# Approaches for Securing Smart Meters in Smart Grid Networks

Mustafa Saed
Electrical and Computer Engineering
University of Detroit Mercy
Detroit, USA
saedma@udmercy.edu

Kevin Daimi and Nizar Al Holou
College of Engineering and Science
University of Detroit Mercy
Detroit, USA
{daimikj, alholoun}@udmercy.edu

***Abstract*— The Traditional Power utilities are gradually moving towards the Smart Grids. These Grids deploy a very large number of smart meters at the consumers' sites using bi-directional communication networks based on Internet protocols. Smart meters collect consumption data and allow customers other useful functions such as control their consumption electrical power and obtaining current energy usage. With the reliance on the internet protocols, the smart grids become vulnerable to various cyber-attacks. Consumers are worried about their privacy, integrity of their data, availability, and confidentiality when managing their power consumption. In an attempt to contribute to the protection of these smart meters against attacks, threes approaches based on cryptographic protocols are proposed for securing the direct and indirect connection of smart meters to collectors. The security requirements; confidentiality, integrity, and authentication are analyzed with respect to these approaches.**

***Keywords- AMI; Direct Connection;Indirect Connecetion; Smart grid; Security***

## I. INTRODUCTION

Within the smart grid, the Advanced Metering Infrastructure (AMI) and security play a major role [1]-[3]. Smart grids utilize bidirectional communication with consumers to facilitate an information-driven style to indirect energy control and management. To this extent, they deploy large scale smart meters at consumer's sites for bidirectional real time communication using Internet protocols [4]. The smart grid characterizes the new trends of the current power grid nationally and internationally. It emerged in response to environmental changes, improved energy efficiency, and reduced pollution emissions [5]. The smart grid, which is supported by information technology and intelligent control, relies on six components, namely; power generation, transmission, transformation, distribution, consumption and dispatching [6]. As shown in Fig. 1, smart grid refers to the next generation power grid, which upgrades the electricity distribution and management by encompassing a scalable and ubiquitous two-way communication infrastructure to enhance control, efficiency, reliability and safety [7]-[8]. It is, therefore, no surprise that many countries are considering it as the future direction of the power grid [9]-[11].

Smart grids have many components, such as smart meter in their architecture to manage and control the power grid [12]. A smart meter is attached to every house to provide utility companies with more accurate electricity consumption data and customers with convenient way to track their usage information. It interfaces a house's appliances and Home Energy Management Systems (HEMS) on the one hand, and interfaces with data collectors on the other [13].

The Smart meters comprise two main components: an electronic meter that measures energy information accurately and a communication module that transmits and receives data [14]. Based on the importance of AMI and the vital role that it plays within the smart grid [15]-[18], it is very demanding that the AMI be protected from various possible cyber-security attacks [19]. Incorporating the Internet in the smart grid will widely open the door for various security attacks traditionally associated with the Internet.

Undoubtedly, Smart Grid systems will significantly improve efficiency and reliability but at the expense of possibly introducing new vulnerabilities. Hence, smart grid utilization should meet rigorous security requirements [19]. Cyber-security, as a vital challenge of the smart grid transformation must be enforced right at the beginning and not glued when attacks take place [21]. Vulnerabilities are expected in power transmission networks, power grid and zone management [22]-[24]. To eliminate vulnerabilities or at least minimize their impact, strong security measures must be put in place. To reach full customer trust and to ensure excellent permanence of the current power supply, all components of smart grid communication network need to be extremely secure to satisfy the security requirements; confidentiality, integrity, availability, and nonrepudiation [25]-[26].

Consumers do not want others to know how much energy they are consuming or how it is being used (confidentiality). Meter readings and control commands should not be modified while they are being transferred (integrity). The availability of meter reading is critical for utilities and consumers. It is also critical that sending and receiving components and devices cannot deny sending information including readings and commands (nonrepudiation). There are a number of possible attacks on AMI components including denial of service, device tampering, snooping, impersonation, wormhole, black hole and routing attacks. Therefore, AMI demands a reliable and secure communication approach between the smart meters and consumer equipment [26]. The AMI architecture used for this approach will be introduced, and the security of the approaches will be analyzed.

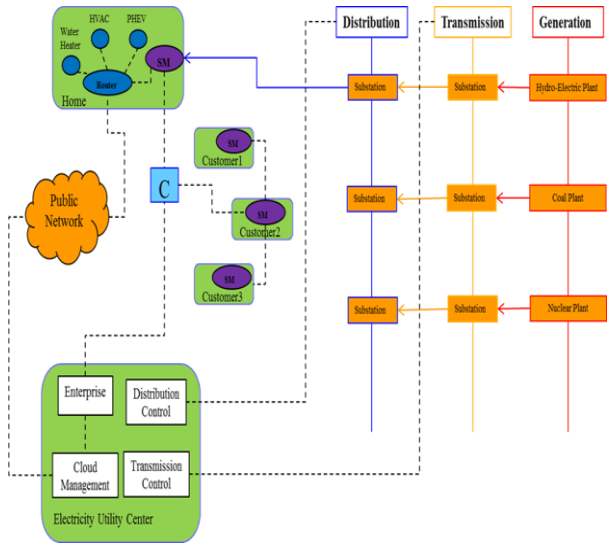


Figure 1. Smart Grid: Power and Information System Architecture.

The reminder of the paper is organized as follows: Related work is introduced in Section II. Section III introduces the AMI architecture & network topology of the smart meter. Section IV deals with the proposed security approaches. The analysis of AMI communication security is presented in Section V. Finally, the paper is concluded in Section VI.

## II. RELATED WORK

Vaidya et al. [28] stressed that many of the available schemes for both single-path and multipath routing are not suitable for meshed AMI network. Consequently, they introduced a security mechanism for multipath routing based on Elliptic Curve cryptology, digital signature, and Message Authentication Code (MAC) for such an AMI network. Their approach allows the Certificate Authority to do a lot more work than they should normally do (issuing certificates) including controlling the nodes' creation of public and private key. Nodes (smart meters) perform a number of computations despite their known limited computing power. This also tends to slow the system. Furthermore, a smart meter sends its information to all the neighboring smart meters with no security. This provides a potential attacker the opportunity for attacking more than one goal (smart meter) as they all have the information of the source meter. The neighboring nodes, acting as intermediate nodes, will do more calculations and broadcast the results. This means all other nodes (smart meters) have now the information. This implies, there are many nodes that the attacker can try and many nodes will be affected.

An interesting security protocol for AMI communications in smart grid where the smart meters are interconnected through wireless network was introduced by Yan et al. [29]. Their techniques indicated that the PKI is not desirable and relied on symmetric key cryptology. However, the number of symmetric keys used is large and possibly comparable to the number of keys should PKI has been followed. Furthermore, smart meters have limited capabilities, and therefore, verifying the MAC should have been left to the collector. The authors did not specify what will happen when the two MAC's are not equal. This implies that the integrity of a meter's reading is not handled correctly [30]-[31].

Seo et al. [32] discussed the use of public key infrastructure (PKI) in smart grid and what security requirements need to be implemented in smart grid architecture including the smart meter to secure the smart meter communication in the AMI. The authors did not propose any security technique/protocols to secure the smart grid network but only provided a survey.

Dong et al. [33] proposed a protection scheme for the automation of smart grid system and patch distribution from the control center to data transmission security. Some of the functions were tested on the simulation platform, through intrusion detection system and using field devices such as smart meter. Their proposal considers the security within smart meter but not for the smart meter communication, such as smart meter to smart meter and smart meter to collector [34]. Furthermore, their proposed protection system did not use digital signature to protect against forgery.

Zhao et al. [35] provide the fundamental limit of cyber-physical security in the presence of low sparsity unobservable attacks. It is shown in [36]-[37] that a complete system matrix can be identified using an independent component analysis method. Nevertheless, such attack schemes might not be easy to implement, as all meter data are required to be known and all the meters are required to be controlled. On the other hand, several detection and defense schemes are provided based on the complete knowledge of the system matrix. The off-line method, based on the Kullback-Leibler distance, is proposed to track malicious attacks using historical data [38]. They added their method may not work very well for continuous small-scale attacks. Our work can tackle continuous small-scale attacks through the various techniques that are proposed in the next sections.

Giani et al. [39] utilize the sparse topology information of the smart grid to determine the attack meter sets. However, these works lack the discussion of the system matrix acquisition. In fact, the design of the attack vector relies heavily on precise knowledge of the system matrix. In this case, it would not be easy to obtain such confidential information for an attacker who has limited access to the smart grid. Overall, a feasible unobservable attack scheme based on the incomplete system matrix has not yet been fully investigated. The authors in their proposal were not covering the smart meter communication attack. They only mentioned for the possible vulnerabilities related to attack meter in physical layer.

Li et al. [40] presented an efficient and robust approach to authenticate data aggregation in smart grids. Aggregation refers to the communication between the smart meters and the collector. This is achieved via deploying signature aggregations, implementing batch verification, and signature

amortization schemes to reduce communication overhead and number of signing and verification operations, and providing fault tolerance. The authors proposed an efficient authentication scheme for power usage data aggregation in Neighborhood Area Networks (NAN) and smart meter to collector communications. The contributions for this work were represented by deploying digital signatures so that when the collector is out of service, alternative or backup collectors can execute the authentication approach without any additional configuration or setup. Their research also sought to reduce the number of signature and verification operations. However, the research is limited to authentication only. Thus, they are not securing the messages' (reading) between smart meter and collector.

F. Li et al. [41] introduced a distributed incremental data aggregation approach, in which data aggregation is performed at all smart meters involved in routing data from the smart meter to the collector unit. In this research, the authors presented an efficient information aggregation approach, in which an aggregation tree, constructed via breadth-first traversal of the graph and rooted at the collector unit, is deployed to cover all smart meters in the neighborhood. This protocol can let the control unit collect all smart meters' information in the area. Furthermore, to protect users' privacy, all information is encrypted by a homomorphic encryption algorithm. Since no authentication scheme is emphasized, the approach faces the potential risk that malicious smart meter can forge packets, thus causing the smart grid system to fil to detect or diagnose bogus data. Adversaries can maliciously forge their own data to manipulate the aggregation results. Therefore, adversaries and false data reports need to be detected through advanced auditing approaches.

This paper proposes schemes for securing the direct and indirect smart meter-to-collector communications. The schemes are based on PKI. Unlike the work of Vaidya et al., the proposed indirect scheme in our paper allows each node to send the encrypted, authenticated, and signed reading of a smart meter to its successor only (just one node). The successor cannot tell the reading of the predecessor node. If a node is attacked, readings of other nodes will not be affected. Our paper also avoids the need for a certificate authority for both proposed schemes by allowing the collector/substation node to take care of issuing certificates to all smart meters under its authority. Furthermore, nodes do not waste time performing lengthy calculations. In contrast to the approach of Yan et al., PKI provides stronger encryption using public and private keys. It is clear how the keys are created/recreated and exchanged. The messages (readings) are small indicating PKI is the convenient way here. The verification of the hash functions is carried out by the collector, which has more powerful computing capabilities. If the computed hash function is not equal to the received hash function for a smart meter's reading, the collector will reject that reading and inform the substation of a possible attack on that smart meter. Therefore, the integrity of a message (reading) is handled correctly. Furthermore, this proposed idea adds anonymity to the meters by using anonymous IDs, and adds confusion to the order of readings of smart meters using a PRNG. Two different security protocols are proposed to enhance the security of the direct (centralized) communication between smart meters and collector in a smart grid. The proposed work contributed to protecting the two-way direct communication of smart meters with collector through the introduction of two cryptographic protocols. The AMI architecture used for this scheme will be introduced, and the security of the schemes will be analyzed.

## III. Advanced Metering Infrastructure (AMI) Architecture & Smart Meter Network Topology

AMI networks are responsible for connecting a substantial number of devices needed to collect readings from smart meters. As this paper is concerned with securing smart meters to collector communication, only this part of the AMI architecture will be introduced. There are two ways of connecting smart meters to connecters; direct and indirect connections. In direct connection, smart meters directly communicate with collectors to transfer readings and exchange information and commands. For indirect connection, one or more smart meters are directly connected to the collector. The rest are either connected to the nearest smart meters that have direct connection with the collector or through a series of smart meters until the one directly connected to the collector is reached. The collector is responsible for collecting readings from all smart meters within its coverage area (network). Coverage area could include both direct and indirect connection. Figure 2 depicts the direct smart meter-to-collector communication topology. The collector (C) is the central point between the substation and the smart meters (SMs). To clarify the connection, an example of an indirect connection is presented in Figure 3.

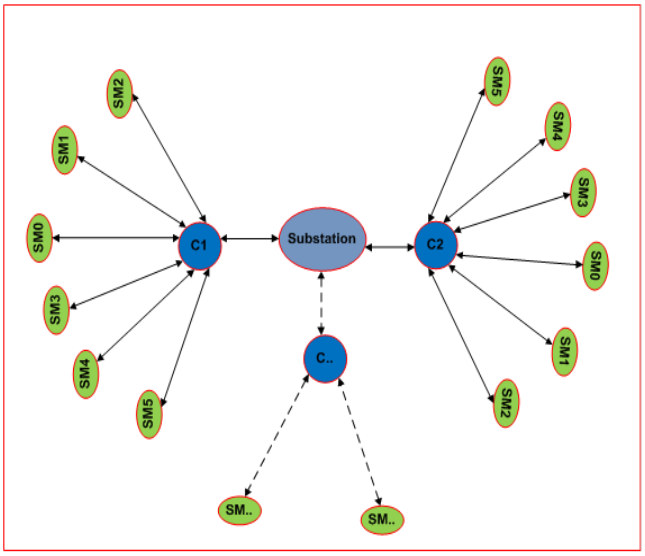


Figure 2. Centralized smart meter-to-collector communication topology.

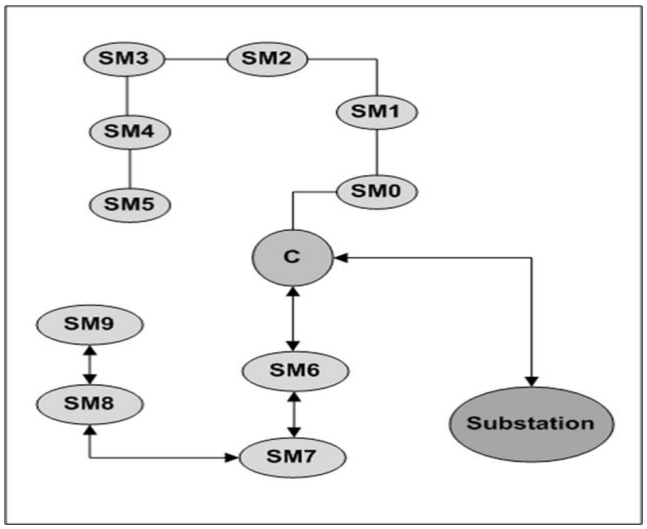


Figure 3. Smart meter-collector indirect connection.

## IV. PROPOSED SECURITY APPROACHES

Two different security protocols are proposed to enhance the security of the direct communication between smart meters and collectors in a smart grid as describes in section (A) and (B). The symbols and notations used in these protocols are summarized in Table I below.

The approach used for the indirect communication between smart meters and collector will be introduced in section (C).

TABLE I. NOTATIONS & SYMBOLS USED

| Symbol | Meaning |
|---|---|
| SMi | Smart Meter #i, i=1, 2, …n |
| C | Collector |
| S | Substation |
| PUc, PRc, PUi, PRi | Public & Private keys for collector & meter respectively |
| IDc, IDi, IDS | Identification for collector, smart meter, and substation |
| Ri | Meter #i 's Reading, i=1, 2, …n |
| Ki | Symmetric Key shared between collector and meter #i |
| H(Ri) | Hash value for meter #i 's reading, i=1, 2, …n |
| Ti | Meter #i 's processor temperature |
| A-IDi, A-IDc , A-IDs | Anonymous ID for meter, collector, and substation |
| Ccert, SMi–cert, CRi | Certificate of collector & smart meter i respectively |
| SM0, SM6 | Smart meters directly connected to C |
| ‖ | Concatenation |
| E | Encrypt |
| → | Send to |
| PRV | Period of validity |

### A. Securing direct communication without certificates

This section relies on public key cryptology. No certificates are needed here. The substation, which is only directly connected to the collector (see Figure 2), will assist in the enrollment and activation part of the protocol. Note that the processor's temperature for each smart meter is used as a random number to further confuse the resulting message.

- Enrollment and activation process:

  The Substation in charge authenticates the SMs and the collector. This includes any newly joined smart meter. The substation provides each smart meter with the ID of the collector for authentication purposes, and the public key, $PU_c$. It also provides the collector, C, with the ID's of the smart meters. The collector sends a message to each smart meter, $SM_i$, requesting the $PU_i$ of each $SM_i$. The collector inserts its ID in the message. The request and ID are encrypted with its private key, $PR_c$. Having verified the collector's ID, each smart meter will send its $PU_i$ and $ID_i$ encrypted with the public key of the collector, $PU_c$.The collector, C, decrypts the message and verifies the $ID_i$. If it is valid, it accepts the $PU_i$. Figure 4 illustrates this process.

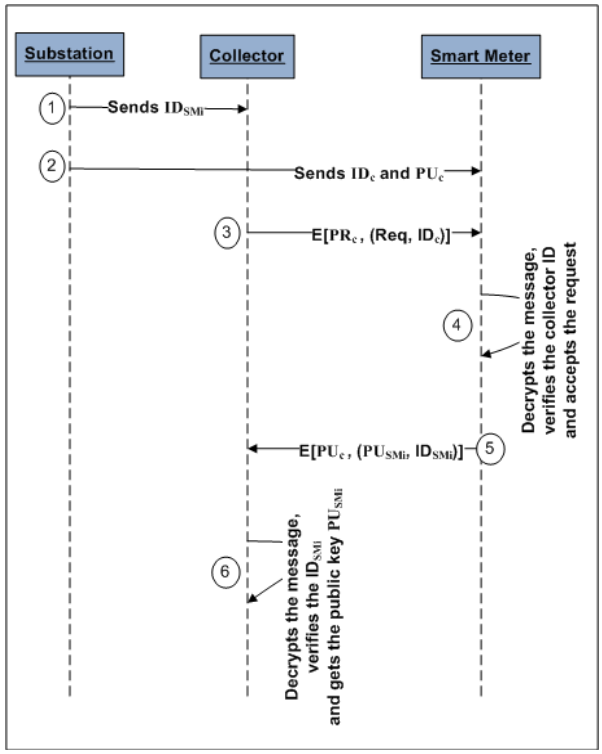


Figure 4. Enrollment and activation-Without Certificate.

- Smart meter to collector security process:

Each $SM_i$ XORs its reading $R_i$, with the processor temperature, $T_i$, to get the message $M_i$, finds the hash function $H(R_i)$ of the reading $R_i$, and concatenate $M_i$, $H(R_i)$, $T_i$, and $ID_i$. Note the $ID_i$ is needed to allow the collector to identify the sender smart meter. The resulting message will be encrypted with collector's public key, $PU_c$, and forwarded to C. Upon receiving the message, the collector, C, uses its private key, $PR_c$, to decrypt the message. It then XORs $M_i$ with $T_i$ to get the reading $R_i$ and the hash function $H(R_i)$. The collector then calculates the hash value of the extracted $R_i$ and verifies it is equal to $H(R_i)$ to ensure the integrity of the reading.
This is clarified in Figure 5.

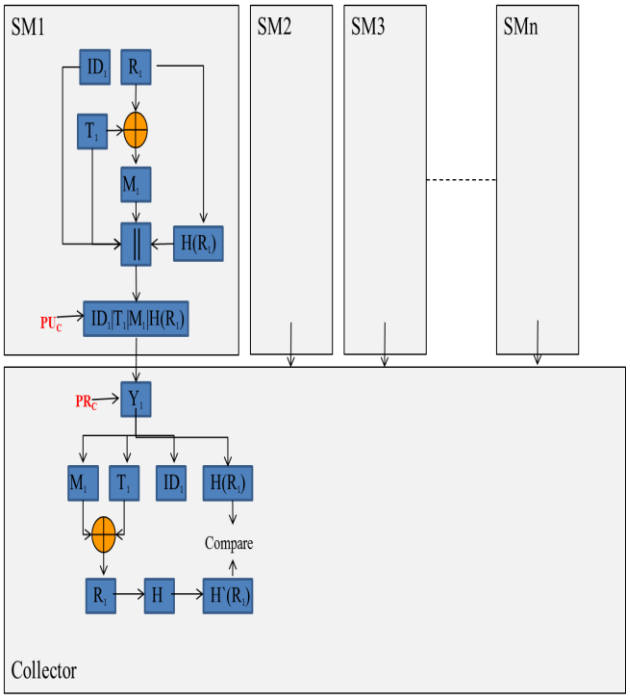


Figure 5. Smart meter-collector security process.

- Key update and exchange process:

After a predefined number of readings, new public keys for both collector and SMs will be generated and exchanged. The collector uses the old $PR_c$ to encrypt the new $PU_c$, old $PU_i$ to encrypt the resulting message, and inserts its $ID_c$ before sending it to smart meter #i, $SM_i$. At the other end, Smart meter i, $SM_i$, decrypts the received message, verifies $ID_c$, and gets the new $PU_c$. The smart meter, $SM_i$, generates new $PU_i$ and $PR_i$. It encrypts the new $PU_i$ with the old $PR_i$, encrypts the resulting message with the new $PU_c$ adds its $ID_i$, and sends it to the collector, C. C reacts by decrypting the received message, verifying the $ID_i$, and then obtaining the new $PU_i$.
This process is further detailed in Figure 6.

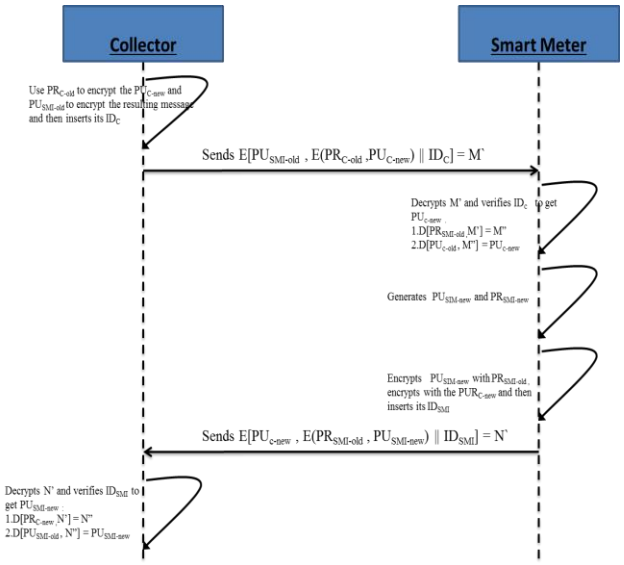


Figure 6. Key update and exchange process.

## B. *Securing Direct Communication using Certificates*

This section relies on certificates. These certificates will be issued by the substation to which the collector connects.

- Enrollment and activation process:

The Substation acts as the Certification Authority (CA). It creates the certificates for all the smart meters and the collector. In these certificates, the real ID of the SMs and collector are replaced with an anonymous ID. These certificates are then sent to the respective party. At the time of setup and installation of the collector and smart meter, the substation's anonymous ID, A-$ID_s$, and public key PUs, will be provided to the collector and smart meters. This will include any newly added smart meter. The collector and smart meters will create their own anonymous $ID_s$. Each collector requests its certificate from the Substation. The request includes the public key of the collector $PU_c$, both $ID_c$ and A-$ID_c$, and a request message, $C_{Cert-Req}$, all encrypted with the substation's public key $PU_s$. This request will be forwarded to S. The Substation creates the collector's certificate, $C_{cert}$= E [$PR_s$,$PU_c$|| A-$ID_c$|| $T_1$ || $T_2$] and then encrypts it with the collector's public key $PU_c$. The encrypted $C_{cert}$ is then sent to the collector. Note that $T_1$ is the creation time, and $T_2$ is the expiration time for the certificate. In a similar way, each smart meter, $SM_i$, demands its certificate from the Substation. The request includes the public key of the smart meter $PU_i$, its ID, $ID_i$, its anonymous ID, A-$ID_i$, and a request message, $SM_{i\text{-}Cert\text{-}Req}$., all encrypted with the substation's public key $PU_s$. This request will be sent to the substation. The Substation creates each smart meter's certificate, $SM_{i–cert}$ = E [$PR_s$ ,$PU_i$|| A-$ID_i$|| $T_1$

|| $T_2$], and then encrypts it with the smart meter's public key $PU_i$. The anonymous ID is concatenated to the encrypted $SM_{i\text{-cert}}$ before sending it to the collector. Knowing it is not its ID; the collector will broadcast the message to all the smart meters connected to it. Only the smart meter with A-$ID_i$ can decrypt the message and get its certificate, $SM_{i\text{-cert}}$. To complete the enrollment process, the substation, S, sends a list of ID pairs including the real and anonymous ID's for all smart meters to the collector to enable it to figure out the sending smart meter. This is because the certificate only contains the anonymous ID, and therefore, there is no way the collector can tell who the sender is. The enrollment process is further demonstrated in Figure 7.

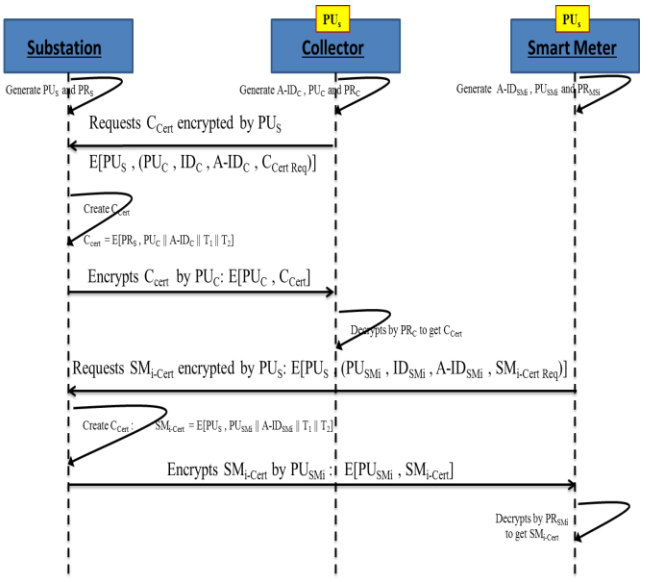


Figure 7. . Enrollment and activation process-With Certificate.

- Smart meter to collector security process:

  The collector and each smart meter will exchange their certificates for authentication purposes. Each party decrypts the received certificate to get the public key and ID of the other party. The keys and $ID_s$ are only trusted after verifying $T_1$ and $T_2$. Once each party obtains the public key of the other, the smart meter to collector security process of section (A) will be applied.

- Certificate update process:

  After a predefined number of readings, new certificates for both collector and SMs will be generated by the substation. The substation will inform the collector and smart meters to create their new public and private keys and to go ahead to request new certificates as above. If either the collector or a smart meter needs to have a new certificate issued as a result of any threat, they can request new certificates from the substation following the process mentioned above.

### C. *Securing Indirect Communication*

The approach for the indirect communication between smart meters and collector will be introduced below. In this approach, anonymous ID's (A-ID's) for the smart meters are used. To create anonymous ID's, each smart meter XORs the current ID (real one initially and then anonymous) with the output of a true random number (TRN) generated by a ring oscillator, $T_i$ [42]. Any other true random value can be used instead of or in addition to the one generated by the ring oscillator. In other words, A-$ID_i$ = $ID_i$ XOR $T_i$ for the first A-$ID_i$, and A-$ID_i$ = Previous A-$ID_i$ XOR $T_i$ for subsequent A-$ID_i$'s. Table I presents the notations and symbols used in these approaches.

- Enrollment-Activation and Certificate Exchange:

  In this approach, the collector C should have initially received all the public keys and IDs of the smart meters. On the other hand, the smart meters, SM's, should have the public key of the collector using any secure process. Furthermore, the predecessor and successor nodes for each smart meter are identified during installation and configuration of each smart meter. The node directly connected to the collector has no successor. The nodes at the end of the connection have no predecessors. Note that the scheme will be applied to the upper part of Figure 3 to observe how smart meters $SM_0$-$SM_5$ securely send their readings to the collector C. The readings for smart meters $SM_6$-$SM_9$ at the lower part of the figure will be collected using the same approach. Each smart meter, $SM_i$, replaces its real $ID_i$ with an anonymous one, A-$ID_i$, appends $ID_i$ to it and encrypts both with the public key of collector, $PU_c$, before sending the resulting message, $E(PU_c, A\text{-}ID_i \parallel ID_i)$, to C through the indirect connection (Figure 8).

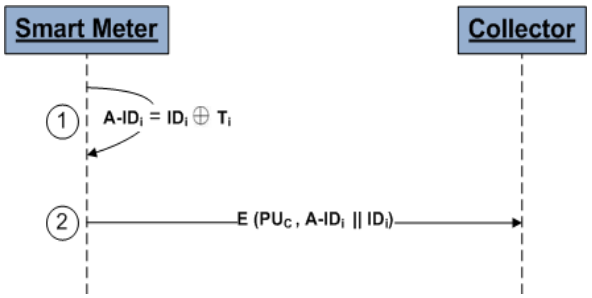


Figure 8. Creating and sending anonymous ID.

The collector, C, creates certificates for each smart meter, $SM_i$. It appends A-$ID_i$ to the public key of each smart meter, $PU_i$, and the period of validity

PRV, and then encrypts $PU_i||A\text{-}ID_i||PRV$ with its private key, $PR_c$ to get the certificate for each smart meter ($CR_i = E(PR_c, PU_i||A\text{-}ID_i||PRV)$ since all smart meters have the public key $PU_c$ of the collector. The $CR_i$ is further encrypted with $PU_i$. Having done that, C then attaches $A\text{-}ID_i$ to the resulting message and forwards $E(PU_i, CR_i) \parallel A\text{-}ID_i$ to smart meters via $SM_0$. Certificate creation is depicted in Figure 9 for both the collector and smart meter.

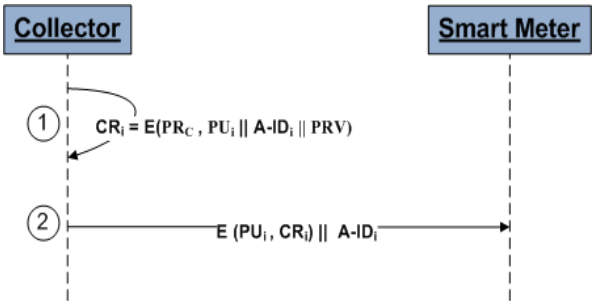


Figure 9. Creating and sending certificates.

Every $SM_i$ checks the $A\text{-}ID_i$. If it is its ID, it decrypts $E(PU_i, CR_i)$ with its private key $PR_i$ to get its certificate. Otherwise, it will forward the message to adjacent smart meters to do the same until all smart meters receive their certificates.

- Secure Reading Collection Process:

Each $SM_i$ XORs its reading, $R_i$, with the TRN produced by the ring oscillator, $T_i$, concatenates the resulting message with $T_i$ and the hash function of the reading $H(R_i)$. The resulting message will be encrypted with $PR_i$ to get $X_i = E [PR_i, M_i \parallel H(R_i) \parallel T_i]$, where $M_i = R_i$ XOR $T_i$. To enable the collector to recognize the source meter's reading, $A\text{-}ID_i$ is attached to $X_i$ and both encrypted with $PU_c$ to get $Y_i = E(PU_c, X_i \parallel A\text{-}ID_i)$. The XOR operation is used to obscure the reading of the meter. $T_i$ is needed to allow the receiver to XOR it with $M_i$ to get $R_i$. Having done that, $R_i$ will be hashed and compared to $H(R_i)$.

The predecessor and successor nodes exchange certificates to authenticate each other. On successful authentication, the predecessor smart meter encrypts its $Y_i$ with the public key $PU_{i-1}$ of the successor, and forward $E[PU_{i-1}, Y_i]$ to the successor.

The receiving successor decrypts the received message with its private key $PR_{i-1}$, prepends or appends its own $Y_{i-1}$ and encrypts the two ($Y_i \parallel Y_{i-1}$, or $Y_{i-1} \parallel Y_i$, for example) with its successor's public key. This process will continue until all $Y_i$'s have been concatenated at $SM_0$. Using Figure 3 above, we should have $Y = Y_5 \parallel Y_4 \parallel Y_3 \parallel Y_2 \parallel Y_1 \parallel Y_0$ or any other ordering. $SM_0$ sends Y to C. Any missing $Y_i$ indicates a problem, possibly an attack, within that meter. If this occurs, the collector will reject the received message and report to the substation to investigate the issue. The decision on whether to append or prepend $Y_i$ is based on pseudorandom number generator (PRNG'), which generates pseudorandom bit stream. $Y_{i-1}$ is prepended if the pseudorandom bit is '0' and appended if the bit is '1'. This will obscure the order of $Y_i$'s and make it hard to relate the $Y_i$'s to their smart meters.

To illustrate this, Figure 10 is provided.

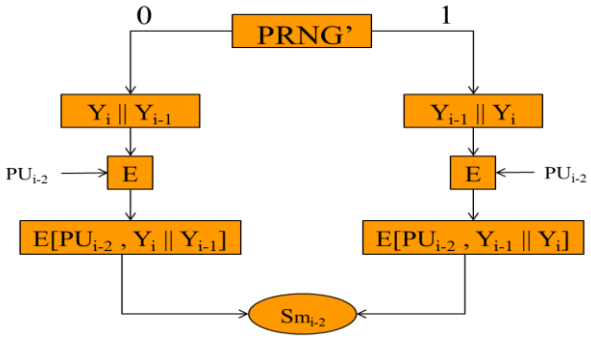


Figure 10. Pseudorandom Number Generator PRNG' operation (Smart mete- to-Smart meter).

The collector, C, uses its $PR_c$ to decrypt Y. Then, based on the $A\text{-}ID_i$, it uses the appropriate $PU_i$ to decrypt each $Y_i$ to obtain $M_i \parallel H(R_i) \parallel T_i$ for each smart meter. It XORs $M_i$ with $T_i$ to get the reading $R_i$. It later finds the hash function of $R_i$ and ensures it is equal to the received hash function $H(R_i)$ to guarantee the integrity of the reading, $R_i$. Figure 10 illustrates the meter readings collection process.

To simplify Figure 11, $Z = Y_5 \parallel Y_4 \parallel Y_3 \parallel Y_2 \parallel Y_1$ (order is based on PRNG') is used. Note that smart meter 5, $SM_5$, has no predecessor, and therefore, no PRNG' unit exists. Only smart meters $SM_4$-$SM_1$ have it because they have predecessors (smart meters connected to them, as depicted in Figure 3).

Once the order of $Y_i$'s is decided, the result is encrypted with the public key of the next meter, $PU_{i-2}$, and forwarded to the next smart meter, $SM_{i-2}$. The PRNG for $SM_0$ is not followed by encryption as in Figure 10 because it is forwarding directly to the collector. To illustrate this, Figure 12 is provided.

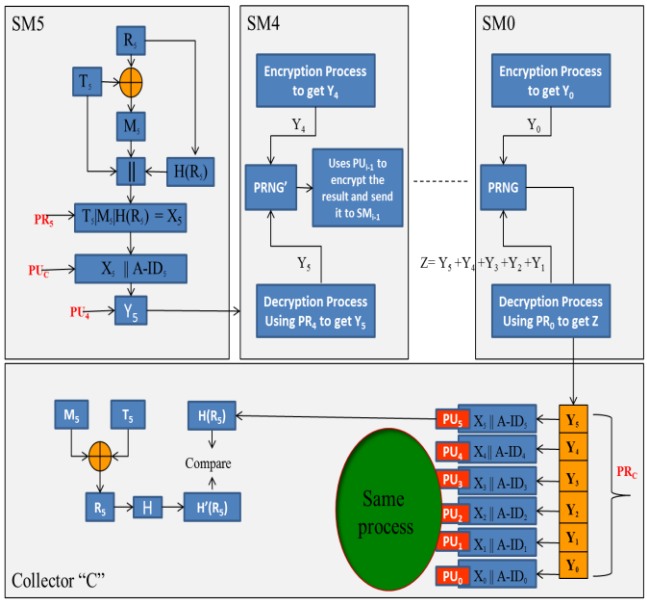


Figure 11. Meter readings collection process.

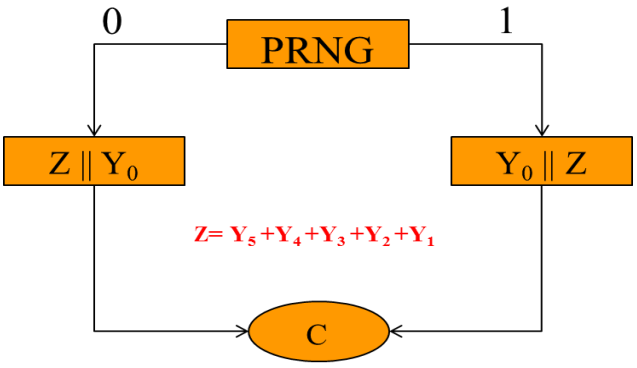


Figure 12. PRNG operation (Smart meter - to - Collector).

- Key Update and Certificate Exchange Process:

After a predefined number of readings or when the validity period PRV of the certificate expires, new keys for both collector and SM's will be generated and exchanged. The collector will use its old $PR_c$ to encrypt the new $PU_c$ and then encrypt the result with the old PUi and attaches $A\text{-}ID_i$ prior to sending it to $SM_i$. The $A\text{-}ID_i$ will allow each smart meter to tell if the message is intended for it. The smart meter in question, $SM_i$, will decrypt this message to get the new public key of the collector. At the other side, each smart meter generates new $A\text{-}ID_i$, $PU_i$ and $PR_i$, appends the new $A\text{-}ID_i$ to the new $PU_i$, encrypts the resulting message with the old $PR_i$ and then with the new public key of the collector, $PU_c$. Finally, the old $A\text{-}ID_i$ is attached before sending it to the collector. The collector will apply the required series of decryptions to get the new $A\text{-}ID_i$ and $PU_i$ of each smart meter. Note that the old $A\text{-}ID_i$ is added to allow the collector to recognize each smart meter. Furthermore, new certificates will be generated and forwarded to the smart meters as mentioned above. This is detailed in Figure 13 below.

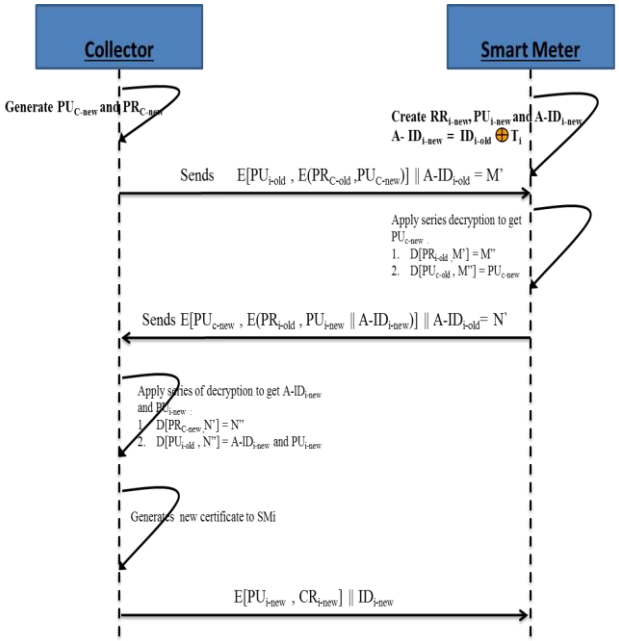


Figure 13. Exchanging new keys, IDs, and certificates.

New keys, certificates, and anonymous IDs are also created and exchanged when an attack is anticipated or has already occurred. An alternative approach is used if the creation and storage of certificates are not desirable due to computing power and memory limitations. For each adjacent smart meter pair, the collector sends the predecessor the public key of the successor encrypted with the public key of the predecessor, and sends the successor the public key of the predecessor encrypted with the public key of the successor. In both cases, the A-IDi is attached to allow smart meters to capture messages belonging to them. Apart from replacing the certificate with the collector providing the public keys for the predecessors and successors, the rest is exactly as in the first approach.

## V. ADVANCED METERING INFRASTRUCTURE (AMI) COMMUNICATION SECURITY ANALYSIS

The security of the above schemes is analyzed with respect to confidentiality, integrity, and authentication. Although hash functions can help with intrusion and virus detection, availability cannot be satisfied by cryptology alone (schemes above), and therefore, it will not be part of the analysis. Table II illustrates the security analysis for both proposed schemes.

TABLE II. ADVANCED METERING INFRASTRUCTURE (AMI) COMMUNICATION SECURITY ANALYSIS

| **Advanced Metering Infrastructure (AMI) Communication Security Analysis** | | |
|---|---|---|
| ***Security Req.*** | ***Direct Communication*** | ***Indirect Communication*** |
| ***Confidentiality*** | The confidentiality achieved when the message that sent from the SMs to the collector is encrypted using the public key of the collector and the only collector will be able to decrypt and read the received message from the smart meter using the collector private key $PR_c$. The hash value, $H(R_i)$ of direct approach, is encrypted with the public key of the collector ($Y_i = E [PU_c, M_i \| H(R_i) \| T_i]$). Only the collector with its private key ($PR_c$) can decrypt the hash value. | The proposed protocol for indirect approach ensure that confidentiality is met through the message that is forwarded to the next smart meter or directly to the collector in the case of SM0 is encrypted with the public key of the collector ($Y_i = E(PU_c, X_i \| A\text{-}ID_i)$). Only the party that has the private key (collector), $PR_C$, can **decrypt** this message. |
| ***Integrity*** | The reading, Ri, in the proposed schemes has its integrity fulfilled through the use of cryptographic hash function, H(Ri). Upon receiving the message, the collector extracts Ri and find its H(Ri). It then compares the computed H(Ri) with the received one. Any mismatch indicates the message has been modified. | The reading, Ri, in the proposed scheme has its integrity fulfilled through the use of cryptographic hash function, H(Ri). Upon receiving a message, the collector extracts Ri and find its H(Ri). It then compares the computed H(Ri) with the received one. Any mismatch indicates the message has been tempered with. |
| ***Authentication*** | The substation, which is only directly connected to the collector (see Figure 2), will assist in the enrollment and activation part of the protocol. The Substation in charge authenticates the SMs and the collector. This includes any newly joined smart meter. The substation provides each smart meter with the ID of the collector for authentication purposes, and the public key, $PU_c$. It also provides the collector, C, with the ID's of the smart meters. The collector sends a message to each smart meter, $SM_i$, requesting the $PU_i$ of each $SM_i$. The collector inserts its ID in the message. The request and ID are encrypted with its private key, $PR_c$. Having verified the collector's ID, each smart meter will send its $PU_i$ and $ID_i$ encrypted with the public key of the collector, PUc. The collector, C, decrypts the message and verifies the $ID_i$. If it is valid, it accepts the $PU_i$. Figure 4 illustrates this process. | The contents of $X_i$ are encrypted with $PR_i$, and then $X_i$ is encrypted with PUc. Therefore, authentication is also taken care of. |

The proposed security protocols introduce an additional enhancement resulting from XORing smart meters' readings with a random value to make it hard for attackers to extract the actual reading. In addition, the replacement of real IDs with anonymous ones will make it hard to relate a reading to a particular smart meter. Finally, the use of pseudorandom number generator (PRNG) introduced further hardship in judging the link between the reading and smart meter. Further, to ensure the message is protected against forgery, digital signature is used.

## VI. CONCLUSION

Efforts to establish the Smart Grids are constantly increasing globally. The Smart Grid is a bi-directional communication system enabling customers through their smart meters to administer their energy service and access a number of features including using energy during low cost intervals, reading consumption electricity bills online, and scheduling turning on/off home appliances. These services need to be available when needed, the integrity of meter readings should be preserved, and privacy of these services need to be maintained. Intruders with access to these services can result in a great damage to consumers and the distribution of services by utilities. Comprising one smart meter can result in comprising many others and the collectors. This paper contributed to protecting the two-way direct and indirect communication of smart meters with collectors through the introduction of two cryptographic protocols based on PKI. Securing indirect communication is harder than the direct one because readings have to travel through other smart meters before reaching the collector. The introduced schemes satisfied the security requirements; confidentiality, integrity, and nonrepudiation. Future work will concentrate on verification of theses protocols.

## REFERENCES

[1] M. Saed, K. Daimi, and N. Al-Holou, "Securing Indirect Communication for Advanced Metering Infrastructure in Smart Grid," in Proc. EMERGING 2015 the Seventh International Conference on Emerging Networks and Systems Intelligence, pp. 84-90, 2015.

[2] J. H. Khan and J. Y. Khan, "A Heterogeneous WiMAX-WLAN Network for AMI Communications in the Smart grid," in Proc. the IEEE third International Conference on Smart Grid Communication (SmartGridComm), Tainan, Taiwan, 2012, pp. 710-715.

[3] U.S. Department of Energy (DOE), "The Smart Grid: an Introduction," Available: http://energy.gov/oe, [retrieved: November, 2017].

[4] Y. Simmhan, A. G. Kumbhare, B. Cao, and V. Prasanna, "An Analysis of Security and Confidentiality Issues in Smart Grid Software Architectures on Clouds," in Proc. IEEE 4th International Conference on Cloud Computing (CLOUD 2011), Washington, DC, USA, 2011, pp. 582-589.

[5] X. Miao, X. Chen, X. Ma, G. Liu, H. Feng, and X. Song, "Comparing Smart Grid Technology Standards Roadmap of the IEC, NIST, and SGCC," in Proc. 2012 China International Conference on Electricity Distribution (CICED 2012), Shanghai, China, 2012, pp. 5-6.

[6] X. Jin, Y. Zhang, and X. Wang, "Strategy and Coordinated Development of Strong and Smart Grid," in Proc. the 2012 IEEE Conference on Innovative Smart Grid Technologies – Asia (ISGT Asia), Tianjin, China, 2012, pp. 1-4.

[7] U.S. Department of Energy (DOE), Available: www.smartgrid.gov/the_smart_grid, [retrieved: November, 2017].

[8] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A Survey on Smart Grid Communication Infrastructures: Motivations, Requirements, and Challenges," IEEE Communications Surveys and Tutorials, vol. 15, no. 1, 2013, pp. 5-20.

[9] A. Ipakchi and F. Albuyeh, "Grid of the Future," IEEE Power and Energy Magazine, vol. 7, no. 2, 2009, pp. 52-62.

[10] R. O'neill, "Smart grid sound transmission investments," IEEE Power and Energy Magazine, vol. 5, no. 5, 2007, pp. 104-102.

[11] H. Tai and E. Hogain, "Behind the Buzz: Eight Smart-Grid Trends Shaping the Industry," IEEE Power and Energy, vol. 7, no. 2, 2009, pp. 96-97.

[12] A. Molina-Markham, P. Shenoy, K. Fu, E. Cecchet, and David Irwin, "Private memoirs of a smart meter," in Proc. of the 2nd ACM workshop on embedded sensing systems for energy-efficiency in building, pp. 61–66, 2010.

[13] E. D Knapp and R. Samani, "Applied Cyber Security and the Smart Grid," implementing Security Controls Into the Modern Power Infrastructure. Newnes, 2013.

[14] Botswana Power Corporation, "A SAP IS-U and Smart Meter," implementation project experience in Botswana, Africa.

[15] I. Joe, J. Y. Jeong, and F. Zhang, "Design and Implementation of AMI System using Binary CDMA for Smart Grid," in Proc. the Third International Conference on Intelligent System Design and Engineering Applications, Hong Kong, 2013, pp. 544-549.

[16] M. Chebbo, "EU Smart Grids Framework: Electricity Networks of Future 2020 and Beyond," IEEE Power Engineering Society General Meeting, Tampa, FL, 2007, pp. 1-8.

[17] D. G. Hart, "Using AMI to Realize the Smart Grid," IEEE Power Engineering Society General Meeting, Pittsburgh, PA, 2008, pp. 1-2.

[18] J. Wang and V. C. M. Leung, "A Survey of Technical Requirements and Consumer Application Standards for IP-based Smart Grid AMI Network," in Proc. the International Conference on Information Networking (ICOIN), Barcelona, 2011, pp. 114-119.

[19] S. Choi, S. Kang, N. Jung, and I. Yang, "The Design of Outage Management System Utilizing Meter Information Based on AMI (Advanced Metering Infrastructure) System," in Proc. the 8th International Conference on Power Electronics, Shilla Jeju, Korea, 2011, pp. 2955-2961.

[20] A. R. Metke and R. L. Ekl, "Smart Grid Security Technology," in Proc. IEEE Conference on Innovative Smart Grid Technologies (ISGT), Gaithersburg, MD, 2010, pp. 1-7.

[21] S. M. Amin, "Smart Grid Security, Confidentiality, and Resilient Architectures: Opportunities and Challenges," IEEE Power and Energy Society General Meeting, San Diego, CA, 2012, pp. 1-2.

[22] G. Chen, Z. Y. Dong, J. H. David, G. H. Zhang, and K. Q. Hua, "Attack Structural Vulnerability of Power Grids: A Hybrid Approach Based on Complex Networks," Physica A: Statistical Mechanics and its Applications, vol. 389, 2010, pp. 595-603.

[23] S. Clements and H. Kirkham, "Cyber-security Considerations for the Smart Grid," IEEE Power and Energy Society General Meeting, Minneapolis, MN, 2010, pp. 1-5.

[24] G. N. Ericsson, "Cyber-security and Power System Communication: Essential Parts of a Smart Grid Infrastructure," IEEE Transactions on Power Delivery, vol. 25, no. 3, 2010, pp. 1501-1507.

[25] M. Wagner, M. Kuba, and A. Oeder, "Smart Grid Cyber Security: A German Perspective," in Proc. International Conference on Smart Grid Technology, Economics and Policies (SG-TEP), Nuremberg, 2012, pp. 1-4.

[26] F. M. Cleveland, "Cyber Security Issues for Advanced Metering Infrastructure (AMI)," IEEE Power and Energy General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century, Pittsburgh, PA, 2008, pp. 1-5.

[27] V. Aravinthan, V. Namboodiri, S. Sunku, and W. Jewell, "Wireless AMI Application and Security for Controlled Home Area Networks," IEEE Power and Energy General Meeting, San Diego, CA, 2011, pp. 1- 8.

[28] B. Vaidya, D. Makrakis, and H. Mouftah, "Secure Multipath Routing for AMI Network in Smart Grid," in Proc. IEEE 31st International Conference on Performance Computing and Communications (IPCCC), Austin, TX, 2012, pp. 408-415.

[29] Y. Yan, Y. Qian, and H. Sharif, "A Secure and Reliable In-network Collaborative Communication Scheme for Advanced Metering Infrastructure in Smart Grid," in Proc. IEEE Wireless Communications and Networking Conference (WCNC), Cancun, Quintana Roo, 2011, pp. 909-914.

[30] G. N. Ericsson, "Cyber security and power system communicationessential parts of a smart grid infrastructure," IEEE Transactions on Power Delivery, Vol. 25, No. 3, pp. 1501-1507, July 2010.

[31] R. Anthony, L. Metke, L. Randy, and Ekl, "Security technology for smart grid networks," IEEE Transactions on Smart Grid, Vol. 1, No. 1, pp. 99-106, June 2010.

[32] J. Seo and C. Lee, "The green defenders," IEEE Power and Energy Magazine, VOL.9, NO.1, pp. 82-90, January/February 2011.

[33] D. Wei, Y. Lu, M. Jafari, P. Skare, and K. Rohde, "An integrated security system of protecting smart grid against cyber -attacks," Innovative Smart Grid Technologies (ISGT), Gaithersburg, MD, USA, 19-21 January 2010.

[34] M. A. Rahman and H. Mohsenian-Rad, "'False data injection attacks with incomplete information against smart power grids," in Proc. IEEE Conf. Global Commun. (GlobeCom), Dec. 2012, pp. 3153-3158.

[35] Y. Zhao, A. Goldsmith, and H. V. Poor, "Fundamental limits of cyber physical security in smart power grids," in Proc. 52nd IEEE Conf. Decision Control, Florence, Italy, Dec. 2013, pp. 200-205.

[36] Y. Huang, Mohammad Esmalifalak, Huy Nguyen, Rong Zheng, and Zhu Han, "Bad data injection in smart grid: Attack and defense mechanisms," IEEE Commun. Mag., vol. 51, no. 1, pp. 27-33, Jan. 2013.

[37] M. Esmalifalak, H. Nguyen, R. Zheng, L. Xie, L. Song, and Z. Han, "A stealthy attack against electricity market using independent component analysis," IEEE Syst. J., to be published.

[38] G. Chaojun, P. Jirutitijaroen, and M. Motani, "Detecting false data injection attacks in AC state estimation," IEEE Trans. Smart Grid, vol. 6, no. 5, pp. 2476-2483, Sep. 2015.

[39] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla, "Smart grid data integrity attacks," IEEE Trans. Smart Grid, vol. 4, no. 3, pp. 1244-1253, Sep. 2013.

[40] D. Li, Z. Aung, J. R. Williams, and A. Sanchez, "Efficient Authentication Scheme for Data Aggregation in Smart Grid with Fault Tolerance and Fault Diagnosis," Innovative Smart Grid Technologies (ISGT), 2012 IEEE PES, pp. 1-8.

[41] F. Li, B. Luo and P. Liu, "Secure Information Aggregation for Smart Grids Using Homomorphic Encryption," in Proc. 2010 IEEE Conf. Smart Grid Communication, pp. 327-332.

[42] P. Schaumont, "True Random Number Generation," Circuit Cellar, No. 268, pp. 52-58, Nov. 2012.