applications perspectives found in the literature. In this survey, the authors have also identified routing design issues for smart grids.

[26] provides the current status of smart meters and outlines various issues and challenges involved in the design, deployment, utilization, and maintenance of smart meter infrastructure. Furthermore, the authors have discussed in detail numerous of validate the expectation of an empirical method in papers using case studies to simulate or conduct pilot runs of the technologies before their massive implementations. Strategies are generally driven by the United States, while other countries are focusing on quality improvements of the already strategized initiatives with an efficiency-related goal taken into account. The user is going to play an important role in the future of smart grids as they are involved in improving the business model with the addition of self-generation and selling-back of any extra capacity to the utility company.

[28] presents a comprehensive survey of cyber security issues for smart grids. In detail, their focus is on reviewing and discussing security requirements, security weaknesses, and attack countermeasures; secure communication networking protocols and architectures in smart grids. In addition, they summarized the design of secure network protocols to achieve efficient and secure information delivery in smart grids.

[29] provides a general idea of smart grids and current advances in distributed sensing, modelling, and control, particularly at both the high-voltage smart grid and at the consumer level. The advances will pave way for the development of an effective, distributed control, and intelligent power system networks with a focus on addressing computation-distributed sensing, controls, dynamic system challenges and opportunities in the future.

The authors of [30] discussed contents, development, and key technologies of wide-area protection. For improved availability of data synchronization or timeliness, and communication technologies applied in smart grids, they can provide high-precision synchronous

data acquisition, meet real-time reliability of data transmission, and provide basic support for wide-area protection principles and applications. There seems to be likely for wide-area protection to association with adaptive protection, such as IEC61850 protocol or multi-agent technology. Currently, secure WAN is a research gap in smart grids, however, significant improvement has already been achieved.

Authors, in [32], present a survey that provides a critical overview in communication, networking and the role that smart grid and middleware technologies will have in the transformation of existing electric power systems into smart grids. This paper presents detailed key technological, economic and societal drivers for the growth of smart grids. The authors of this work present a conceptual model of communication systems for smart grids and from the data-centric perspective, many smart grid applications can be described as operations where a subset of data is consumed within a definite specified time or temporal locality. This work briefly identifies functional components, communication topologies and communication services that are needed to support. The authors introduce the major research challenges in this area including network reliability, QoS, time synchronization, data management and autonomic behaviours.

As summarized in the above research, none of these survey and research works focuses on the theoretical and practical challenges of management of cryptographic key protocols by considering securing major smart grid components.

3.2. Security Challenges in Smart Grid

Security challenges are one of the main considerations that should be addressed for smart grids. Is includes situations where malicious users and attackers can modify customers' data or cause any type of attack on an unsecured smart grid network. Therefore, we should take into account the following security requirements and challenges in smart grids. In this section, a general and brief review of security requirements in smart grids will be presented including availability, data confidentiality, data integrity and authentication, as well as cryptographic issues, key management, availability, secure routing.

3.2.1. Data Confidentiality

In order to secure smart grid data from hackers, it is important to protect the confidentiality of smart grid data and make sure that data are not changed or lost. Only authorized entities should be given access to the data to ensure the level of security is high. The best way to achieve confidentiality in the smart grid is by encrypting data and establishing a shared secret key among nodes. This is a standard method and relies on a shared secret key to exist between communicating parties. However, encryption itself is not effective enough because a malicious attacker can perform traffic analysis on the overheard cipher text, which could release sensitive information from the data. Moreover, to avoid the exploitation of information and confidentiality of sent data in smart grids, access control policies must also be applied [33].

Furthermore, to maintain the confidentiality in smart grids, secure channels should be built into the network. Also, public node information, such as identities, must be encrypted to some extent to defend against traffic analysis attacks [33]. Compromising a node physically becomes a problem of data confidentiality, whereas, a malicious user physically captures a node, it is generally expected that the adversary can obtain all data from that node such as reading meter data or customers' data.

3.2.2. Availability

One of the primary aims of security is the availability of data on the entire network. It is a requirement that nodes on a smart grid network should be functional throughout their lifetime. The best way to achieve this is to have network management and supervision by implementing a reliable and suitable transport layer solution. Therefore, resources in nodes should be available throughout the whole network.

Nodes should have the capability to self-heal to mitigate for failure. For example, in the case where power to the node is lost, nodes need to reorganize themselves to maintain availability [34]. An attack that results in failure of availability is known as a Denial-of-Service (DoS) attack. It takes place when a system denies service to authorized nodes. This may be caused due to resource exhaustion by unauthorized nodes. DoS are a real challenge for the smart grid.

Additionally, it is difficult to stop an on-going attack since the victim and its nodes may not catch the attack. In this kind of attack, the attacker prevents legal users from having access to information and services by targeting the victim's device and the network connection. This attack stops the user from making outgoing connections on the smart grid. Jamming is one of the DoS attacks which targets wireless communication frequencies in the smart grid [35]. When they are in close range, large amounts of noise may be generated in these appliances. The communication can be jammed so as to make the signal noise very low, and this could lead to the non-functioning of the smart grid [36]. Loss of availability may have a serious effect in some smart grid components such as the controlling system. Loss of availability may impact the operation of many critical real-time applications in the smart grid such as those in the DR.

3.2.3. Access Control and Security Policies

It is important to ensure that data transmitted via smart grids is kept confidential and that no one but the intended receiver is able to see the message. In addition, smart grids contain many components that are interconnected [37]. Because of security concerns related to this, authentication is needed to verify the identity of the receiver in order to avoid any disruption or exploitation [38]. Access to the control centre, transmission and distribution grids is allowed only for authenticated users, groups and services [39]. Furthermore, it is necessity for suitable security policies to establish relationships among consumers, utilities and third parties, although applying security and privacy policies should not result in unsatisfactory latencies. Information security policies define the guiding rules that security controls are applied to secure data; communication routing, processes and systems. In various cases, the information and network protection policies

used by utilities need to be updated [40]. Smart grid provides many benefits to consumers such as control and transparency over their energy usage. For example smart grid allow consumer to login into their electric account and view their energy usage based on data reported from their smart meter and it allows receiving alerts based on outages by the preferred communication channel and so on [11]. However, to realize these advantages there will be a need to utilize personal data and smart grid will collect personal data. Despite advantages, privacy concerns pose challenges. The effect on privacy may allow unwanted parties to know of activities on the property. There are concerns from consumer about smart meter, which allow unpermitted third parties to easily obtain personal information. Therefore, it is important to consider privacy controls, security and privacy assessment for smart grid.

In other to address this privacy concerns, several research has being carried out such as the one by Li et al [70]. In their work, it was pointed out that Power usage and operational data can be abused to infer personal information of customers. Without a well-designed privacy preservation mechanism, adversaries can capture, model and divulge customers' behaviour and activities. This led them to first investigate the natures of privacy leakages and explore potential privacy threat models. After that, they designed and implemented a new protocol named privacy reserving demand response based on the attributed-based encryption, and formally proved its validity. To demonstrate its viability, the protocol was adopted in several types of DR programs on an emulated smart grid platform. Experimental results show substantially lighter overheads while formidable privacy challenges are addressed.

3.2.4. Cryptographic and Key Management Challenges

Cryptographic mechanisms are one of the best ways to achieve confidentiality and provide protection for data among smart grids. However, the suitable management of keys is necessary for the effective use of cryptography for protection. Smart grid consists of heterogeneous communication network. Therefore, key management is particularly challenging in smart grid, and it is not practical to design a universal key management scheme for the entire smart grid. Keys are analogous to the combination of a safe. If the combination is known by an adversary, the strongest safe provides no security against penetration [41]. However, weak key management may easily compromise strong algorithms. Furthermore, it can be time and cost consuming if it is not handled correctly. Managing keys in a proper manner could cause additional storage and bandwidth usage. Therefore, the security of information protected by cryptography directly depends on the strength of the keys, the effectiveness of mechanisms and protocols associated with the keys, and the protection the keys provide [41].

4. Cryptography Key Management

In smart grids, communications can be monitored and nodes are potentially subject to capture and surreptitious use by an adversary. For example, an attacker can modify customers' data or cause any type of attack for an unsecured smart grid network. For that reason, cryptographically secure communications are required.

Cryptography is used as a protection technique to provide confidentiality, authentication, data integrity and non-repudiation in smart grid communication. A number of different approaches have been used for cryptography such as hash functions.

4.1. Cryptography Research

In cryptography, the most crucial and challenging step is Key management [42]. Key management is critical and to obtain good security the keys' length should be long enough to reach the security requirement in the smart grid communication. Furthermore, the key's lifetime should fit with the security requirement [43]. A keying relationship can be used to facilitate cryptographic mechanisms in smart grid communication.

Cryptographic techniques make use of two types of keys, either symmetric or asymmetric. Symmetric cryptography relies on a shared secret key between two nodes to enable secure communication. Asymmetric cryptography, applies two different keys, a private key and a public key. The public key is used for encryption and can be published. The private key is used for decryption. From a computational point of view asymmetric cryptography requires orders of magnitude more resources than symmetric cryptography. In general, key management is considered of four sorts of keys as following: one-time session symmetric keys, public keys, private keys, passphrase-based symmetric keys.

The session keys are used once and generated for each new message. The public keys are used in asymmetric encryption. On the other hand, private keys are also used in asymmetric encryption. Passphrase-based keys are used to protect private keys. A single node can have multiple public or private key pairs [43].

4.2. Key Management in the Smart Grid

The smart grid contains heterogeneous communication networks, including small-scale (e.g., a substation system) and large-scale (e.g., the AMI system) networks, wireless and wire-line networks. It is not practical to design a single key management infrastructure to generate and distribute keys for all networks in the smart grid. Moreover, key management on a smart grid is to be performed and protected on its communications networks among various parties such as a smart meter, AMI, sensors, IED and SCADA. Therefore, it is not practical to design a single key management infrastructure to generate and distribute keys for all systems and parties in the smart grid. Furthermore, it is important to consider the security requirements of various systems in the smart grid for chosen key management schemes [44].

Many approaches have been proposed so far to implement a key management system for smart grids. In order to understand the key management issues and inconveniences for smart grids, we first need to review and compare these recently proposed approaches and architectures aimed at distributing and managing authenticated keys for smart grid systems. We have classified key management schemes in smart grid networks as follows.

4.2.1. Key Management for AMI

The writers in [19] proposed key management for an AMI system which is built based on the key graph. They define the secure exchange between a Management Side (MS) (e.g., utility) and appliance or devices (SX) at the customer premise (i.e., smart meters). There are three different key management processes proposed in KMF to deal with the hybrid transmission modes; the contents of key management for unicast, broadcast, and multicast modes. Relatively simple cryptographic algorithms are chosen for key generation and refreshing policies due to the storage and computation constraints of SMs. The KMF has been defined as KMF = *(U, K, R)* where *U* nodes in the AMI system; *K* denote keys of nodes, g_k is group of keys and *R* is the binary relation between *U* and *K*, therefore, *useru* knows key *k* if and only if *(u, k)* is in *R*. Furthermore, user set $k = \{u|(u, k) \in R\}$. In the proposed scheme, the root key k_0 is used for broadcast; the group keys $\{g_{k1}, g_{k2}, .., g_{km}\}$ are used for multicast in different DR project groups; the keys $\{k_1, k_2, \ldots, k_n\}$ are used for unicast communication between management side MS and each devices SX. The proposed KMS is closely integrated and supports the unicast, broadcast, and multicast. The distribution of the keys and related data will not affect the normal network traffic in an AMI system. Moreover, the proposed scheme can deal with normal security attacks. Furthermore, forward and backward security is dealt with in the proposed scheme. The authors of [19] apply the hierarchy of keys or a rooted tree, therefore, every user is given a subset of keys which contains its individual key, a key for the entire group for group communications, and a key for its subgroup. However, the proposed scheme requires updating the key redistribution for each joining or leaving of the session. Furthermore, the network topology has not been taken into account, which will cause some unwanted nodes in a group to receive rekey messages.

The authors in [45] propose a lightweight key distribution and management scheme tailored to AMI. Specifically, a group ID-based mechanism is proposed to establish the keys for a large amount of entities with a small overhead. They propose a group identifier-based mechanism to establish the symmetric keys, in which a gateway shares a different secret key with every single smart meter and the keys are generated based on the D-H algorithm; however, without authenticating the smart meters during the key generation phase. Moreover, they add a verification step to the pair wise key construction. Since the proposed scheme requires every single meter to have a symmetric key, it is not scalable for smart grids. Moreover, use of symmetric keys is vulnerable to MITM attack.

Subir et al., in [46], proposed a unified key management mechanism (UKMF) that can generate ciphering keys for multiple protocols of multiple communication layers from a single peer entity authentication procedure. The unified key management mechanism is suitable for smart grid use cases, especially for smart metering, where smart meters are assumed to be low-cost wireless devices for which repeated peer entity authentication attempts for each protocol can be contributed to increased system overhead. The proposed mechanism is flexible in that peer entity authentication can be treated as either network access authentication or application-level authentication. However, the mechanism has established that information discovery for bootstrap application ciphering is an important and as yet missing piece to realize the unified key management framework vision. This part needs further analysis.

4.2.2. Key Management for SCADA

Sungjin et al. [47] proposed a key management scheme that address the broadcasting and multicasting communication in SCADA system. The proposed scheme uses a Iolus framework [48] as an underlying architecture, which is based on hierarchy of nodes. The hierarchy provides a structure of managed and manager nodes; to manage a protected distribution tree where every node is managed through a subgroup manager. Through the Iolus framework, the key structure is divided into two types, which are between master terminal unit MTU and SUB-MTUs and between SUB-MTUs and RTUs. Each type has a separate controller. One is responsible for the top-level management, which is called the Group Security Controller (GSC).

The second level is responsible for the rest of the subgroups, called Group Security Intermediary (GSI). The secret group key is shared between GSIs with GSC, whereas every node subgroup key is shared with every node of GSI. Therefore, a Logical Key Hierarchy (LKH) structure is used to manage keys. The use of Iolus's hierarchy provides the ability of multicasting and broadcasting for multiple RTUs. Furthermore, it also helps to minimize the number of keys to be stored. However, the scheme provides limited multicasting. In addition, it generates increased number of keys that are stored in RTUs, which incurs more computational overhead.

To address the scalability issue in key management solutions, Wong et al. [49] proposed the logical key hierarchy protocol, which is based on constructing a logical tree of keys. From its leaf to the root, every node shares symmetric keys. Whenever a member wants to join/leave the session, all the symmetric keys are revised in the tree. The proposed key management scheme is scalable; however, the main drawback of the scheme is that the keys are hashed rather than encrypted and distributed if a new member joins the session [50]. Choi et al. [51] proposed a key management scheme named as Advanced Key Management Architecture (ASKMA), for message broadcasting and secure communications. Their scheme performs well and minimizes the burden on low power nodes. Their scheme uses a logical key hierarchy. The scheme has many benefits; however, it may be less efficient during the multicast communication process. Another issue for ASKMA is its lack of availability, that is, the continuity of the security processes when there is a node failure or when a new node joins in.

Choi et al. [50] proposed ASKMA+, an improvement to ASKMA. This new scheme reduces the number of stored keys and provides efficient and protected multicast and broadcast communications. However, the availability issue of ASKMA+ is still not resolved.

National Laboratories proposed the SKE (Secure Key Establishment) scheme to secure SCADA system. SKE started with classifying the keys exchange on the SCADA network into two parts [52]. The first is Controller-to-Subordinate (C-S) MTU-RTU, and SUB-MTU-RTU which uses symmetric keys. The second classification is a Subordinate-to-Subordinate (S-S) communication, which works as a peer-to-peer communications using public key

cryptography. However, SKE cannot support RTU-to-RTU communications. Broadcast and multicast scenarios are also not supported by SKE.

4.2.3. Key Management for vehicle-to-grid (V2G)

The idea of vehicle-to-grid (V2G) is that electric vehicles (EVs) communicate with the smart grid to sell demand response services by delivering electricity into the grid. The operation of V2G networks is based on continuously monitoring the status of individual EVs as well as a designed incentive scheme to attract sufficient participating EVs.

Authors of [53] have proposed V2G communication protocol with privacy preservation. They propose a secure and privacy-preserving communication protocol for V2G networks, which utilizes the restrictive partially blind signature to protect the identities of the EV owners and is also based on certificate less public key cryptography to simplify the certificate management as in traditional public key infrastructure and to overcome the key escrow problem as in identity-based public key cryptography. The proposed protocol can achieve the properties of completeness, identity and location privacy, confidentiality and integrity of the communications, and known-key security, and is secure against the replay attacks and existential adaptively chosen message attacks [53].

4.2.4. Key Management for WSNs

LEAP [54] is Key Management protocol. It aims to increase the protection of non-security protocols. It supports 4 kinds of keys to each node. One node is shared with the base station, which contains individual keys. Then pair-wise keys are shared with nearby nodes. Cluster keys are shared with a set of nearby nodes. Finally, one key is shared with all nodes in the network, which is a group key. LEAP supports a protocol to authenticate local broadcast. Furthermore, it supports in-network processing for its key sharing. Therefore, it sufficiently protects the sensor networks from many security attacks. Finally, the LEAP scheme is effective for key creation and key updating while maintaining the necessity of small storage for each node.

5. Key Management and Security for AMI

Nicanfar et al., propose using a CA as a Security Associate (SA) server in the utility network [55]. Their system has two secret values with the SA keeping the first secret (the main part) and smart meters keeping the second secret value, which is only a counter generated by SA and it is part of the system secret values managed by SA). The authors do not consider the security issues when appliances are installed in the SM perimeter and focus instead on the security between the SM and the utility.

To minimize public key and private key management network overheads, the authors propose an ID-based cryptography model along with a one-way hash function applied to each node ID to provide the public key of the node. According to [72], the SA and a new SM are mutually authenticated during the synchronization phase of the new SM. The new SM chooses a previously initialized node (Authentication Agent (AG)) for this step. During this step, the SM's private key is sent by the SA after computing both the SA's and the AG's public keys and after several symmetric and asymmetric encryption operations by the involved entities. The benefits of involving AG in the middle of communications between a new SM and the SA are not clear and b) the way to detect if an AG has been compromised is also not discussed in detail. Moreover, the synchronization phase could be achieved offline (during the factory or site acceptance tests) thereby reducing the computational overheads associated with this approach.

A Distribution grid management, which focuses on improving the performance of various feeders and transformers, by having a networked distribution system, which can integrate transmission systems with the needs of customer management. The different Smart Grid capabilities are needed in order to ensure that AMI and other systems can be developed in order to ensure that various systems can lead to improvement in the grid management systems. One of the factor which is important to consider that efficient and reliable systems can lead to power systems which can reduce the peak loads, and improve the capabilities of the smart grind in managing the different renewable energy source. This will also ensure that improvement in the systems can be managed in order to create a competitive advantage for the company who may be using such a grid system.

In their research [66], the authors develop a secure and lightweight scalable security protocol that allows a power system operator (PO) to collect data from measurement devices (MDs) using data collectors (DCs). The security protocol trades off between computations and device memory requirements and provides flexible association between DC and MDs. These features allow data to be securely transferred from MDs to POs via mobile or untrustworthy DCs. The complexity and security of the protocols is analysed so as to validate its performance using experiments. The results confirm that the proposed protocol collects data in a secure, fast and efficient manner.

In this work, the authors propose and analyse a key establishment and data collection protocol, SELINDA, which allows a PO to establish shared keys with multiple MDs via an untrusted DC. The DC behaves like a relay for data communications although it is not continuously connected to the PO. Besides, the DC has no access to the keys established between the PO and the MDs. Therefore, the DC can potentially be mobile and untrusted, which makes the scheme essential for ensuring the security of community aided data collection in the smart grid.

The protocol has four key features that distinguish it from existing protocols. First, the protocol is computationally lightweight for the MDs as it requires the MDs to perform very few expensive cryptographic operations and to send few messages. Thus the protocol supports resource constrained MDs with limited memory and a slow CPU. Second, the protocol allows to trade off computation for memory requirements in the MDs. There is one long-term secret per entity, its private key. Thus, the PO needs to maintain the public key of all MDs in the system. It also maintains state information for the current session of data collection. The MD only needs to remember its own private key and the public key of the

PO. They can recalculate or store the session keys, depending on their computational and memory constraints. Third, the protocol provides flexible association between DCs and MDs. As an MD does not need to know the public key of any DC, the PO can assign different DCs to collect data from the same MD at different times. This feature is particularly important in scenarios where the DCs are mobile or the infrastructure is evolving so that different mappings or assignments between DCs and MDs can be used at different times after the deployment of the MDs. Finally, the protocol protects the collected data from a compromised DC. Thus, an attacker cannot access the collected data even if it is in control of a DC. This allows the PO to outsource the data collection procedure without sacrificing security.

In [67], the authors introduce a cryptographic key management mechanism for secure and efficient key revocation and exchange. The scheme is based upon a well-known cryptographic protocol: Broadcast encryption using a media key block (MKB). In comparison with the individual identification process in the PKI-signature based IKE protocol, this approach is more efficient. In the IKE scheme, each device need to verify signatures in the certificate and CRL for each device before each communication starts, whereas this proposed scheme only requires each device to perform an MKB process to extract the media key (or, shared key) which contains one signature verification at the system's setup step.

MKB to all devices in the same management area as proposed is more efficient than the PKI based scheme, which need to distribute individual certificate for each device. The comparison results show that in most cases this proposed scheme is efficient and cost-effective for power devices and systems in the smart grid. Similarly, in [68], an efficient group key (GK) management scheme aimed at securing the group communications, for instance, from the utility to appliances and smart meters located in different homes is presented. The scheme is based on the X.1035 password-authenticated key exchange protocol standard and also follows the cluster-based approach to reduce the costs of the GK construction and maintenance for large groups. The protocol enables secure communications utilizing any communication technology. Analysis using one of the best evaluation tools in the technical community shows that the constructed GK is valid and secure against well-known attacks. They also show that the proposed scheme supports forward and backward secrecy and is more efficient in comparison with other GK mechanisms.

They propose the password authenticated cluster-based GK agreement (PACGKA) protocols to manage the security of group communication in Smart grid to support multiparty applications. PACGKA extends the password-authenticated key exchange (PAKE) protocol to construct and manage a GK among a cluster of devices, utilizing a pre-shared password for authentication. We show that key management using PACGKA is more efficient than existing methods without sacrificing security

6. User Privacy in Smart Grid

The authors of [69], proposes a privacy-preserving aggregation (PARK) scheme with adaptive key management and revocation like in [67], to prevent user's data from being disclosed to untrusted entities in smart grid. Specifically, they first investigate a lightweight aggregation scheme with efficient aggregate authentication, which protects the individual user's data from disclosure to the untrusted aggregator. Furthermore, a proposal for an adaptive key management mechanism with effective revocation, where users can automatically update their encryption keys if no user joins or departs from the system. The expiry time of the key is determined by user's reputation for the adaptive key management. Finally, the security analysis demonstrates that the PARK can achieve privacy preservation, forward and backward secrecy at the same time, while the performance evaluation shows that the PARK consumes reasonable costs.

In [71], the authors propose a group ID-based mechanism to establish the keys for a large number of entities as we expect in the smart grid environment with many home users. A multiplicative group $*q$ Z ($q$is a prime number) is used to generate secret keys as thus; Every device securely accesses a Certification Authority (CA) which issues certificates each of which is loaded with the following primitives: the device Identifier (ID) (serial number), the multiplicative group parameters ($*q$ Z, q, a), where $\boldsymbol{a}$ primitive root of q, and H (the hash function). According to this approach, the gateway GW (e.g., HEG) and each neighboring device X (e.g., smart meter and appliances) selects a random number in the multiplicative group and generates its public key (e.g. X selects x and computes ax).

Then a group key is generated and shared between a gateway GW and a group of N devices ($X1$, $X2\ldots$ XN) in the HAN as follows: first, GW and each device Xi use the unauthenticated group key to generate Xi GW K based on the Diffie-Hellman (DH) key exchange method. Then GW will aggregate all the symmetric keys to compute the common group key Gk, which is the multiplication of the aggregated keys. Finally, GW sends Gk to every device Xi after encrypting it using Xi GW K. The authors claim that their approach provides forward secrecy (i.e., if the secret material is compromised, an attacker should not be able to decrypt messages that were previously encrypted by that key material). However, if the secret is compromised, an attacker will be able to decrypt every message intercepted before the Key update. Due to the DH deployment, frequently updating the keys make this approach to be computationally very expensive. Moreover, the gateway is a single point of failure in the architecture. This approach only protects the messages being exchanged between HAN devices and the gateway.

Kamto et al [72] propose a framework for key distribution and management for both aggregation and accountability in a neighbourhood area network employed by a utility company in its power distribution system. Specifically, a key distribution table is set up for each smart meter to carry out homomorphic encryption for secure data aggregation, while a loose time synchronized key scheme is proposed for low rate data collection of each smart meter. Specifically, a secure pair-wise key agreement scheme is designed to provide the authenticity of the end user in a wireless mesh network configuration of SMs. This scheme works in concert with the homomorphic encryption to provide the utility company

with the real-time bulk power demand while keeping the end user's power usage a secret during the distributed aggregation. Furthermore, they propose a loose time synchronized key mechanism for secure collection of relatively slow paced readings of power consumption recorded by each individual meter and allocate each end-user's individual power demand necessary for accurate power usage billing and potential Cheaters and attacks identification.

Seo et al [73], in this paper, propose an efficient encryption key management mechanism for end-to-end security in the AMI. By applying certificate-less public key cryptography (CL-PKC) for smart meter key management, the approach eliminates certificate management overhead at the utility. Moreover, our mechanism is practical, because it does not require any extra hardware for authentication of the smart meters. In this approach, the utility supports a PKI and has its own public key certificate, but smart meters are not required to have certificates. Instead of using certificates for the smart meters, the concept of CL-PKC to generate and manage the keys of the smart meters is utilized. Unlike the utility, which is a static entity, smart meters are dynamic entities which often leave or join the AMI. If smart meters are required to have certificates, the utility has the burden of managing these smart meter's certificates.

In CL-PKC, each user's complete private key is a combination of a partial private key generated by a Key Generation Centre (KGC) and an additional secret generated by the user. The advantage of this approach is that the KGC is not prone to the problem of key escrow, because the KGC is no longer responsible for the complete user private key. Therefore even if the attacker compromises the KGC, the attacker cannot obtain the private keys of the users. Moreover, the special structure of CL-PKC allows a user to encrypt a message without having to verify the public key of the message receiver via a public key certificate. By utilizing key settings of CL-PKC for smart meters, the authors eliminate the utility's overhead of certificate management.

[74] proposes an efficient scheme that mutually authenticates a smart meter of a home area network (HAN) and an authentication server in the Smart Grid (SG) by utilizing an initial password, by decreasing the number of steps in the secure remote password protocol from five to three and the number of exchanged packets from four to three. Furthermore, it proposes an efficient key management protocol based on an enhanced identity-based cryptography for secure SG communications using the public key infrastructure. This proposed mechanisms are capable of preventing various attacks while reducing the management overhead. The improved efficiency for key management is realized by periodically refreshing all public/ private key pairs as well as any multicast keys in all the nodes using only one newly generated function broadcasted by the key generator entity.

[75] proposes to protect sensitive energy usage information of consumers by the use of a virtual ring architecture that can provide a privacy protection solution using symmetric or asymmetric encryptions of customers' requests belonging to the same group. They compare the efficiency of the proposed approach with two recently proposed smart grid privacy approaches namely, one based on blind signature and other based on a homomorphic encryption solution [72]. They show that this approach maintains the privacy of customers while reducing the performance overhead of cryptographic computations by more than a factor of 2 when compared with the aforementioned past solutions. It is further demonstrated that the smart grid privacy solution is simple, scalable, cost-effective, and incurs minimal computational processing overheads. The proposed solution can support both symmetric and asymmetric based authentication schemes. Furthermore, they demonstrate that the privacy solution is computationally more efficient than two of the more recently proposed smart grid privacy solutions and is more resilient to a wide range of attacks such as replay, known session key and man-in-the middle attacks.

With large-scale AMI deployments, addressing security issues is challenging. In particular, as data travels through several networks, secure end-to-end communication based on strong authentication mechanisms and a robust and scalable key management schemes are crucial for assuring the confidentiality and the integrity of this data [76]. The authors propose an approach based on PUF (physically unclonable function) technology for providing strong hardware based authentication of smart meters and efficient key management to assure the confidentiality and integrity of messages exchanged between smart meters and the utility. This approach does not require modifications to the existing smart meter communication.

In this work, the problem of designing a key management scheme able to achieve secure end-to-end communication in the AMI is addressed. Specifically, their solution provides an efficient approach to manage keys and a strong authentication mechanism. The solution is based on the use of PUF (physically unclonable function) devices, which are inexpensive to manufacture and provide hardware based strong authentication mechanism resistant to spoofing attacks.

The PUF devices' hardware is based on one-way function to generate and re-generate the symmetric keys and access level passwords for smart meters. The PUF based secret generation mechanism provides strong protection against key leakage, as the master key is never stored in memory. PUFs (Physically clonable functions) are one-way functions that are embedded in a physical structure [77]. A PUF takes an input challenge $Ci \in C$, where C is the set of all-possible challenges and produces a response $R_i \in R$, where R is the set of all possible responses. Mathematically, a PUF can be represented as a function PUF: $C \rightarrow R$. The function is based on the intrinsic randomness that exists in the integrated circuit used to generate the response and cannot be controlled. As PUF relies on the random variations during the integrated circuit fabrication process, even two PUFs with the same layout results in two different functions. In other words, it is physically impossible to make two PUFs behave identically. This PUF device is incorporated in a feedback loop for a system-on-chip(SoC) design. The *ECU* (Error Correcting Unit) performs error correction on the PUF response with transmission noise so that, in a real setting, every time the same challenge is given the PUF along with the ECU produces the same response.

The *CC* (Cryptographic Core) is a stand-alone hardware component that provides cryptographic services to the communication board of the smart meter. The operation of the CC depends on the required functionality. In this

approach, the CC implements a secure hashing, and encryption operations for use by smart meters. The Reg(register) stores the initial challenge and then later get overwritten by the subsequent responses from PUFECU component. Notice that PUF-ECU-Reg forms a feedback loop. We utilize this feedback mechanism to generate keys chaining responses in a sequence. This technique is similar to using hash chains to generate one-time keys where a cryptographic hash function is applied repeatedly to obtain a new key.

[77], proposes an efficient and scalable key management protocol for secure unicast, multicast, and broadcast communications in a smart grid network. The proposed protocol is based on a binary tree approach, and supports all these three types of secure communications by using only one binary tree. The analysis and discussion show that the proposed protocol is versatile, and hence suitable for secure smart grid communications.

The authors propose an efficient and versatile key management protocol for secure smart grid communications. The proposed protocol is based on a key management protocol for secure broadcast communications in pay-tv broadcasting systems. This work defines and discusses a new requirement for key management in secure smart grid communications. It also proposes a key management protocol for secure unicast and multicast communications as well as secure broadcast. The proposed key management comprises of three protocols: the system initialization, the key management for secure broadcast communications, and the key management for secure unicast/multicast communications

7. Conclusion

Cyber security has apparently become an important concern globally that needs to be addressed. Smart-grid metering and control systems hold vast opportunities for improving efficiency, convenience and sustainability of electronic data. It is also aimed at providing a scalable, pervasive and interactive communication infrastructure with new energy management and demand response capabilities. Cyber security in the smart-grid metering and control system is a crucial and rapidly growing area that has drawn attention from governments and various industries.

The study presented considered various key management schemes. In general, it is observed that there are two approaches taken for the initial authentication with the network – using a pre-deployed key or dynamically generating a key. Most schemes prefer to use a symmetric key and justify its use with the low computing power required, the low computing delay and the low storage required due to the reduced key length (typically 128 to 160 bits). However, there are schemes that choose to use asymmetric key cryptography, designating an upstream server as a trusted CA. Such schemes use asymmetric key cryptography for the initial authentication and key exchange. A symmetric key is used for encrypting data exchanged.

Schemes that are originally designed for WSNs can be effectively implemented for Smart Grid use. However, there are certain factors that determine the suitability of a specific key management solution. These factors depend upon the functional topology of the Smart Grid segment where the devices are deployed (*i.e.*, a HAN or a NAN). The functional topology, in turn depends upon the data flow patterns (*i.e.*, sensor-to-sensor or sensor-to-NOC), the direction of the flow, radio range and connectivity (single hop *vs* multi-hop) and the data reliability required. This impacts the type of communication that is used to distribute the keys – unicast and multicast/broadcast. Likewise, the choice of using a unique key per sensor or a group key is impacted. Added to these are the limitations of the sensor devices in terms of energy use, computing capability and memory storage. The various key management schemes presented address different aspects mentioned above. It is therefore evident that each of the schemes are efficient for a specific set of factors and no single scheme claims to provide a generic solution, deployable across the Smart Grid, efficiently.

It is to be noted that this survey does not address specifically, the various malicious attacks possible on the Smart Grid. Therefore, it does not comment on the impact of such attacks or the characteristics of various key management schemes to be resilient to such attacks. Node-capture attacks are expected to cause a high impact and have the potential to compromise large portions of the network.

References

[1] T. Flick and J. Morehouse, *Securing the Smart Grid: Next Generation Power Grid Security*: Elsevier Science, 2010.

[2] J. Gao, Y. Xiao, J. Liu, W. Liang, and C. L. P. Chen, "A survey of communication/networking in Smart Grids," *Future Generation Computer Systems*, vol. 28, pp. 391-404, 2012.

[3] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart Grid - The New and Improved Power Grid: A Survey," *Communications Surveys & Tutorials, IEEE*, vol. 14, pp. 944-980, 2012.

[4] K. Iniewski, *Convergence of Mobile and Stationary Next-Generation Networks*: Wiley, 2011.

[5] F. Rahimi and A. Ipakchi, "Overview of Demand Response under the Smart Grid and Market paradigms," in *Innovative Smart Grid Technologies (ISGT), 2010*, 2010, pp. 1-7.

[6] P. K. Steimer, "Enabled by high power electronics-Energy efficiency, renewables and smart grids," in *Power Electronics Conference (IPEC), 2010 International*, 2010, pp. 11-15.

[7] N. E. Bassam, P. Maegaard, and M. L. Schlichting, *Distributed Renewable Energies for Off-grid Communities: Strategies and Technologies Toward Achieving Sustainability in Energy Generation and Supply*: Elsevier, 2013.

[8] E. D. Knapp and J. Langill, *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*: Syngress, 2011.

[9] N. Kayastha, D. Niyato, E. Hossain, and Z. Han, "Smart grid sensor data collection, communication, and networking: a tutorial," *Wireless Communications and Mobile Computing*, pp. n/a-n/a, 2012.

[10] J. Weiss, *Protecting Industrial Control Systems from Electronic Threats*: Momentum Press, 2010.

[11] E. D. Knapp and R. Samani, "Chapter 1-What is the Smart Grid?," in *Applied Cyber Security and the Smart Grid*, ed Boston: Syngress, 2013, pp. 1-15.

[12] R. L. Krutz, *Securing SCADA Systems*. Indianapolis, Indiana: Wiley Publishing, 2006.

[13] F. Daryabar, A. Dehghantanha, N. I. Udzir, N. F. B. M. Sani, and S. bin Shamsuddin, "Towards secure model for SCADA systems," in *Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on*, 2012, pp. 60-64.

[14] S. Nabil and B. Mohamed, "Security solution for semantic SCADA optimized by ECC mixed coordinates," in *Information Technology and e-Services (ICITeS), 2012 International Conference on*, 2012, pp. 1-6.

[15] J. A. Zubairi and A. Mahboob, *Cyber Security Standards, Practices and Industrial Applications: Systems and Methodologies*: Igi Global, 2011.

[16] B. Shahid, Z. Ahmed, A. Faroqi, and R. M. Navid-ur-Rehman, "Implementation of smart system based on smart grid Smart Meter and smart appliances," in *Smart Grids (ICSG), 2012 2nd Iranian Conference on*, 2012, pp. 1-4.

[17] Fadi Aloula, A. R. Al-Alia , Rami Al-Dalkya, M. Al-Mardinia, and a. W. El-Hajjb, "Smart Grid Security: Threats, Vulnerabilities and Solutions " *International Journal of Smart Grid and Clean Energy* vol. 1, 2012.

[18] M. Badra and S. Zeadally, "Key management solutions in the smart grid environment," in *Wireless and Mobile Networking Conference (WMNC), 2013 6th Joint IFIP*, 2013, pp. 1-7.

[19] L. Nian, C. Jinshan, Z. Lin, Z. Jianhua, and H. Yanling, "A Key Management Scheme for Secure Communications of Advanced Metering Infrastructure in Smart Grid," *Industrial Electronics, IEEE Transactions on*, vol. 60, pp. 4746-4756, 2013.

[20] S. S. Iyengar and R. R. Brooks, *Distributed Sensor Networks, Second Edition: Sensor Networking and Applications*: Taylor & Francis, 2012.

[21] M. Z. Huq and S. Islam, "Home Area Network technology assessment for demand response in smart grid environment," in *Universities Power Engineering Conference (AUPEC), 2010 20th Australasian*, 2010, pp. 1-6.

[22] E. Hossain, Z. Han, and H. V. Poor, *Smart Grid Communications and Networking*: Cambridge University Press, 2012.

[23] L. T. Berger and K. Iniewski, *Smart Grid Applications, Communications, and Security*: Wiley, 2012.

[24] F. Bouhafs, M. Mackay, and M. Merabti, "Links to the Future: Communication Requirements and Challenges in the Smart Grid," *Power and Energy Magazine, IEEE*, vol. 10, pp. 24-32, 2012.

[25] N. Saputro, K. Akkaya, and S. Uludag, "A survey of routing protocols for smart grid communications," *Computer Networks*, vol. 56, pp. 2742-2771, 2012.

[26] S. S. S. R. Depuru, L. Wang, and V. Devabhaktuni, "Smart meters for power grid: Challenges, issues, advantages and status," *Renewable and Sustainable Energy Reviews*, vol. 15, pp. 2736-2742, 2011.

[27] J. A. Cardenas, L. Gemoets, J. H. Ablanedo Rosas, and R. Sarfi, "A literature survey on Smart Grid distribution: an analytical approach," *Journal of Cleaner Production*.

[28] W. Wang and Z. Lu, "Cyber security in the Smart Grid: Survey and challenges," *Computer Networks*, vol. 57, pp. 1344-1371, 2013.

[29] S. Massoud Amin, "Smart Grid: Overview, Issues and Opportunities. Advances and Challenges in Sensing, Modeling, Simulation, Optimization and Control," *European Journal of Control*, vol. 17, pp. 547-567, 2011.

[30] L. Luo, N. Tai, and G. Yang, "Wide-area Protection Research in the Smart Grid," *Energy Procedia*, vol. 16, Part C, pp. 1601-1606, 2012.

[31] M. Fadaeenejad, A. M. Saberian, M. Fadaee, M. A. M. Radzi, H. Hizam, and M. Z. A. AbKadir, "The present and future of smart power grid in developing countries," *Renewable and Sustainable Energy Reviews*, vol. 29, pp. 828-834, 2014.

[32] E. Ancillotti, R. Bruno, and M. Conti, "The role of communication systems in smart grids: Architectures, technical solutions and research challenges," *Computer Communications*.

[33] P. Stavroulakis and M. Stamp, *Handbook of Information and Communication Security*: Springer, 2010.

[34] Z. Zhang, H. Liu, S. Niu, and J. Mo, "Information security requirements and challenges in smart grid," in *Information Technology and Artificial Intelligence Conference (ITAIC), 2011 6th IEEE Joint International*, 2011, pp. 90-92.

[35] L. Husheng, L. Lifeng, and R. C. Qiu, "A denial-of-service jamming game for remote state monitoring in smart grid," in *Information Sciences and Systems (CISS), 2011 45th Annual Conference on*, 2011, pp. 1-6.

[36] L. Zhuo, W. Wenye, and C. Wang, "Hiding traffic with camouflage: Minimizing message delay in the smart grid under jamming," in *INFOCOM, 2012 Proceedings IEEE*, 2012, pp. 3066-3070.

[37] S. Ruj and A. Nayak, "A Decentralized Security Framework for Data Aggregation and Access Control in Smart Grids," *Smart Grid, IEEE Transactions on*, vol. 4, pp. 196-205, 2013.

[38] M. Jung, T. Hofer, S. Dobelt, G. Kienesberger, F. Judex, and W. Kastner, "Access control for a Smart Grid SOA," in *Internet Technology And Secured Transactions, 2012 International Conferece For*, 2012, pp. 281-287.

[39] M. B. Line, I. A. Tondel, and M. G. Jaatun, "Cyber security challenges in Smart Grids," in *Innovative Smart Grid Technologies (ISGT Europe), 2011 2nd IEEE PES International Conference and Exhibition on*, 2011, pp. 1-8.

[40] E. Pallotti and F. Mangiatordi, "Smart grid cyber security requirements," in *Environment and Electrical Engineering (EEEIC), 2011 10th International Conference on*, 2011, pp. 1-4.

[41] W. Stallings, *Cryptography and Network Security: Principles and Practice, International Edition: Principles and Practice*: Pearson Education Limited, 2014.

[42] Alfred J. Menezes, P. C. v. Oorschot, and a. S. A. Vanstone, *Handbook of Applied Cryptography*, 1996.

[43] H. R. Nemati and L. Yang, *Applied Cryptography for Cyber Security and Defense: Information Encryption and Cyphering*: Information Science Reference, 2011.

[44] W. Wang and Z. Lu, "Survey Cyber security in the Smart Grid: Survey and challenges," *Comput. Netw.*, vol. 57, pp. 1344-1371, 2013.

[45] J. Kamto, Q. Lijun, J. Fuller, and J. Attia, "Light-weight key distribution and management for Advanced Metering Infrastructure," in *GLOBECOM Workshops (GC Wkshps), 2011 IEEE*, 2011, pp. 1216-1220.

[46] S. Das, Y. Ohba, M. Kanda, D. Famolari, and S. K. Das, "A key management framework for AMI networks in smart grid," *Communications Magazine, IEEE*, vol. 50, pp. 30-37, 2012.

[47] Sungjin Lee, Donghyun Choi, a. Choonsik Park, and S. Kim, "An Efficient Key Management Scheme for Secure SCADA Communication," *World Academy of Science, Engineering and Technology*, vol. 45, 2008.

[48] S. Mittra, "Iolus: a framework for scalable secure multicasting," presented at the Proceedings of the ACM SIGCOMM '97 conference on Applications, technologies, architectures, and protocols for computer communication, Cannes, France, 1997.

[49] W. Chung Kei, M. Gouda, and S. S. Lam, "Secure group communications using key graphs," *Networking, IEEE/ACM Transactions on*, vol. 8, pp. 16-30, 2000.

[50] C. Donghyun, L. Sungjin, W. Dongho, and K. Seungjoo, "Efficient Secure Group Communications for SCADA," *Power Delivery, IEEE Transactions on*, vol. 25, pp. 714-722, 2010.

[51] C. Donghyun, K. Hakman, W. Dongho, and K. Seungjoo, "Advanced Key-Management Architecture for Secure SCADA Communications," *Power Delivery, IEEE Transactions on*, vol. 24, pp. 1154-1163, 2009.

[52] C. L. Beaver, D.R. Gallup, W. D. NeuMann, and a. M. D. Torgerson. Key Management for SCADA [Online]. Available: http://energy.sandia.gov/wp/wp-content/gallery/uploads/013252.pdf

[53] T. Huei-Ru, "A secure and privacy-preserving communication protocol for V2G networks," in *Wireless Communications and Networking Conference (WCNC), 2012 IEEE*, 2012, pp. 2706-2711.

[54] S. Zhu, S. Setia, and S. Jajodia, "LEAP+: Efficient security mechanisms for large-scale distributed sensor networks," *ACM Trans. Sen. Netw.*, vol. 2, pp. 500-528, 2006.

[55] W. Chung Kei, M. Gouda, and S. S. Lam, "Secure group communications using key graphs," *Networking, IEEE/ACM Transactions on*, vol. 8, pp. 16-30, 2000.

[56] C. Donghyun, L. Sungjin, W. Dongho, and K. Seungjoo, "Efficient Secure Group Communications for SCADA," *Power Delivery, IEEE Transactions on*, vol. 25, pp. 714-722, 2010.

[57] C. Donghyun, K. Hakman, W. Dongho, and K. Seungjoo, "Advanced Key-Management Architecture for Secure SCADA Communications," *Power Delivery, IEEE Transactions on*, vol. 24, pp. 1154-1163, 2009.

[58] C. L. Beaver, D.R. Gallup, W. D. NeuMann, and a. M. D. Torgerson. Key Management for SCADA [Online]. Available: http://energy.sandia.gov/wp/wp-content/gallery/uploads/013252.pdf

[59] T. Huei-Ru, "A secure and privacy-preserving communication protocol for V2G networks," in *Wireless Communications and Networking Conference (WCNC), 2012 IEEE*, 2012, pp. 2706-2711.

[60] L. Yee Wei, M. Palaniswami, G. Kounga, and A. Lo, "WAKE: Key management scheme for wide-area measurement systems in smart grid," *Communications Magazine, IEEE*, vol. 51, pp. 34-41, 2013.

[61] S. Zhu, S. Setia, and S. Jajodia, "LEAP+: Efficient security mechanisms for large-scale distributed sensor networks," *ACM Trans. Sen. Netw.*, vol. 2, pp. 500-528, 2006.

[62] L. Yue, "Design of a Key Establishment Protocol for Smart Home Energy Management System," in *Computational Intelligence, Communication Systems and Networks (CICSyN), 2013 Fifth International Conference on*, 2013, pp. 88-93.

[63] J.-Y. Kim and H.-K. Choi, "An efficient and versatile key management protocol for secure smart grid communications," in *Wireless Communications and Networking Conference (WCNC), 2012 IEEE*, 2012, pp. 1823-1828.

[64] W. Dapeng and Z. Chi, "Fault-Tolerant and Scalable Key Management for Smart Grid," *Smart Grid, IEEE Transactions on*, vol. 2, pp. 375-381, 2011.

[65] H. Nicanfar, P. Jokar, and V. C. M. Leung, "Smart grid authentication and key management for unicast and multicast communications," in *Innovative Smart Grid Technologies Asia (ISGT), 2011 IEEE PES*, 2011, pp. 1-8.

[66] Gyorgy Dan, King-Shan Lui, Rehana Tabassum, Quanyan Zhu, and Klara Nahrstedt3, "SELINDA: A Secure, Scalable and Light-Weight Data Collection Protocol for Smart Grids," IEEE Smartgridcomm 2013 Symposium-smart grid cybersecurity and privacy pp. 480-485, 2013.

[67] Fangming Zhao, Yoshikazu Hanatani, Yuichi Komano, Ben Smyth, Satoshi Ito, Tom Kambayashi, "Secure Authenticated Key Exchange with Revocation for Smart Grid". IEEE. 2011.

[68] H. Nicanfar and V. C. M. Leung, "Password-authenticated cluster-based group key agreement for smart grid communication," security and communication networks vol. 2, pp. 221-233, 2014.

[69] Kuan Zhang, Rongxing Lu, Xiaohui Liang, Jian Qiao, and Xuemin (Sherman) Shen, " PARK: A Privacy-preserving Aggregation Scheme with Adaptive Key Management for Smart Grid," IEEE/CIC international conference on communication in china (ICCC): QRS: QOS, Reliability and security, 2013, pp. 236-241.

[70] Depeng Li, Zeyar Aung, John R. Williams & Abel Sanchez," No peeking: privacy-preserving demand response system in smart grids," International Journal of Parallel, Emergent and Distributed Systems (2013).

[71] J. Kamto, L. Qian, J. Fuller, J. Attia, "Light-weight key distribution and management for Advanced Metering Infrastructure", IEEE International Workshop on Smart Grid Communications and Networks, 2011.

[72] J. Kamto, L. Qian, J. Fuller, J. Attia and Y. Qian, "Key Distribution and Management for Power Aggregation and Accountability in Advance Metering Infrastructure," IEEE Smartgridcomm 2012 Symposium-cybersecurity and privacy, pp. 360-365. 2012.

[73] S.H. Seo, X. Ding and E. Bertino, "Encryption Key Management for Secure Communication in Smart Advanced Metering Infrastructures," IEEE Smartgridcomm 2013 Symposium-cybersecurity and privacy, pp. 498-503. 2013.

[74] H. Nicanfar, P. Jokar, K. Beznosov, and V. C. M. Leung, "Efficient Authentication and key management mechanisms for smart grid communications", IEEE systems journal 2013.

[75] M. Badra and S. Zeadally, "Design and Performance Analysis of a virtual ring architecture for smart grid privacy", IEEE transactions on information forensics and security, vol. 9, no. 2, 2014.

[76] M. Nabeel, S. Kerr, X. Ding, E. Bertino, " Authentication and Key Management for Advanced Metering Infrastructures Utilizing Physically Unclonable Functions", IEEE Smartgridcomm 2012 Symposium-cybersecurity and privacy. pp. 324-329.

[77] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Silicon physical random functions," in *CCS '02*. New York, NY, USA: ACM, 2002, pp. 148-160.

[78] X. Long, D. Tipper, and Y. Qian, "An Advanced Key Management Scheme for Secure Smart Grid Communications", IEEE Smartgridcomm 2013 Symposium-cybersecurity and privacy. pp. 504-509.

[79] P. V. Jasud, M. D. Katkar, S. D. Kamble, "Authentication Mechanism for Smart Grid Network International Journal of Soft Computing and Engineering (IJSCE).

[80] M. Ibrahim, M. M. Salama, "Smart distribution system volt/VAR control using distributed intelligence and wireless communication" in *IET Generation, Transmission & Distribution, 9* (4), 2015, 307-318.

[81] Bashar Alohali, Madjid Merabti, and Kashif Kifayat "Key Management in Smart Grid: A Survey", ISBN: 978-1-902560-27-4.