An Efficient ECIES based Encryption scheme for Smart Grids in Wireless Communication

Rishi Kushwah\(^1\), Sini Shibu\(^2\)

\(^1,2\) Computer Science and Engineering, NRIIST, Bhopal, India

Abstract — The next evolution of the Smart Grid represents will involve the development and mixing of proceed communications and information technology into all aspects to further improve and optimize the power generation, delivery consumption and other effectiveness operations. The increased functionality joined together with the integration into information systems also comes with increased safety and privacy of user-related data is of vital importance in Smart Grid circumstances and a key consideration is to make certain cyber security, particularly as schemes that have conventionally been physically-isolated, closed and proprietary change towards more networked, open architectures based on IP standards.

For the instant, the environments of smart grids and smart buildings—such as having limited computation power of smart devices and limitations in communication network capabilities, while requiring being extremely consistent make key based scheme is a challenging task.

Index Terms— Component, formatting, style, styling, insert. (key words)

I. INTRODUCTION

Smart Grid is the movement of next generation power distribution and management network that make possible interactive communication and operation between consumers and providers, so as to accomplish intellectual reserve allocation management and to make more efficient. The wireless mesh network technology shows potential infrastructure solution to highlight and support these smart functionalities flexibly and scalable, as well as it can provide redundant routes for the smart grid communication network to guarantee the network availability. On the other hand, the wireless mesh network infrastructure is vulnerable to some cyber-attacks which need to be addressed. The Smart Grid refers to a modernized power delivery and monitoring system that intends to substitute the deprecated electrical grid of the 20th century. Technological breakthroughs during the past decades in the field of information and communication technology have facilitated the development of the Smart Grid.

Figure: The advancement of the power grid.

For a century, utility companies have had to send workers out to gather much of the data needed to provide electricity. The workers read meters, look for broken equipment and measure voltage. However, increasing automation and communications within the electricity grid potentially has a dark side allowing increased vulnerability to attack. In order to deploy the two-way communication, one possible solution is to use advanced metering infrastructure (AMI) that contains a key component in the smart grid system called smart meter. A smart meter usually has a processing chip and a nonvolatile storage so that it can perform smart functions like being able to report periodic usage updates to end-users as well as the generation facilities at Power Company and interact directly with “smart” appliances at home to control them [13]. For example. Most of the devices utilities use to deliver electricity have until now to be automated and computerized. Now, many options and products are being made available to the electricity industry to make grow it. A key characteristic of the smart grid is automation technology that lets the effectiveness regulate and be in command of each individual device or millions of devices from a central location.
Using two-way flow of electricity and information, smart grid manufactures an automated, highly distributed energy escape network. It integrates real-time information switch over with the intention to balance supply and demand [12]. The main smart grid services include:

- **Automatic meter reading.**
- **Power grid monitoring:** electrical assets such as voltage and current of the power grid infrastructure are monitored.
- **Demand side management:** it is comprised of two parts:
  - Load shifting/demand response.
  - Energy conservation, e.g., using energy efficient products [10]
- Home networking between electrical gadgets for energy management.
- **Vehicle to power grid technology:** vehicles store power during off hit the maximum position hours and send it back to the power grid for the duration of on peak hours.

Smart grid consists of seven major blocks namely: bulk generation, transmission, distribution, operation, market, customer and service provider [11].

As well, under the demand response program, several customers allow the usefulness companies to control their smart electric devices at home. Hence, utilities are allowed to turn the customers devices off in case of emergency or during peak hours.

- **Power quality for the 21st century:** through monitoring the power factors such as current and voltage, the power work forces are able to identify the power grid problems.
- **Integration of all generations and storage options:** smart grid aims to integrate distributed electrical generations, e.g., renewable energies with the power grid and micro grids. Thus, managing the produced power would be easier.
- **Self healing:** the power grid would be able to heal itself automatically. It can decide based on the collected data and react dynamically.
- **Flexibility against attacks and disasters:** this characteristic can be provided by increasing power grid robustness, protecting key assets from physical attacks and providing sufficient redundancy in the power grid [12].
- **Asset management and operational efficiency:** quality of assets and how efficient they are working in the power grid will be monitored. For example, the cable temperature is measured. New markets and operations: smart grid will integrate and open new businesses to the power grid. For instance, it integrates IT infrastructure to the power grid; smart devices are needed to be designed and communication infrastructures are needed to be developed.

To get accomplish the above-point out goals there is a need for communication infrastructure to provide a two-way communication between the service side and customer side.

### III. SMART GRID KEY COMPONENTS

The SG incorporates a collection of enabling technologies and components that facilitate its orderly operation [13].

Integrated Communications: Integrated communication technologies are a critical component of the SG. All the data produced during the SG operation has to be transmitted from and to several other SG entities. However, different SG components use different communication protocols. In fact, this non-uniformity is an impediment towards an effective, fully-integrated communication infrastructure. Integrated communications is believed to create a dynamic and interactive grid where users and sophisticated devices, such as control centers and smart meters, will interact efficiently.

Sensing and Measurement: Sensing and measurement technologies of the SG primarily focus on the evaluation of the equipment health and the integrity of the infrastructure.
They also help mitigate congestions and radically reduce emissions by engaging motivated customers into DR programs. Advanced sensing and measurement technologies include, among others, smart meters, asset condition monitors and wide area monitoring systems (WAMS). In particular, smart meters describe digital meters that record energy usage data and frequently report their measurements both to the users and the utility company. The communication of the power usage information is backed by the advanced metering infrastructure (AMI). In its turn, the AMI is an architecture that automates and facilitates the bidirectional communication between the smart meters and the aforementioned stakeholders.

Advanced Control Methods: Advanced Control Methods aspire to provide the appropriate technologies in terms of hardware and software which will contribute in analyzing, diagnosing and predicting the conditions under which Smart Grid’s orderly operation can fail. Moreover, advanced SG devices and algorithms assist in determining the appropriate actions to be taken when alert conditions are identified. The ultimate objective is the avoidance of outages and power quality disturbances. Advanced control functions are supported by distributed intelligent systems (control agents), analytical tools (statistical algorithms) and operational applications such as SCADA and substation automation.

Advanced Electric Components: The modern grid needs advanced electric components to meet the performance requirements in power transmission and distribution. Consequently, they determine the electrical behavior of the grid. Advanced components realization has relied on the significant research and development efforts in the areas of power electronics, superconductivity, materials and chemistry. Examples of such components are the distributed generation and energy storage, the fault current limiters, the advanced switches and conductors, the solid state transformers as well as the microgrids.

Improved Interfaces & Decision Support: Improved interfaces and decision making (IIDS) are essential enabling technologies for the SG. The focus of this Smart Grid component is the transformation of complex power-system data to comprehensible information. It is achieved by virtual reality approaches and other sophisticated data-display techniques. As an immediate consequence, the operators can identify potential problems faster and take the appropriate actions to prevent them. IIDS technologies include, among others, visualization, decision support and system operator training.

IV. SMART GRID COMMUNICATION NETWORKS AND ITS REQUIREMENTS

Smart Grid is an intelligent network built in some integrated, high-speed, two-way communication networks. Its intention is to put into operation the power reliability, security, and efficiency, as well as clean energy supply by using advanced sensor technology, measurement technology and advanced decision support systems. Smart Grid transmits a extensive range of data, including the key tools function parameters, the power facility information, the power distribution and scheduling information, the electricity usage state, early warning information, and so on. By using the rich information, Smart Grid can efficiently control the power generation, transmission, distribution, scheduling, and sub-time pricing, as well as timely error check etc. The hierarchical model of information flows in Smart Grid is shown in Figure.

![Figure: The hierarchical model of information flows in Smart Grid.](image-url)
The communication networks related to Smart Grid consist of cable networks and wireless networks. The wireless networks mainly refer to wireless sensor networks that are usually used in some places where cable networks are not applicable to deploy or wireless sensor networks is more suitable. Smart Grid has a remarkable feature that its networks must be safer than other networks for general purposes. To be precise to say, Smart Grid must survive the physical destructions and malicious network attacks without blackouts or a high cost of recovery. Smart Grid security involves many aspects, where the data transmission security is one of the most important issues. Since the security mechanisms and techniques in cable networks are already quite rich and mature, we focus on trying to improve the security of the data in wireless sensor networks for Smart Grid.

Wireless sensor networks are a multi-hop self-organized network system, which contains a large amount of miniaturized sensor nodes. These sensor nodes are distributed in an examined area, and communicate in a multi-hop ad hoc way. They collaborate with each other to collect the sensitive information of monitored objects, and send them to a decision sustain interior. The purposes of wireless sensor networks consist of data collection, data transmission, and data scrutiny and processing. A sensor node, the smallest logical unit of wireless sensor networks, is a micro-system, which is combined by sensor modules, data processing modules and communication modules. Sensor nodes ever-increasing wireless connections to form self-organized and distributed network architecture, depending on a certain network routing protocol that can fuse and aggregate the collected data and transmit them to the information processing centre.

Network architecture of wireless sensor networks is shown in figure Smart Grid involves a large number of wireless sensor networks, so the data transmission security is an important issue in Smart Grid. On the other hand, due to wireless sensor networks with the large magnitude of energy-constrained sensor nodes and the high network dynamics originate by the node mobility or node failure, there still exist a lot of probable threats to the protection of wireless sensor networks.

- The unauthorized interception of information. A sensor node transmits information to others by transmitting, so any of communication pieces of equipments within its RF radius may receive and intercept the information.
- Sensor nodes are vulnerable to be captured easily. We must take into account what measurements should be taken to fight against, while a sensor node is captured and used as a pseudo terminal to launch malicious attacks.
- In the realistic situations, we must also consider which routing methods should be adopted, in the case that some of sensor nodes do not work because of failures or attacks.
- Tampering with information is usually regarded as the most dangerous attack. The tampered information can be spread throughout networks like normal messages, which can attack or even control the whole networks.

These potential threats to wireless sensor networks cause unsafe data communications in Smart Grid. To obtain safe communication services from Smart Grid, we must solve the security issues about wireless sensor networks. However, because of the differences between wireless sensor networks and conventional networks, the security guidelines for wireless sensor networks should not be borrowed directly from the existing mature security solutions for traditional networks. The security guidelines should be more appropriate for wireless sensor networks.

Data encryption methods are widely used in traditional networks, where the information needed to be protected is generated to cipher-text information without readability or understandable relationship. Yet the resources of computation and storage at sensor nodes are inadequate and incomplete. The conventional data encryption schemes will sincerely put away the costly resources at sensor nodes, because they necessitate more power and memory space to achieve the data encryption procedure. Therefore, we need to use digital watermarking methods to implement the security policies in wireless sensor networks, because digital watermarking needs much less resources at sensor nodes than traditional data encryption.

The appearance of machine-to-machine (M2M) communication has also begun in developing smart power grid.
Such communication happens among different components of smart grid such as sensors, smart meters, gateways and other intelligent devices [10]. A three-level hierarchy can be defined for smart grid communication network which includes the Home Area Network (HAN), Neighborhood area network and Wide Area Network (WAN). In smart grid advanced metering infrastructure (AMI) makes use of the HAN, NAN and WAN for metering-related functions.

It consists of designing them from scratch with security in mind, as opposed to adding security features to an already built product. Security-in depth implies the realization that any security feature by itself is breakable with enough effort, and only multiple security barriers layered in a concentric way around protected assets can provide a security level superior to the sum of the individual parts. End-to-end security relates to the fact that the security of a network is as strong as it weakest link. Therefore, network administrators have to maintain the same level of security in all segments of the network.

Low latency, high reliability, scalability and security are the characteristics that describe the SGCN. The SGCN is responsible for collecting and transmitting data between all the nodes/actors of the smart grid. According to the, latency and reliability are considered to be the main SGCN requirements.

Latency: As stated in, latency is defined as the summation of the node processing time and network processing time from the sending node to the receiving node. For each kind of smart grid data traffic, a certain amount of latency is acceptable. Some components of the SGCN are more latency tolerant while some are less and need a quick response. Reliability: The probability that an operation will complete without failure over a specific period.

Bandwidth: Bandwidth represents how much data can be sent over a specific network connection per given unit of time. The IEEE P230 standard is still trying to precisely define the bandwidth requirements for a SGCN.

Security: Smart grid data traffic such as billing, signal prices and control messages is very important traffic that needs to be encrypted and prevented from malicious changes and unauthorized access. Integrity (no malicious modification), and authenticity (message originality and access rights) are the important security aspects in a SGCN.

V. COMMUNICATION NETWORK ARCHITECTURE IN THE SMART GRID

In this part, we here present the essential design of communication networks in the Smart Grid, which is followed by widely-adopted communication protocols for power grids.

Fundamental Architecture: Electric power systems are very complex physical networks. For example, statistics [12] showed that there are over 2000 power distribution substations, about 5600 distributed energy facilities, and more than 130 million customers all over the US.

According to NIST’s conceptual model [12], the Smart Grid consists of seven logical domains: massiveness Generation, Transmission, allotment, Customer, Markets, Service Provider and Operations.
The first four feature the two-way power and information flows. The last three feature information collection and power management in the Smart Grid. In order to interconnect all these domains, the communication network must be highly-distributed and hierarchical. As shown in Fig. 1, we represent the Smart Grid communication network onto a hybrid and hierarchical network, including the back network and millions of local-area networks. The backbone network is established for inter-domain communication. It consists of communications nodes, which can be either gateways for local-area networks or high-bandwidth routers to forward messages across a variety of domains in the Smart Grid. In the backbone network, conventional wire line communication technologies, such as fiber optical technologies, can be used to achieve high speed data and bulk information delivery across domains. For example, the SCADA system is a power operation monitoring system across the Operations, Transmission, and Distribution domains. All power signal quality samples are delivered from local-area systems in Transmission and Distribution domains via the backbone network to the Operations domain for centralized management.

A local-area network is used for intra-domain communication. A local-area network consists of ad-hoc nodes, which are meters, sensors or intelligent electronic devices (IEDs), installed on the power infrastructure. They are usually equipped with limit bandwidth and computational ability for certain monitoring or protection purposes. Ad-hoc nodes in a local-area network are not limited to use wire line communication. It has been shown that there are a number of advantages for using wireless communication technologies in the Smart Grid [12–12], including untethered access to utility information, mobility, reduced cost, low complexity, and off-the-shelf products such as WiFi and ZigBee. Alongside research efforts, industry companies are also endeavoring to develop new wireless communication products for the Smart Grid. For example, ZigBee embedded products have been released recently to target the Smart Grid applications, such as smart meters, demand response, and home-area network devices for the AMI system in the Customer domain [10].

Therefore, comparing with legacy power systems, the Smart Grid will leverage both wire line and wireless network technologies to provide a revolutionary paradigm of large-scale, highly-distributed, and hierarchical communication infrastructures for energy delivery and management in the future. To ensure secure and reliable operation, such a complicated information system requires a comprehensive security treatment [10] based on the specific features in the Smart Grid communication network, which will be described in the following subsection.

Features of Smart Grid Communication Networks: It is evident that the Smart Grid communication network is similar to the Internet in terms of the complexity and hierarchical structure. However, there are fundamental differences between these two complex systems in many aspects.

Performance metric: The basic function of the Internet is to provide data services (e.g., web surfing and music downloading, etc.) for users. How to achieve high throughput and fairness among users is of great importance in the Internet design. Whereas, power communication networks are used not to provide high-throughput services, but to ensure reliable, secure, and real-time message delivery and non-real-time monitoring and management. Hence, latency is much more important than the throughput in power systems, leading to delay-oriented design in power communication protocols. For example, in power substation communications, time-critical messages for protection purposes are passed from the application layer directly to the MAC layer to avoid redundant processing [10].

Traffic model: It is well known that many Internet traffic flows have the self-similarity property, such as the World Wide Web (WWW) traffic [10]. In power networks, however, a large amount of traffic flows are periodic [09, 09] for the purpose of consistent monitoring, such as raw data sampling in power substations and periodic meter reading in home-area networks [12]. Thus, it can be expected that the majority, if not all, of communication traffic in the Smart Grid differs from that in the Internet.

Timing requirement: Over the Internet, most IP traffic is best-effort traffic while the delay-sensitive traffic has delay requirements of 100–150 ms in order to support voice-over-IP and multimedia services [5]. However, the Smart Grid features a wider range of delay requirements from milliseconds to minutes [12]. Therefore, the Smart Grid has much more stringent timing requirements for message delivery than the Internet.

Communication model: The end-to-end principle is the basis of the Internet such that it can support peer-to-peer communication between any node pair in the world. In legacy power grids, the most commonly used communication model is one-way communication: electronic devices report their readings to the control center. In contrast, the Smart Grid enables a two-way communication model: top-down (center to device) and bottom-up (device to center). The Smart Grid also supports the peer-to-peer communication model, but usually restricts the model in local-area networks for security concerns [10, 12].
Protocol stack: The Internet is built upon the IP protocol and is moving forward to IPv6. It has been widely expected that the Smart Grid will use IPv6 [12] as the major network-layer protocol. However, the Smart Grid is not limited to IPv6 and can have heterogeneous protocol stacks, depending on network functionalities and requirements. For example, ATM switching has been proposed to guarantee quality-of-service (QoS) for time-critical message delivery in power transmission systems. As a result, the Smart Grid will feature heterogeneous protocol stacks for a variety of applications.

We can see that although the Internet offers a paradigm for the design of large-scale communication network infrastructures, the design of communication networks for the Smart Grid still needs to be revisited comprehensively to ensure efficient, robust and secure information delivery for energy management of a variety of power facilities.

VI. SMART GRIDS ATTACKS

How was point out before the grid connected to the network could suffer several kinds of attacks, Chen, Cheng, and Chen, in [11] introduces three main attack categories and their countermeasures in smart grid communication networks.

Vulnerability attack: This type of attack is induced by the malfunction of a device or communication channel, or the de-synchronization of feedback information. Feedback information may be deteriorated by erroneous data delivery or unreliable channel conditions, which leads to an incorrect control process at the control center. The vulnerability attack is mainly caused by the inherent reliability in the communication network instead of malicious attacks with specific attempts, and it can be prevented by introducing the fault diagnosis scheme to infer the fault detection and localization.

Data injection attack: This type of attack alter the measurements of some meters in order to manipulate the operations of the smart grid. Although the integrity of meter data and commands is important, their damage is mostly limited to revenue loss. In addition, countermeasures with which it is possible to defend against malicious data injection if a small subset of measurements can be made immune to the data injection attacks.

Intentional attack: If an adversary is able to have full understanding of the network topology, it can fully utilize the network structure to disrupt the network operations by paralyzing some fraction of nodes with the highest degree. Intentional attack can be implemented via coordinated denial-of-service (DoS) attack and contributes to network disruption due to node disconnections in the communication network. From a graph-theoretic point of view, an intentional attack on a specific node is identical to node removal on the corresponding network.

VII. PRIVACY IN THE SMART GRID

Smart grid AMI brings on new security challenges since it is composed of the devices that are placed in physically insecure locations and it makes use of wireless communication that can be possibly corrupted. These resources can be accessed by careless or malicious users. Cleveland in [10] discusses the security requirements and related threats of the main components of an AMI. Security concerns for AMI can be classified into:

Information Confidentiality and in particular, privacy, which can strongly affect the customers’ view of deploying smart grid. Customers might not like unauthorized people, or companies to know about their usage patterns. Usage patterns also can reveal life habits and even the presence/absence of residents that could be used by thieves. If people’s concerns are not satisfied, they may refuse to cooperate in deploying smart grid, i.e., they may refuse to let the utility providers install smart meters at their places.

Information Integrity in AMI systems means preventing any changes in the metering data received form meters and control commands sent to the meters. One of the scenarios that may happen is when a hacker sends disconnect command by breaching into a meter management system and disconnects millions of smart meters.

Information Availability is considered as the most crucial requirement in AMI since some systems or applications are real time and they possibly deal with the availability of power.

Information Non-repudiation is also needed since different entities are involved in financial transactions, owning data and even generating control commands. Audit logs of interactions are mainly used for non-repudiation, although these logs can be affected by integrity and availability attacks.

Information Privacy: Information privacy is another critical concern in Smart Grid communication network. As customer’s information is available on the Smart Grid in service providers database some parties like business adversaries may misuse this information for marketing competition.

In AMI, availability and integrity of data take precedence over confidentiality. Attacks targeting AMI can be classified into three categories: network compromise, system compromise and denial of service (DoS) [10]. Traffic modification, false data injection, replay and traffic analysis attacks try to compromise the network while compromised node and spoofing of metering devices, authentication violation and access to encryption keys are examples of attacks which target the systems. Flaws or misuses of routing, configuration, name resolution and signal jamming are considered as DoS attacks.
Smart Grid intends to substitute the traditional electrical grid while offering, at the same time, new opportunities for the utility companies. For instance, load monitoring could assist the operators to foresee future power consumption and to adjust their production and delivery approaches. AMI supports advanced SG operations such as load monitoring, power generation planning as well as demand response. These can be achieved by constantly sending consumption data towards the utility facilities and more specifically to Energy Management Control System (EMCS). Such a control system requires a continuous flow of information in order to perform efficiently. Nevertheless, frequently sent, fine-grained data transmission introduces new challenges that have to be addressed. Privacy related issues are of significant value since there having been proofs that individuals’ privacy could be violated [13].

Non-Intrusive Load Monitoring: Non-intrusive load monitoring, usually abbreviated as NILM or NALM, refers to set techniques that enable the identification of appliances usage in the customers’ premises. The information that a NILM process can infer refers to the type of appliances and their state (on or off) associated with the respective time-frame. Much like an AMI records the power consumption; a non-intrusive sensor is needed in order to provide the necessary aggregated data for the identification procedure. The aggregated data corresponds to house-wide or room-wide power consumption information. Even though AMI and NILM sensors are technically similar, the NILM sensors record the power trace in a higher frequency, usually at second or sub-seconds intervals. NILM techniques are characterized as non-intrusive because they eliminate the need for outlet or appliance-level meters or other laborious and intrusive sensors in the household.

Non-intrusive load monitoring is used for a variety of reasons. First and foremost, it assists in analyzing the power consumption patterns and designing techniques to achieve energy demand reduction. Moreover, load forecasting can be supported while NILM algorithms also contribute information for energy saving audits. Collecting load data, designers of appliances can develop more environmental friendly apparatus whereas utilities can detect appliance failure. Last but not least, NILM technology enables demand side load management and contributes in the implementation of incentive programs for particular appliance usage patterns.

Various appliances or classes of appliances have distinct power consumption features which constitute their so-called power signatures. NILM mechanisms try to uncover these signatures from the aggregated power information in order to identify the appliances which have contributed to the power consumption. However, several actors in the SG can repurpose power consumption data and the extracted information might be used in ways other than originally intended.

Furthermore, information extracted from load monitoring systems could help organized crime to better plan burglaries and marketers to conduct direct marketing campaigns for the consumers. In conclusion, NILM can undoubtedly assist towards a more efficient SG, but the privacy concerns are justified.

User mode detection: While NILMs identify the apparatus in use along with its schedule, use mode detection attempts to deduce the activity being performed with a particular device. Experiments have shown that TV channels and web browsing recognition is possible with high accuracy. For instance, Greveler et al. [10] employ a method to identify the displayed TV channels. They exploit smart meter measurements with sampling rate of 0.5 hz to develop a function that predicts the power consumption of a LCD monitor lighting system. The power consumption of the monitor is analogous to the brightness of the displayed content. They have demonstrated the effectiveness of their method by showing high correlation between the viewed movie and the power consumption. The correlation is proved by a Pearson coefficient with values 0.93/0.94/0.98 for the three movies they have experimented with. In a different setting, Clark et al. [12] attempt to detect the website that a computer is rendering on the browser from a collection of 8 web-pages. To achieve this, they apply direct load monitoring on the computer with power recording frequency of 1 kHz. Utilizing a set of classification techniques and coupling them together they managed good accuracy, of almost 60%, with the absence of false positives.

Behavior deduction: The behavior deduction of all classes of customers, namely residential, commercial or industrial is beneficial for the design of Demand Response programs as well as for the prediction of the electricity demand under certain behavioral conditions. Nevertheless, NILM and activity detection methodologies reveal the appliances schedule and the associated activities that the customers undertake. On a higher level, this information can be used to extract customers’ behavioral trends. Utilities can record behavioral patterns and this fact could work as an impediment for the DR adoption because of the privacy concerns it arises for the residential users, in particular. Lisovich et al. [09] conducted an experiment in a students’ residence in order to prove that repurposed energy consumption traces can reveal behavioral patterns and habits. The experiment lasted two weeks. They were constantly collecting electrical data while, for verification purposes, they also installed a video surveillance. After they undergone the behavior extraction module a training phase, they were able to detect load events and predict behaviors. The behaviors were divided in several categories, such as presence, sleep schedule, meal times. A degree of disclosure metric was then associated to each of those behaviors.
As they claim, their behavior extraction system performed quite well indicating that privacy concerns are justifiable.

VIII. LITERATURE REVIEW

To satisfy smart grids’ privacy-preserving requirement for multicast communication, a common and efficient solution is to deploy a symmetric group key shared by all multicast participants, e.g. smart meters, data concentrators, Intelligent Electronic Devices (IED), etc. With the support of this shared key (group key), multicast communication data can be encrypted and decrypted. Outsiders cannot peek. Therefore, a group key management protocol that computes the symmetric group key and forwards the partial keys to all legitimate multicast members is central to the privacy preservation of the multicast communication in smart grids.

When one or more member leaves or joins the group, the group key should be updated so that only current group members understand the group key. This process is called rekey. There are two kinds of rekey approaches: individual rekey and periodical batch rekey. The former rekeys the group key for every group membership update such as joining /leaving. The later processes the joining and leaving requests in a batch at the end of each rekey interval. In this paper, we utilize individual rekeying to process join request and periodical rekeying to process leaving requests because: 1) In smart grids, most smart devices e.g. Smart meters playing the group member role have stationary membership. The group membership change events e.g. joining /leaving are rare; 2) Periodical rekeying introduces vulnerability window but also leads efficiency. Considering that some group members, e.g. Smart meters show low-end processing capacity, the tradeoff between performance and security is affordable. 3) Periodic rekeying introduces group key refresh at the end of time interval even there are no membership changes. This promotes the security level.

Furthermore, in view of architecture, group key management schemes can be broadly classified into two categories, namely, centralized and contributory: In a typical centralized group key management scheme e.g. Logical Key Hierarchy (LKH) [11], a trusted third party, known as the key server, is responsible to generate, to encrypt and to distribute the symmetric group key, partial keys and individual keys to all other group members. It has the advantages of efficiency of the symmetric key encryption /decryption. However, it suffers from the following drawbacks. 1) Since all group secrets are generated and stored in one place, the key server could present itself as an attractive attack target for opponent. 2) The key server can turn out to be the particular point of failure.

To solve this key problem [12] by introducing a special type of public-key encryption which we call key-aggregate cryptosystem (KAC). In KAC, users encrypt a message not only under a public-key, but also under an identifier of cipher-text called class. That means the cipher-texts are further categorized into different classes. In other words, the secret key holder can release a constant-size aggregate key for flexible choices of cipher-text set in network storage, but the other encrypted files outside the set remain confidential. The key owner holds a master-secret called master-secret key, which can be used to extract secret keys for different classes. More importantly, the extracted key have can be an aggregate key which is as compact as a secret key for a single class, but aggregates the power of various such keys, i.e., the decryption power for any separation of cipher-text classes. With our solution, Alice can simply send Bob a single aggregate key using a secure e-mail. Bob can download the encrypted photos from Alice’s Drop box space and then use this aggregate key to decrypt these encrypted photos. The scenario is depicted in Figure 1. The sizes of cipher-text, public-key, and master-secret key and aggregate key in our KAC schemes are all of constant size. The public system parameter has size linear in the number of cipher-text classes, but only a small part of it is needed each time and it can be fetched on demand from large (but non-confidential) network. Here there work is flexible in the sense that this constraint is removed, there is no extraordinary relation is necessitated between the classes.

In a group authentication [10], participants belonging to the same group are authenticated. It is many-to-many type of authentication, which is more suited for group oriented IoT applications as there are more number of devices. Group authentication for users is presented in [10], which is t-secure, m-user, n-group Group Authentication Scheme (GAS): ((t, m, n) GAS), where t is a threshold of the proposed scheme. In [10], resources, constrained devices are not considered. Scalable and decentralized group authentication protocol for vehicular communication is presented in [10]. Detail security analysis of the proposed scheme is not presented in [10]. Group-based handover authentication scheme for mobile WiMAX networks is presented in [10], where handover of security context takes place at the each mobility. It consists of point multiplication operation at each node which adds extra overheads. Secure mutual authentication protocol for RFID is presented in [10]. Hash-based encryption adds more overhead to this scheme. In [10], the profile based authentication, and authorization is discussed without implementation details, and results. A group-based negotiation in peer to peer system is presented in [10], but authors have failed to discuss the security analysis of the proposed scheme.

91
Resource negotiation language is discussed in the scope of this paper but, its applicability to other ad-hoc networks is left unaddressed. A lightweight, and distributed group authentication scheme for ad-hoc network devices is presented in [09]. Performance analysis of the proposed scheme is not discussed in [09].

In particular, they propose [12] a secure and reliable in-network collaborative communication scheme to provide secure and reliable for AMI in smart grid with smart meters interconnected through a multi hop wireless network. Here AMI system approach can provide trust services, data privacy and reliability by mutual authentications whenever a new smart meter starts and connects the smart grid AMI network. Data integrity and confidentiality are accomplished through message authentication and encryption services respectively using the corresponding keys established in the mutual authentications. A transmission method is proposed to make easy the data collection and management message delivery between smart meters and a local collector for AMI communications. The performance of the proposed security scheme is verified through simulations and results show that the proposed method has a better end-to-end delay and packet losses comparing with a basic security method and the proposed method can provide secure and reliable communications for AMI in smart grid systems.

In [2000], the author has achieved group authentication by releasing token based on Shamir’s (t, n) secret sharing scheme. This paper extends this work using Paillier Threshold Cryptography. Proposed TCGA scheme[09] for the IoT which verifies authenticity of all the devices taking part in the group communication. This paper also presents TCGA framework which is flexible and secure. Also establishes a secret session key at the end of each group authentication which can be used for group application. TCGA scheme is implemented in WI-FI environment. The head of the group is required to generate, and distribute the new key pairs every time a new member enters the group to maintain group key leakage, and it is referred as Group Authority (GA) in this paper. TCGA comprises algorithms for these following five modules are presented below.

1. Key Distribution.
2. Key Updating.
3. Group Credits Generation.
4. Authentication Listener.
5. Message Decryptor.

Time analysis of key distribution shows that it takes O(n) time for ‘n’ devices which is linear time, and, hence efficient for large number of devices. Time analysis of group authentication is polynomial time with O (n²) which is fairly good time for group oriented applications in IoT.

In contrast, in contributory group key management schemes e.g. Tree-based Group Diffie-Hellman (TGDH) [12], every group member contributes to the group key generation. It has the advantage of fault-tolerance. However, for group membership changes, it lacks scalability in terms of computational cost. For example, TGDH has the following drawbacks. 1) Every group member performs the expensive Diffie-Hellman key exchange with times exponentiation operations for every group membership update where n is the group size. 2) Every sponsor should sign and forward a large number of rekeying multicast messages to update a group key. It results in expensive communication overhead and computational costs. In this paper, we are willing to propose hybrid architecture which combines both centralized and contributory group key schemes to protect the privacy of smart grid multicast service.

IX. SMART GRID SECURITY OBJECTIVES AND RESEARCH PROBLEMS

The cyber security working group in the NIST Smart Grid interoperability panel has recently released a comprehensive guideline for Smart Grid cyber security [11]. In smart grid AMI brings on new security challenges since it is composed of the devices that are placed in physically insecure locations and it makes use of wireless communication that can be possibly corrupted. These resources can be accessed by careless or malicious users [10-10].

![Security Objectives in the Smart Grid](image)

Figure: Three high-level security objectives for the Smart Grid.

- **Availability**: Ensuring timely and reliable access to and use of information is of the most importance in the Smart Grid. This is because a loss of availability is the disruption of access to or use of information, which can additional challenge the power delivery. It is considered as the most crucial requirement in AMI since some systems or applications are real time and they possibly deal with the availability of power.
- **Integrity**: Guarding against improper information modification or destruction is to ensure information non-repudiation and authenticity.
A loss of integrity is the unauthorized modification or destruction of information and can further induce incorrect decision regarding power management. In AMI systems means preventing any changes in the metering data received from meters and control commands sent to the meters. One of the scenarios that may happen is when a hacker sends disconnect command by breaching into a meter management system and disconnects millions of smart meters.

- **Confidentiality**: In particular, privacy, which can strongly affect the customers’ view of organizing smart grid? Customers may not like unauthorized people, or companies to know about their usage patterns. Usage patterns also can reveal life habits and even the presence/absence of residents that could be used by thieves. If people’s concerns are not satisfied, they may refuse to cooperate in deploying smart grid, i.e., they may refuse to let the utility providers install smart meters at their places. Preserving authorized restrictions on information access and disclosure is mainly to protect personal privacy and proprietary information. This is in particular necessary to prevent unauthorized disclosure of information that is not open to the public and individuals.

In AMI, availability and integrity of data take precedence over confidentiality [10], [10]. From the perspective of system reliability, availability and integrity are the most important security objectives in the Smart Grid. Confidentiality is the least critical for system reliability; however, it is becoming more important, particularly in systems involving interactions with customers, such as demand response and AMI networks.

As a result, we are motivated to investigate cyber security issues in the Smart Grid, which is of critical importance to the design of information networks and has been considered as one of the highest priorities for the Smart Grid design [2000-28]. Since the research on cyber security for the Smart Grid is still in its early stage, our objective is to provide an overview, analyze potential cyber security threats, review existing security solutions, and summarize research challenges in the Smart Grid. Specifically, the following issues are discussed in the paper:

**Objectives and requirements**: We first describe the objectives and requirements of cyber security in the Smart Grid, with a focus on identifying fundamental differences between the Smart Grid and another large scale network paradigm, the Internet.

**Probable cyber security threats**: In view of the fact that cyber attacks generally come from malicious threats in communication networks, we review cyber attacks in electric power systems, and provide an extensive analysis of network vulnerabilities under important use cases in the Smart Grid.

**Attack prevention and defense**: To efficiently counter react cyber attacks, it is essential to widely deploy attack prevention and defense strategies all the way through the Smart Grid. Consequently, we accomplish an estimation of the surviving solutions, including network and cryptographic countermeasures, by think about case studies and applications in the Smart Grid.

**Network protocols and architectures**: As attack counter measures will be integrated into network protocols to achieve reliable information exchange, the effectiveness of security solutions needs to be evaluated in the course of message delivery for real-time observing, manage and defense in the Smart Grid. Therefore, here they present discussions on existing cyber security solutions, as well as open research issues, in combination with communication architectures and protocols in the context of real-time and non-real time circumstances for the Smart Grid.

**X. RESEARCH CHALLENGES ON SMART GRID**

(11wk )The smart grid is a large-scale complex power system interconnecting an enormous number of power devices that are equipped with significantly diverse computation and communication capabilities. It is challenging to address the security problems in the smart grid communication networks due to the network size and heterogeneity. Specifically, the research challenges exist in the following categories.

**Requirements mapping**: The communication networks in power systems transmit diversified classes of messages. Different types of messages may require different security protections. For example, the system control messages must be protected with information availability, integrity and authenticity, while the system status sampling data without emergency may only need integrity and authenticity and the availability requirement may not always be necessary, as occasional packet loss is acceptable. A careful classification of the message types and their mapping to the security objectives must be determined.

**Minimum-latency solutions**: Security protection mechanisms for emergent messages must incur minimum latency to satisfy the message delay requirements. For the time critical messages, delivery beyond their acceptable delay windows renders the messages useless. The delays introduced by the security computations and protocol setups add on top of the message transmission delays and therefore they should be kept minimum. In general, computationally intensive W. Wang et al. / Computer Networks 55 (2011) 3604–3629

security solutions provide strong protection but incur long delay, so a practical tradeoff between the security performance and the computational delay may be reached in the design of security solutions.
Security evaluation: Each security scheme used in the power system communication networks must be carefully evaluated on its strength. Typical evaluation metric is the computational time required for compromising the security scheme. The security strength should be sufficiently high such that it is practically impossible to compromise the scheme within a reasonable amount of time. For a security protocol design, every step in the protocol should be inspected to preclude any potential security holes. The security evaluation should also include an assessment of the possible equipment damages and service losses in case that the scheme is compromised.

Acknowledgment

The preferred spelling of the word “acknowledgment” in America is without an “e” after the “g”. Avoid the stilted expression, “One of us (R. B. G.) thanks . . .” Instead, try “R. B. G. thanks”. Put applicable sponsor acknowledgments here; DO NOT place them on the first page of your paper or as a footnote.

REFERENCES