Attacks, Vulnerabilities and Security Requirements in Smart Metering Networks

Muhammad Daniel Hafiz Abdullah, Zurina Mohd Hanapi, Zuriati Ahmad Zukarnain, Mohamad Afendee Mohamed

Department of Communication Technology and Network

Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, Malaysia

[e-mail : {daniel_hafiz, zurinamh, zuriati, afendee}@upm.edu.my]

*Corresponding author: Muhammad Daniel Hafiz Abdullah

Received February 10, 2014; revised May 14, 2014; revised June 21, 2014; revised November 20, 2014; accepted February 27, 2015; published April 30, 2015

Abstract

A smart meter is one of the core components in Advanced Metering Infrastructure (AMI) that is responsible for providing effective control and monitor of electrical energy consumptions. The multifunction tasks that a smart meter carries out such as facilitating two-way communication between utility providers and consumers, managing metering data, delivering anomalies reports, analyzing fault and power quality, simply show that there are huge amount of data exchange in smart metering networks (SMNs). These data are prone to security threats due to high dependability of SMNs on Internet-based communication, which is highly insecure. Therefore, there is a need to identify all possible security threats over this network and propose suitable countermeasures for securing the communication between smart meters and utility provider office. This paper studies the architecture of the smart grid communication networks, focuses on smart metering networks and discusses how such networks can be vulnerable to security attacks. This paper also presents current mechanisms that have been used to secure the smart metering networks from specific type of attacks in SMNs. Moreover, we highlight several open issues related to the security and privacy of SMNs which we anticipate could serve as baseline for future research directions.

Keywords: Smart metering networks, smart grid, security attacks, privacy

http://dx.doi.org/10.3837/tiis.2015.04.013 **ISSN : 1976-7277**

1. Introduction

The limitations of legacy power grid systems have introduced a new power grid system called the smart grid. The smart grid can be defined as an integration of power grid systems with communication systems [1, 2]. It is undeniable that the integration of communication systems into the power grid systems has improved the ways of managing and controlling the resources of power grid systems such as power flow and data management system. This integration also enables a two-way communication between utility provider and energy consumers which also allows an efficient ways to manage and monitor data flow from a hierarchical structure of the smart grid systems. The smart grid consists of two main components namely power grid systems and communication systems. Subsequently, power grid systems can be further divided into three major sections; power generation, power transmission and power distribution. These three sections are responsible for supplying electrical power to consumers' homes, factories and business buildings. On the other hand, the communication systems comprise of different network topologies such as Wide Area Network (WAN), Neighborhood Area Network (NAN), Building Area Network (BAN) and private network called Home Area Network (HAN) [3]. These four network topologies are the core networks that allow data exchange between utility provider and consumers. The smart grid's function is not only about adding communication systems; it also covers sustainable energy system, efficient energy management and secure energy supply [4].

In order to ensure interoperability between different types of network topologies with different set of communication technologies, a smart device called smart meter has been introduced. A smart meter is a digital device that provides advanced functionalities of remote meter reading for collecting smart meter data. This includes sending and executing control commands such as remote connect or disconnect [5]. By communicating with other smart meters, a network of smart meters called smart metering networks (SMNs) is formed. This network is also known as Advanced Metering Infrastructure (AMI) and it is part of the smart grid communication systems that is responsible for managing and delivering smart meter information such as billing data, command data, request data and Demand-response (DR) data [6, 7, 8]. These data will be sent to the nearest utility provider office as well as consumers for analysis and billing process. With these abilities, a smart meter is not only can provide effective communication but also enable consumers to efficiently manage and monitor their own energy usage through DR programs such as incentive-based or time-based programs [9, 10, 11].

The growing dependability of smart meter communications on Internet-based communication has increased the vulnerabilities of smart metering networks to Internet-based attacks such as eavesdropping, false data injection, denial of service (DoS), impersonation, replay, repudiation and node compromised attacks [12]. These attacks are dangerous to the smart grid systems in the sense that it can cause problems like power instability and huge financial losses. Nowadays, many security solutions have been proposed to secure data transmission in wired and wireless networks. However, these solutions cannot simply be applied to SMNs due to limitations on smart metering devices such as memory, communication and computational capabilities. Apart from security issues, privacy has also becoming hot issue that has been publicly raised by researchers in power industries and academia realm [13, 14, 15, 16, 17, 18, 19, 20]. Within every 1, 5, 10, 15 or 30 minutes intervals, smart meter data will be recorded and transmitted to utility servers and as such there is vast amount of data will be exchanged between utility provider server and consumers [17, 21, 22, 23]. These frequent data collection of smart meters have increased the risk of violating human privacy such as information theft and profiling human behavioral patterns [24].

To the best of our knowledge, to date, there are only three available surveys on threats and vulnerabilities have been covered in the area of SMNs [25, 26, 27]. However, most of the existing surveys focus more on defining the types of attacks and vulnerabilities without providing detail security analysis. Furthermore, providing good solution to address security attacks in SMNs is still becoming a void of this area that needs to be filled in. Our paper provides detail discussions on the fundamental architecture of smart meter communication networks and explains how such networks can be vulnerable to security attacks. Our paper also provides detail security analysis on attacks, vulnerabilities and countermeasures that have been discussed in the existing schemes in order to defend against specific types of attacks in SMNs. In addition, we also highlight several security challenges and open issues related to privacy, data aggregation and node compromise attack which have been neglected by most of the existing schemes. We anticipate that this paper would provide some significant insights for research on improving the security and privacy issues of SMNs.

The rest of this paper is organized as follows. In Section 2, we discuss a hierarchical structure of smart grid communication systems. In Section 3, we provide discussion on the network topologies that involved in smart grid communication systems. The types of security attacks in SMNs are presented in Section 4. In Section 5, we list and explain several security requirements for data communication security. Section 6 discusses security analysis on the existing schemes in SMNs. Section 7 discusses several open issues, future research directions and possible solutions to cater the node compromise attack and last but not least, section 8 concludes this paper.

2. The Smart Grid: Communication and Power Grid Systems

The smart grid systems can be divided into two separate systems which are communication systems and power grid systems. As depicted in **Fig. 1**, the smart grid communication systems consist of several numbers of network topologies implemented and structured in a hierarchical manner. As can be seen, the base station acts as a data collector acquired from the lower distribution networks encompassing Wide Area Network (WAN), Neighborhood Area Network (NAN), Building Area Network (BAN) and Home Area Network (HAN). These four network topologies are the core communication network in smart grid and will be further discussed in the following section.

On the other hand, from the perspective of power grid systems point of view, energy can be generated via a variety of power generation plants such as nuclear, hydro, wind and solar systems. The generated energy is then distributed via two different power substations. The first substation known as transmission substation and it is normally located in a subsequent position of the power generation plant. This substation is responsible for supplying high amount of voltage from power generation plant to the next substation known as distribution substation. Basically, the distribution substation is located in close proximity of industrial or residential areas where it is responsible for converting the high voltage power supply into medium voltage power supply prior to distributing it to low voltage feeder pillars. The low voltage feeder pillar then distributes the low voltage power supply to the nearest industrial or residential areas such as commercial buildings and homes.

3. The Smart Metering Networks

To facilitate data communication in the smart grid, several types of networks such as HAN, BAN, NAN and WAN have been introduced. Details about these networks will be discussed in the following subsections.

3.1 Home Area Network (HAN)

HAN is a dedicated network connecting all smart devices that operate within a home network. To enable communication in HAN, a wireless smart meter is placed within consumer's home which is then act as a HAN gateway that is responsible to manage all the data communication involved [28]. Through this network, consumer can control and monitor energy consumptions and data flow between home appliances such as thermostats, air conditioners, fridges, washers, dryers and stoves [29].

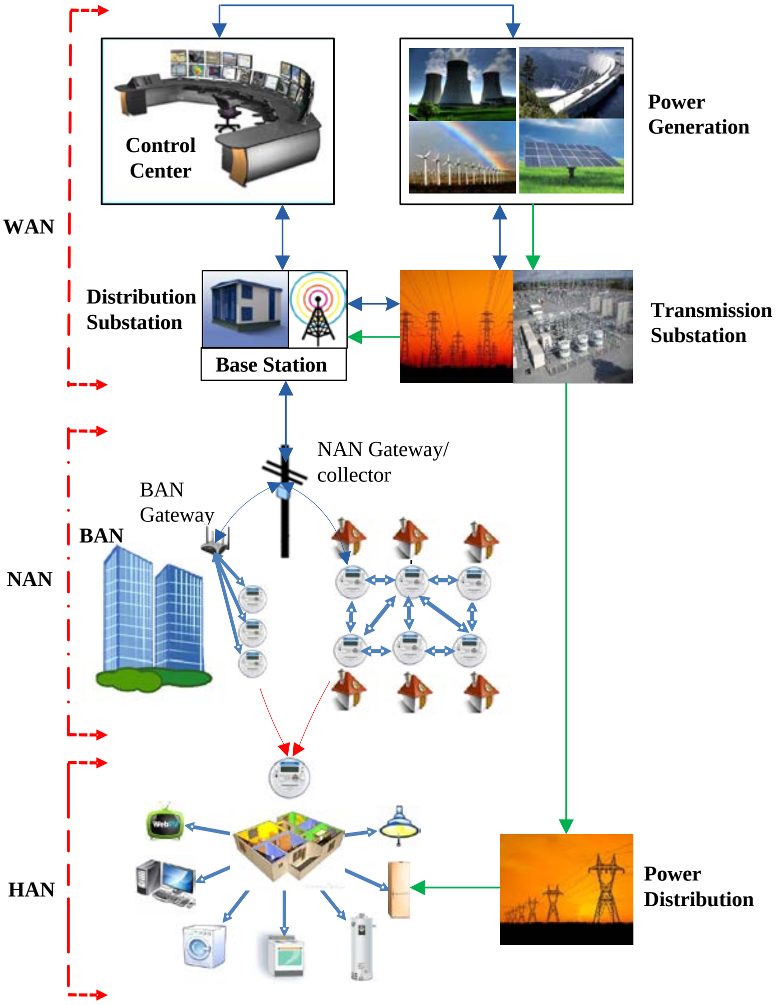

Fig. 1. The smart grid: Communication and power systems

↔	Communication Flows
→	Power Flows
WAN	Wide Area Network
NAN	Neighborhood Area Network
BAN	Building Area Network
HAN	Home Area Network

A typical HAN consists of three main functional components known as coordinator/gateway, digital devices and communication protocol. The coordinator/gateway is responsible to manage, control and monitor the communication links between all digital devices that operate within the home network. The coordinator/gateway is also responsible in enabling the communication between the HAN and BAN gateways in the case of the HAN gateway is attached to a building network which consists of hundreds or thousands of home apartments. Meanwhile, the digital devices are responsible in providing information for energy management purposes and the communication protocol is used to ensure the interoperability and compatibility between different hardware, protocols and data exchange formats. **Fig. 2** shows the example of HAN. Nowadays, many communication protocols have been proposed in order to ensure the high level of interoperability between different type of devices in HAN including ZigBee, 6LoWPAN, Z-Wave, Wireless HART, Bluetooth, ISA 100.11a and M-Bus. However, detail information about these protocols will not be discussed in this paper.

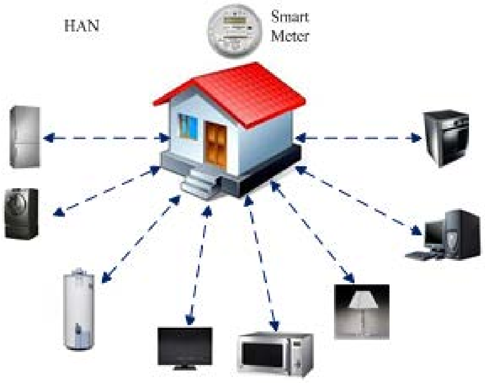

Fig. 2. Home area network (HAN)

3.2 Building Area Network (BAN)

BAN is a network that covers the communication within a building which consists of a number of apartments or homes. **Fig. 3** shows the BAN network topology that consists of several numbers of HANs. In order to maintain communication links between BAN and HANs, a device called BAN gateway is installed in the building. The functions of this gateway are to aggregate, monitor and provide information such as power requirement and energy consumption on its HANs, whereby, this information will be sent to the nearest data collector center or NAN gateway. In order to enable the communications between BAN gateway and its HANs, network technologies such as Wi-Fi or WiMAX is a preferably suitable alternative to be used. However, recent work by [3, 30] shows that Wi-Fi might not be of a well-suited technology to support the communications in BAN due to the need to have long distance (over one hundred meters) coverage for a particular apartment to the BAN gateway.

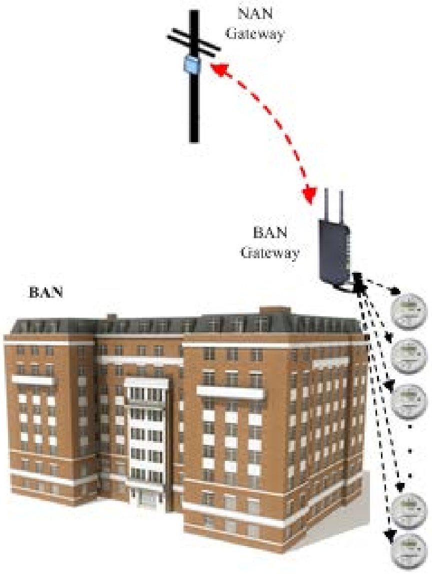

Fig. 3. Building area network (BAN)

3.3 Neighborhood Area Network (NAN)

NAN is a network which provides communication links between utility providers to smart meters that are installed in consumer sites as shown in **Fig. 4**. Through a NAN collector, the energy consumption of a certain neighborhood can be measured and monitored by the corresponding distribution substation. Nowadays, there are over 20 million and 78 million smart meters installed in North America and Japan respectively. All these smart meters are equipped with RF (Radio Frequency) mesh communication technology for the purpose of collecting different types of smart meter data [7, 31]. RF mesh has been the preferred technology to be implemented in smart metering networks for its unique properties such as capability to cater for multihop network and dynamically form ad hoc communication links among neighboring smart meter nodes. Besides RF mesh technology, there are other solutions such as WiMAX, power-line communication (PLC) and cellular technologies. However, the use of such technologies is still not widely implemented due to several factors such as requiring high investment cost and expensive equipment to be deployed.

3.4 Wide Area Network (WAN)

WAN is a communication network that covers long-distance data transmission from NAN gateway points to utility's back-office systems or control center. As shown in **Fig. 1**, the interface between WAN and NANs consists of base stations, while the interface between NAN and BANs is a BAN gateway which is then connected to smart meters which act as an interface between BAN and HANs. However, in the case of individual residence house, the smart meters act directly as an interface between NAN and HANs. To facilitate the communications within WAN, communication technologies such as WiMAX, cellular, PLC and fiber optic are among suitable technologies that can be used to fulfill the requirements for WAN communication.

It is indubitable that the introduction of communication technologies in the power grid systems has enabled two-way communication between utility provider and consumer. This two-way communication has allowed more adaptive, efficient and effective ways to manage and utilize the electrical energy. However, with all the provided advantages, the dependency of smart metering networks on Internet-based communication has raised the vulnerabilities, cyber-attacks and privacy violation in smart metering networks [12, 32, 33, 34, 35]. Therefore, it is important to provide appropriate security and privacy mechanisms in order to protect the data communication in the smart grid system as well as the consumer's private and confidential data.

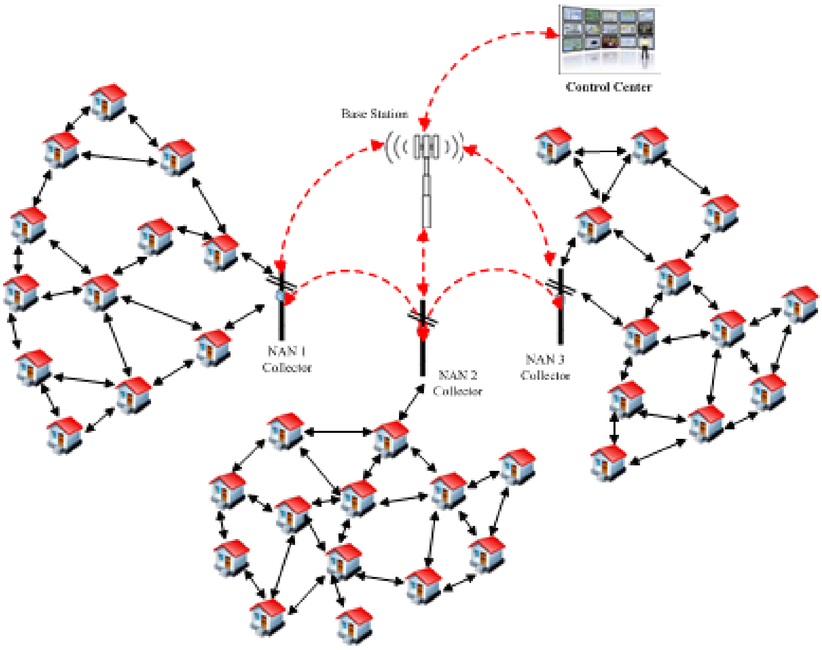

Fig. 4. Neighborhood area network (NAN)

4. Security Attacks in Smart Metering Networks

Similar to other wireless networks such as wireless sensor networks (WSNs) and Mobile Ad hoc Networks (MANETs), SMNs is also vulnerable to different types of security threats such as impersonation, false data injection and node compromise attacks [12]. Although these networks have similar issues in term of having limited memory and communication bandwidth, dependability on multihop-fashion communication and having low processing power, SMNs tends to be more vulnerable to security attacks due to the introduction of two-way communication between utility provider and customers that can open door for any attackers to jeopardize the network [8, 30].

In this section, we discuss several types of security attacks on SMNs and explain how these attacks work and what are the effects and consequences of these attacks towards SMNs.

4.1 False Data Injection Attack (FDI)

FDI is a kind of attack that tries to manipulate data integrity by injecting false data into the network with the aim to mislead the control center to make erroneous decision on contingency analysis, power dispatch and billing process [36]. In SMNs, the FDI occurs when attacker successfully intercept and alter the content of the data prior to being sent back to the network. Since wireless medium and broadcast-based communication are used to transmit data in SMNs, data transmitted by smart meters using wireless communication mediums can be easily captured or intercepted by the attacker. This type of attack can be very harmful especially when several attackers are colluding to inject false data into the network. To the best of our knowledge, colluding FDI is among the challenging attacks to be detected in authenticated SMNs due to the lack or insufficient of misbehavior detection mechanism used in current security schemes. As a consequence, when these nodes are successfully being compromised or hijacked, injecting false data can be easily done by the attacker. FDI attack is not only can cause damage to the original data, but it can also lead to other damages such as power demand overwhelming, power instability, blackout or even a power generator to self-destruct [36, 37].

4.2 Denial-of-Service Attack (DoS)

DoS is a common attack in wired or wireless communications whereby the most well-known DoS in SMNs is jamming attack. A jamming attack basically occurs in wireless networks in which a jammer tries to disrupt the radio frequencies used by the smart meters by transmitting another radio signals to interrupt data transmission process [8, 38]. In order to mitigate this attack, the authors in [38] have used a game theoretical-based approach called zero-sum stochastic. In this game, both sensor (smart meter) and jammer compete with each other in delivering the data to control center while the jammer tries to block the available communication channels. Other than jamming attack, packet flooding and packet dropping attacks are also other examples of attacks that fall under DoS category.

4.3 Eavesdropping Attack (EVD)

EVD is another common attack in SMNs which can be defined as an act of secretly listening to and recording of data communication over neighboring smart meters. EVD may or may not be dangerous; it depends on the eavesdropper’s motivations. However, EVD can invade human’s privacy via illegitimate actions such as information theft, identity fraud and profiling human’s behavioral patterns. Currently, there exist several schemes focusing on detecting and countering the EVD [19, 39, 40, 41, 42, 43, 44]. However, almost all of the schemes focus more on improving data encryption techniques that require extra memory and high computational power for execution.

4.4 Impersonation Attack (IMP)

IMP or man-in-the-middle attack is an attack where a malicious smart meter snatches the identity of other legit smart meters. By masquerading as a legitimate smart meter, an attacker is able to receive and alter the content of the received messages [45]. What worse, the IMP is used by masquerader acting as several fake smart meters identities performing various illegal actions that introduce a more severe threat known as Sybil attack. The Sybil attack has the ability in crippling or degrading the smart meter network operation by colluding together to launch DoS attacks such as packet dropping and flooding attacks. IMP may not only happen on meter-to-meter communication but also on meter-to-smart appliances communication which can cause scenarios like demand exceeding supply, billing overcharge or even electricity shutdown to happen [8, 28, 46].

4.5 Replay Attack (REP)

REP is an attack attempting to disrupt security by storing or recording unauthorized data and retransmitting the data back at a later time after some modification have been made to the original data. For example, data transmission between smart meters can be captured or intercepted by an attacker and replay the data after performing some modifications. REP can be prevented by using nonce techniques such as timestamp or message sequence number [47]. However, the use of message sequence number requires reliable communication channels whereas, using timestamp would require the exchange of extra messages which may cause communication overhead.

4.6 Repudiation Attack (RPD)

RPD can be referred to as denial of participation in the communication. The role of non-repudiation functions in smart metering networks is mainly to ensure that the consumers or the utilities will not deny that they have been sending and/or receiving their authenticated metering data due to motive like avoiding responsibility. The scheme proposed by [48] uses one-time signature generation method in order to protect the smart meter data from repudiation-based attacks. The scheme has the ability to counter against non-repudiation attack and at the same time helps to reduce the energy consumption and computational cost. However, the use of one-time signature generation generates another problem called signature flaw. This flaw is related to the use of one key for all authentication process. If this key is compromised, the security of the whole network will be at risk since only one signature is used for the entire communication process.

4.7 Node compromise Attack (CMP)

CMP is the most interesting and challenging attack in SMNs which involves hijacking action from a node by physically accessing the smart meter node with the aims to take control of communication and gain unauthorized access to the node’s sensitive data such as cryptographic information [49]. This attack is significantly dangerous for the fact that even if only one node is compromised, shared keys would possibly revealed and thus, allowing the attacker to participate in encryption and decryption process [50]. In the worst case scenario, the attacker may also inject false data into the network after some modifications have been made on the original encrypted data. In order to mitigate this attack, the scheme proposed by [51] uses reputation-based trust management which is based on a majority rule trust algorithm to detect any misbehaved nodes that give false reading on sensed data.

5. Security Requirement for Smart Metering Networks

Due to unique properties of SMNs such as two-way communication, it is difficult and challenging task to secure and protect smart meter data from being compromised by the attackers. Although there are many security solutions available for wired and wireless networks, they cannot simply be directly implemented into SMNs. Therefore, it is important to explore the security requirements for this network in order to ensure the security of data communication in SMNs.

In this section, we highlight and discuss several security requirements for SMNs. As shown in **Fig. 5**, there are six security requirements, namely, data confidentiality, data integrity, data freshness, data availability, non-repudiation and authentication which are of important aspects to be considered in ensuring the security of data communication in SMNs.

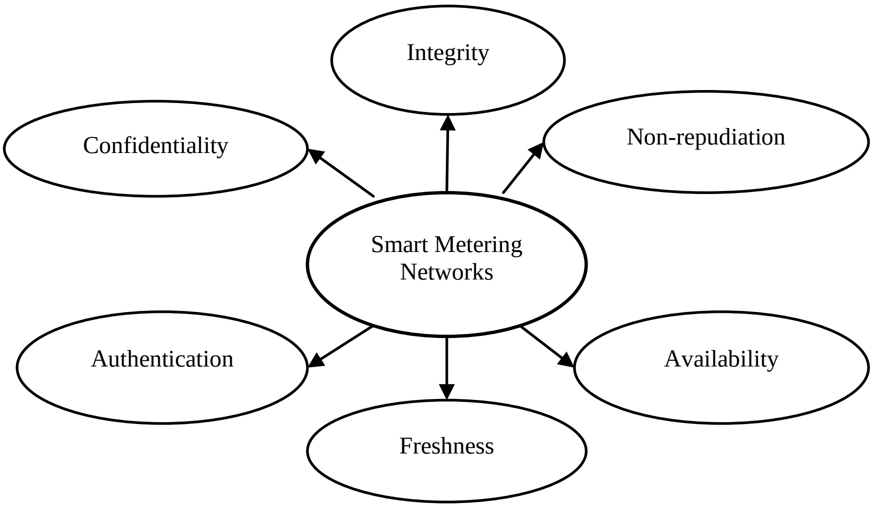

Fig. 5. Security requirements for SMNs

5.1 Data Confidentiality

Data confidentiality needs to be preserved to ensure that the content of data being transmitted will never be exposed to unauthorized parties. In SMNs, data confidentiality is an essential requirement to protect data from attacks like EVD and men-in-the-middle (MIM) and to preserve user's privacy information. In SMNs, data confidentiality can be ensured by using data encryption techniques such as symmetric or asymmetric encryption.

5.2 Data Integrity

When transferring data over the network, the sender would have wanted to ensure that the receiver gets the data that are of genuine or similar as have been transferred earlier. The purpose of having data integrity in smart metering communication is to ensure that the content of the original data has not been modified or altered either accidentally or maliciously during transmission process. To guarantee data integrity in SMNs, hash functions or Message Authentication Code (MAC) can be added to the encrypted data so that any unauthorized changes to the original data can be detected.

5.3 Data Freshness

Data freshness is another important security requirement to ensure that the transmitted data is fresh and recent. In SMNs, data freshness can be achieved by using nonce techniques which can be represented in the form of a counter, timestamp or message sequence number that is generated randomly using random number generator. To avoid from being altered by an attacker, the nonce will be encrypted with the message before it can be sent to its destination. The purpose of having such requirement is to protect the data from being manipulated by replay attacker.

5.4 Data Availability

If confidentiality is associated to privacy, data availability on the other hand is associated to survivability. In SMNs, data availability ensures that the network is alive, and data is accessible even in the presence of DoS attack. A DoS attack could be launched at any layer of SMNs such as jamming attacks which can disrupt physical and Medium Access Control layers functions. At the network layer, an attacker could interrupt or destroy the routing protocol whereas at the application layer, an attacker could disable or deactivate important services such as network broadcast and key management services.

5.5 Non-Repudiation

Non-repudiation is a security requirement to ensure that a sender or receiver cannot deny of having sent or received a message. This requirement is essential especially to detect any existence of an attacker that tries to launch false data injection, flooding and replay attacks. There are many ways to enable this requirement; one of them is by using public key cryptography.

5.6 Authentication

Authentication is the process of determining or verifying either someone or something is who or what it is claimed to be. Authentication can be divided into entity authentication and data authentication [49]. Entity authentication (EA) or source authentication gives the opportunity to a receiver to verify whether the received data is sent by the right source or not. In this case, an attacker cannot participate or join into any activities in the targeted network because it has no privilege to access the network. Without entity authentication, an attacker could masquerade as a legit smart meter, thus gaining unauthorized access to sensitive data. On the other hand, data authentication (DA) allows a receiver to verify that the received data are of similar ones that have been transmitted.

6. Security Analysis on Existing Schemes in Smart Metering Networks

This section discusses the security analysis on existing secure SMNs schemes. The discussion covers the type of security attacks, vulnerabilities and countermeasures that have been used to defend against specific type of attacks in SMNs. As depicted in **Table 1**, 14 existing schemes have been evaluated against seven different types of attacks in which, 11 schemes utilize the cryptographic-based mechanism [16, 17, 19, 39, 40, 41, 42, 44, 46, 48, 52] whereas the remaining three schemes are architectural-based [29], mixing algorithm [28] and compression technique [43]. There are seven types of attacks have been considered, namely, FDI, DoS, EVD, IMP, REP, RPD and CMP attacks. As shown in **Table 1**, most of the attacks occurred in NAN (11 schemes) while the remaining 3 schemes occurred in HAN.

From **Table 1**, it can be seen that 10 out of 14 existing schemes are able to resist FDI whereas seven schemes [16, 39, 42, 44, 46, 48, 52] use MAC, while the remaining 3 schemes [17, 19, 41] use digital signature techniques. Based on this quantitative analysis, we can conclude that MAC technique is the most popular technique used by the existing schemes as compared to digital signature technique. MAC and digital signature are the two techniques that have the ability to provide data integrity service that is very useful and effective technique to detect FDI. These two techniques can also provide source authentication service that can be used to detect any smart meter nodes attempting to launch IMP. Although MAC seems to be a very popular technique to ensure data integrity in SMNs, this technique has failed to provide non-repudiation service. This is because, MAC used symmetric encryption, whereby sender and receiver used the same key for encrypting and decrypting processes. Unlike MAC, digital signature used asymmetric encryption whereby, a sender or a receiver use two different keys for encrypting and decrypting process. For instance, a sender needs to digitally sign his message using his private key before it is being sent to the receiver and upon receiving the message; the receiver can verify the message by decrypting it using the sender's public key. If the message is decrypted successfully then the receiver knows that the message is sent by the genuine sender. Otherwise, the message will be considered as malicious message. In this case, the digital signature does offer non-repudiation service while MAC is not. This is because, by using digital signature, the sender of the message cannot deny of having sent a message to the receiver because the receiver has already been successfully decrypted the message using the sender's public key. However, if we were to compare between these two techniques in terms of computational complexity, memory saving and fast algorithm execution, MAC performs much better than digital signature.

DoS is another common attack in SMNs especially when the data delivery system is based on wireless communication [53]. The most known DoS in SMNs is jamming attack. Besides jamming attack, network exhaustion attack (e.g. flooding attack) and node exhaustion attack (e.g. selective forwarding attack) are the other examples of DoS attacks that can cause massive packet delay and packet loss problems. As shown in **Table 1**, there are two schemes [28, 29] that are robust to DoS and five other schemes [39, 42, 44, 46, 52] are vulnerable to DoS. The robust scheme proposed in [29] uses ID-based mechanism to defend against DoS. In this scheme, each of the smart meters in the network will be assigned a unique ID by the data collector before joining the network. This collector is responsible for keeping the entire registered ID for authentication purposes. In the case of malicious smart meter node tries to join the network, the collector will check as to whether or not the ID provided by the malicious node is registered or not. If not, the malicious smart meter will be blocked from participating in any network activities. Although ID-based can be an efficient mechanism to prevent from DoS attacks, this mechanism is known to be susceptible to guess-based and brute-force attacks. On the other hand, the other robust scheme presented in [28] uses a channel-switching algorithm to counter the DoS attack. This algorithm works by switching to other available channels if the current channel is detected of having significant interference such as high packet loss rate. Even though channel-switching algorithm provides good mechanism to secure smart metering communication, this mechanism shows poor packet delivery ratio in the case where the jammer is able to congest almost all of the available communication channels. This is an interesting problem and the author of this paper has not proposed any solution to overcome this problem.

As aforementioned, the EVD problem is normally related to confidentiality and privacy type of attacks such as information theft, identity fraud and profiling human behavioral patterns. Further analysis shows that five schemes [39, 42, 44, 46, 52] have managed to provide a robust mechanism using shared key or pair-wise key technique to defend against EVD. A shared key or a pair-wise key is a cryptographic technique that works by sharing identical key for encrypting and decrypting processes. On the other hand, instead of using shared key or pair-wise key, four schemes [16, 19, 40, 41] use different encryption technique called homomorphic encryption. Homomorphic encryption is one of the cryptographic techniques that allow direct computation on encrypted data without the need to decrypt it first. Homomorphic encryption is among the good and the secure mechanism to provide end-to-end data confidentiality and privacy. However, such encryption technique requires extra memory, computationally expensive and impracticable to be implemented in SMNs.

Table 1. Attacks, vulnerabilities and countermeasures in existing smart metering networks

MAC	Message Authentication Code	HAN	Home Area Network

Attack Scheme	Domain	FDI	DoS	EVD	IMP	FRN - REP	RPD	CMP
Fouda et al. [29]	HAN	NA	® - ID -Based	NA	® - ID-Based	NA	NA	V
Aravinthan et al. [28]	HAN	NA	® - Chnl -Swtg	V	® - Pwd-Based	® - Nce – Sequence number	® - Evt-Log	V
Lu et al. [19]	NAN	® - DiSgn	NA	® - Homomorphic	® - DiSgn	® - Nce – Timestamp	® - DiSgn	V
Li et al. [40]	NAN	V	NA	® - Homomorphic	NA	®- Nce – Timestamp	NA	V
Varodayan et al. [43]	NAN	V	NA	® - SWC + Information-theoretic confidentiality	NA	® - Nce - Timestamp	NA	V
Deng & Yang [41]	NAN	® - DiSgn	NA	® - Homomorphic	® - ID-Based	® - Nce – Timestamp	® - DiSgn	V
Bartoli et al. [39]	NAN	® - MAC	V	® - Shared key (AES)	® - Shared key (AES)	® - Nce - Timestamp	NA	V
Efthymiou & Kalogridis [17]	NAN	® - DiSgn	NA	V	® - ID-Based	NA	® - DiSgn	V
Yan et al. [44]	NAN	® - MAC	V	® - Pair-wise key	® - ID-Based	NA	NA	V
Kim et al. [42]	NAN	® - MAC	V	® - Shared key (ECC)	® - Shared key (ECC)	® - Nce - Sequence number	® - DiSgn	V
Ayday et al. [46]	HAN	® - MAC	V	® - Pair-wise key (AES)	® - ID-Based	V	NA	V
Choi et al. [48]	NAN	® - MAC	NA	NA	® - DiSgn	V	® - DiSgn	V
Chim et al. [16]	NAN	® - MAC	NA	® - Homomorphic	® - DiSgn	® - Nce – Timestamp	NA	V
Bartoli et al. [52]	NAN	® - MAC	V	® - Pair-wise key (AES)	® -Pair-wise key (AES)	® - Nce - Timestamp	V	® - Key-Mgt

DiSgn	Digital Signature	DoS	Denial-of-Service Attack
Nce	Nonce	EVD	Eavesdropping Attack
ECC	Elliptic Curve Cryptography	IMP	Impersonation Attack
AES	Advanced Encryption Standard	REP	Replay Attack
ID-Based	Identifier-Based	RPD	Repudiation Attack
Pwd-Based	Password	CMP	Node Compromise Attack
Chnl-Swtg	Channel-Switching	FDI	False Data Injection Attack
Key-Mgt	Key Management	V	Vulnerable
Evt-Log	Event-Log	®	Robust
SWC	Slepian-Wolf Coding	NA	Not Applicable
NAN	Neighborhood Area Network		

An interesting analysis on **Table 1** comes when 12 schemes [16, 17, 19, 28, 29, 39, 41, 42, 44, 46, 48, 52] have managed to provide a good mechanism to counter against IMP using secure authentication approaches. With respect to that aspect, five of the schemes [17, 29, 41, 44, 46] use ID-based approach, one scheme [28] uses password-based approach and each of these three schemes [39, 42, 52] and [16, 19, 48] use shared key and digital signature respectively. Among four of these approaches, ID-based and password-based approaches provide faster authentication approach as compared to shared key and digital signature approaches. However, as aforementioned, these two approaches are susceptible to guess-based and brute-force attacks. Therefore, in order to implement such approaches, rigorous studies need to be carried out to overcome the identified vulnerabilities. Shared key and digital signature approaches seem to be the better solutions to defend against IMP. However, these approaches require a device with large memory capacity and powerful computational ability. Moreover, shared key approach is also vulnerable to CMP by means of device tempering. Therefore, significant tamper proof improvement is necessary for smart meter device in order to ensure this approach can be effectively implemented.

Analysis on **Table 1** also shows that nine of the schemes [16, 19, 28, 39, 40, 41, 42, 43, 52] are robust to REP. Surprisingly, all the schemes are using nonce as a technique to fight against the REP. In cryptographic term, nonce is an absolute number that used only once in a particular communication [54]. Commonly, nonce can be represented as timestamp or message sequence number that are basically represented in a number format; generated randomly. Timestamp and message sequence number are important in smart meter communication in order to ensure that old communication session will not be reused by the REP. Although timestamp and message sequence number present some advantages in terms of efficient and lightweight security mechanisms, both of these techniques require reliable communication channels to ensure message synchronization. In addition, these techniques also require extra message exchange process which in turn caused significant communication overhead especially when data is collected by the smart meters more frequently, within short time intervals.

The use of digital signature to ensure data integrity can also be leveraged to ensure non-repudiation service whereby five of the existing schemes [17, 19, 41, 42, 48] have implemented this technique for that purpose. The work in [28] on the other hand, uses event-log technique to provide non-repudiation service. The event-log technique works by recoding and storing all the event-log history for a specified number of days that will be invoked for tracking specific event upon receiving any possible complaint. Event-log technique is the most lightweight and simple technique that can provide non-repudiation service as compared to digital signature technique. However, this technique is vulnerable to insider attack since the utility provider or the third party could tamper the event-log files. Therefore, additional regulations and enforcements are needed to ensure that the event-log files cannot be tampered or manipulated by these authorized entities.

Further analysis shows that 13 out of 14 of the schemes are vulnerable to CMP [16, 17, 19, 28, 29, 39, 40, 41, 42, 43, 44, 46, 48]. This is because smart meter devices are vulnerable to physical access tampering due to lack of tamper-resistant packaging and unsecure placement of smart meter node (open area). Tampering on smart meter devices can be done using software or hardware-based techniques. In software-based technique, tampering is done by extracting all credentials stored in the smart meter device such as cryptographic information. Meanwhile, in hardware-based technique, tampering may be done by removal of physical smart protection such as anti-tampering and circuit protection seals. Once compromised, all of the other attacks such as FDI, DoS, IMP, REP and RPD can be easily launched without being detected or noticed because usually a compromised smart meter node is also a legit node that has been authenticated earlier. Analysis on **Table 1** also shows that 10 out of 13 of the vulnerable schemes have implemented cryptographic-based techniques to secure the communication from different types of attacks in SMNs. However, none of the proposed cryptographic techniques can provide a good detection mechanism on CMP. The authors in [52] proposed a scheme that works by periodically changing pair-wise and group-wise keys for the purpose of combating this attack. Although the authors claimed that their scheme has the ability to fight against the CMP, the technique used in this scheme seems impractical to be implemented due to memory and computational limitation on smart metering device. Moreover, periodic keys exchange also requires extra message exchange that may cause communication and computational overheads. Consequently, it seems that cryptographic-based techniques are not the best solution to counter CMP in SMNs. Thus, there is a need to investigate other solutions to complement the cryptographic solution in addressing CMP problem such that the efficiency would not incur unreasonable overhead.

7. Open Problems and Future Work

In this section, we will discuss several important open problems on security and privacy issues, together with some potential issues related to data aggregation in SMNs. To date, although there have been several existing works addressing these kind of problems, the proposed contributions are still at their infancy stages which require lots of improvements in order to effectively secure and protect the SMNs from security threats and privacy attacks. We also provide some possible solutions to secure SMNs from CMP. As have been identified in our literature survey, CMP has been overlooked and neglected by most (if not all) of the existing security schemes for SMNs.

7.1 Privacy Issue

It is undeniable that smart meter plays important roles in delivering smart meter data such as billing, DR, command/request information, errors and anomalies report. As smart meter communication is expected to operate in real-time or near real-time, lots of different data with high frequency intervals and different priority task will be transferred between metering devices and collector. With high frequency and short intervals of data collection by the smart meters, privacy information such as user private information, billing data and power usage data [13] would have the tendency to be revealed more easily. Once compromised, these data can be analyzed to determine energy load signature (energy fingerprint) and human behavioral patterns [55] such that privacy may be harmfully exposed. According to [55], load signature is different between devices; therefore, it is easy to determine the presence of people doing their normal routines such as when they are back from work, the usual time to sleep, when they are away from home and what type of home appliances they have. As a consequence, consumer's behavior can be profiled and monitored by cyber attackers or even burglars. These violations of privacy have raised public awareness mainly through the Internet, articles, newspapers or even in conferences [16, 56, 57, 58, 59]. In addition, improper use of consumer's privacy information can also lead to privacy abuses such as identity theft, real-time surveillance, home invasion or even unwanted publicity and embarrassment. Some other types of potential privacy threats and impacts can be found in the National Institute of Standards and Technology (NIST) [60].

7.2 Data Aggregation Issue

Data load handling in smart meters is one of the important issues that need to be catered as smart meters are responsible to collect quite an amount of abundant data in high frequency rate. Since metering data will be collected every 1, 5, 10, 15, 30 or 60 minutes, these data are considered very large for RF based network especially in a network with thousands of smart meters. This scenario somehow might cause network bottleneck problem which also contributes to delay or network latency especially when the data are sent independently by each of the smart meters. To solve this problem, data aggregation can be used as a technique to combine the data together so that the data can be sent in the form of packages rather than being transmitted individually. Data aggregation is also a useful technique for saving network bandwidth and this can be done by maximizing the use of network links by joining multiple data together prior to being sent to the next destination.

7.3 Security and Privacy Issues in Aggregated Smart Metering Data

Security is an important issue for data aggregation in order to ensure confidentiality, integrity and authenticity of data. Secure data aggregation is a new mechanism in SMNs and lots of works need to be done in order to counter from different types of attacks in smart metering networks. In data aggregation point of view, CMP seems to be the most difficult to be detected especially when the aggregator nodes have been compromised. To the best of our knowledge, there is no secure data aggregation scheme being implemented specifically to counter CMP. Hence, this could be a good and interesting problem for future research work.

Nowadays, privacy also becomes another challenging issue in aggregating smart metering data. Several works have been done to ensure privacy in aggregated smart metering data using cryptographic techniques [17, 40, 44]. However, due to real-time or near-real-time data collection in SMNs, cryptographic based solution need to be reconsidered in order to tailor this solution with the limitations on SMNs. Existing research claimed that homomorphic encryptions are the best solution to protect consumer's privacy [61, 62]. However, implementing this technique requires extra memory and powerful computing capability. Therefore, applying homomorphic encryptions in SMNs needs to be further studied in order to ensure that the requirements for executing such encryptions are tolerable with the available constraints in smart metering devices. To the best of our knowledge, there are limited number of work have been done using homomorphic encryption to protect privacy in SMNs [16, 19, 40, 41]. Therefore, designing and implementing lightweight homomorphic encryption are highly demanded, and this can become another good and interesting future research area. Other than homomorphic encryption, there is a scheme that has utilized elliptic curve cryptography (ECC) to protect consumer's privacy [63]. However, the use of ECC cryptographic function to preserve privacy is still immature and rigorous investigation and exploration of this function can be of a good research direction.

7.4 Solution for Node Compromise Attack (CMP)

The security analysis discussed in **Table 1** reveals that different types of attacks may need to be solved using different types of countermeasures. Our qualitative analysis result shows that CMP has attained less attention in most of the existing schemes. Based on our ongoing literature survey, we have also discovered that current detection mechanisms on CMP are still lacking in providing effective solutions, thus, motivates us to propose enhancement in fulfilling the identified gaps.

Detecting and eliminating node compromised attack is a challenging task in SMNs due to resource constraint issues and other unique characteristics of SMNs such as memory, computational capacity, two-way communication and wireless transmission medium are among the factors that need to be considered. In addition, due to compromised smart meter nodes are actually legit nodes that have been authenticated, thus, detecting and eliminating this attack on legit smart meter nodes becomes significantly challenging tasks. However, on the positively contrary side, since the behavior of the compromised smart meter nodes can be monitored and profiled, that would give us some advantages in the sense that certain parameters and abnormal activities such as packets dropping rate, packets flooding rate, packets modification, packets misroute and false meter reading reports can also be obtained. In order to achieve this, reputation-based trust systems will be investigated and our expected contribution will be on the implementation of this system which has been neglected by the existing schemes for SMNs.

According to **Table 1**, it is found that key management approach is the only solution that has been implemented in the current scheme to defend against node compromise attack. Key management is the management of cryptographic keys in a cryptosystem which includes the key generation, key exchange, key update, key replacement and key storage processes. However, this approach has some disadvantages in term of having high computational and communication capacities that lead to overheads Intuitively, using reputation-based trust approach may not only expected to be able to provide effective and efficient solutions to detect and eliminate node compromise attack, but can also contribute to minimize the overhead.

8. Conclusion

The transformations of power grid systems have brought significant benefits to not only utility providers but also to consumers and environment. The introductions of smart meter, wireless technologies and bidirectional communication to the power grid system have urged the need for a reliable communication for data exchange in smart metering networks. Smart metering networks are part of AMI system which is responsible for managing and delivering all metering information including billing data, DR data and anomalies report. This network is formed of a collection of hundreds or thousands of smart meters that are connected together to deliver metering information to the control center for billing and analysis purposes.

In this paper, we present the fundamental discussion of SMNs communication architecture which consist of several topologies including HAN, BAN, NAN and WAN. We have also investigated several types of attacks that occurred in SMNs and listed out some important security requirements in ensuring optimal security level of data transmission in SMNs can be achieved. We also provide detail security analysis on attacks, vulnerabilities and their corresponding countermeasures in current existing security schemes. At the end of this paper, we highlight some security challenges and open issues related to privacy, data aggregation and some potential solutions on dealing with node compromise attack. We hope that this paper could serve as a good starting point in exploring the fundamental knowledge of the communication structure, security and privacy issues of SMNs.

Acknowledgment

The main author would like to thank the anonymous reviewers for their constructive comments, and Normalia Samian from UPM for her reviews and shared suggestions in this article.

References

[1] C. W. Potter, A. Archambault, and K. Westrick, "Building a Smarter Smart Grid Through Better Renewable Energy Information," *Proceeding of the IEEE/PES Power Systems Conference and Exposition (PSCE '09)*, pp. 1-5, 2009. Article (CrossRef Link)

[2] V. K. Sood, D. Fischer, J. M. Eklund, and T. Brown, "Developing a Communication Infrastructure for The Smart Grid," *Proceeding of the IEEE Electrical Power & Energy Conference (EPEC)*, pp. 1-7, 2009. Article (CrossRef Link)

[3] M. M. Fouda, Z. M. Fadlullah, N. Kato, L. Rongxing, and S. Xuemin, "Towards a Light-weight Message Authentication Mechanism Tailored for Smart Grid Communications," *Proceeding of the IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp. 1018-1023, 2011. Article (CrossRef Link)

[4] E. SmartGrids, "Strategic Deployment Document for Europe's Electricity Networks of the Future," *European Technology Platform SmartGrids. Brussels*, 2008.

[5] G. Kalogridis, M. Sooriyabandara, Z. Fan, and M. A. Mustafa, "Toward Unified Security and Privacy Protection for Smart Meter Networks," *IEEE Systems Journal*, pp. 1-14, 2013. Article (CrossRef Link)

[6] S. S. S. R. Depuru, W. Lingfeng, V. Devabhaktuni, and N. Gudi, "Smart Meters for Power Grid - Challenges, Issues, Advantages and Status," *Proceeding of the IEEE/PES Power Systems Conference and Exposition (PSCE)*, pp. 1-7, 2011. Article (CrossRef Link)

[7] I. Kitagawa and S. Sekiguchi, "Technologies Supporting Smart Meter Networks," *FUJITSU Sci. Tech. J*, vol. 49, pp. 307-312, 2013.

[8] V. Namboodiri, V. Aravinthan, S. N. Mohapatra, B. Karimi, and W. Jewell, "Toward a Secure Wireless-Based Home Area Network for Metering in Smart Grids," *IEEE Systems Journal*, pp. 1-12, 2013. Article (CrossRef Link)

[9] P. Khajavi, H. Abniki, and A. B. Arani, "The Role of Incentive Based Demand Response Programs in Smart Grid," *Proceeding of the 10th International Conference on Environment and Electrical Engineering (EEEIC)*, pp. 1-4, 2011. Article (CrossRef Link)

[10] W. M. Taqqali and N. Abdulaziz, "Smart Grid and Demand Response Technology," *Proceeding of the IEEE InternationalEnergy Conference and Exhibition (EnergyCon)*, Manama, Bahrain, pp. 710-715, 2010. Article (CrossRef Link)

[11] J. Wang, M. Biviji, and W. M. Wang, "Case Studies of Smart Grid Demand Response Programs in North America," *Proceeding of the IEEE PES Innovative Smart Grid Technologies (ISGT)*, pp. 1-5, 2011. Article (CrossRef Link)

[12] F. M. Cleveland, "Cyber Security Issues for Advanced Metering Infrasttructure (AMI)," *Proceeding of the IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century*, Pittsburgh, pp. 1-5, 2008. Article (CrossRef Link)

[13] A. Bleicher, "*Privacy on the Smart Grid: Are Smart Meters Spies? They Don't Have To Be,*" Available: http://spectrum.ieee.org/energy/the-smarter-grid/privacy-on-the-smart-grid, Access on 12 May 2011.

[14] D. Chen, S. Barker, A. Subbaswamy, D. Irwin, and P. Shenoy, "Non-Intrusive Occupancy Monitoring using Smart Meters," *Proceeding of the 5th ACM Workshop on Embedded Systems For Energy-Efficient Buildings*, pp. 1-8, 2013. Article (CrossRef Link)

[15] D. Chen, D. Irwin, P. Shenoy, and J. Albrecht, "Combined Heat and Privacy: Preventing Occupancy Detection from Smart Meters," *Proceeding of the 12th IEEE Conference on Pervasive Computing and Communications (PerCom)*, 2014. Article (CrossRef Link)

[16] T. W. Chim, S. M. Yiu, L. C. K. Hui, and V. O. K. Li, "PASS: Privacy-preserving Authentication Scheme for Smart Grid Network," *Proceeding of the IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pp. 196-201, 2011. Article (CrossRef Link)

[17] C. Efthymiou and G. Kalogridis, "Smart Grid Privacy via Anonymization of Smart Metering Data," *Proceeding of the First IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pp. 238-243, 2010. Article (CrossRef Link)

[18] S. McLaughlin, P. McDaniel, and W. Aiello, "Protecting Consumer Privacy from Electric Load Monitoring," *Proceeding of the 18th ACM Conference on Computer and Communications Security*, pp. 87-98, 2011. Article (CrossRef Link)

[19] L. Rongxing, L. Xiaohui, L. Xu, L. Xiaodong, and S. Xuemin, "EPPA: An Efficient and Privacy-Preserving Aggregation Scheme for Secure Smart Grid Communications," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, pp. 1621-1631, 2012. Article (CrossRef Link)

[20] W. Yang, N. Li, Y. Qi, W. Qardaji, S. McLaughlin, and P. McDaniel, "Minimizing Private Data Disclosures in the Smart Grid," *Proceeding of the ACM conference on Computer and Communications Security*, pp. 415-427, 2012. Article (CrossRef Link)

[21] IBM, "*Build Smart Metering Solutions With IBM Informix TimeSeries,"* Available: http://www.itf-edv.de/fileadmin/user_upload/Aktuelles_Start/5106-build-smart-metering-solutions-with-ibm-informix-timeseries.pdf

[22] S. Karnouskos, P. G. d. Silva, and D. Ilic, "Assessment of High-Performance Smart Metering for The Web Service Enabled Smart Grid Era," *Proceeding of the 2nd ACM/SPEC International Conference on Performance Engineering*, pp. 133-144, 2011. Article (CrossRef Link)

[23] MAXIM, "*Smart Meters Overview,"* Available: http://www.maxim-ic.com/solutions/guide/smart-grid/smart-meter.pdf

[24] L. Husheng, M. Rukun, L. Lifeng, and R. C. Qiu, "Compressed Meter Reading for Delay-Sensitive and Secure Load Report in Smart Grid," *Proceeding of the First IEEE International Conference onSmart Grid Communications (SmartGridComm)*, pp. 114-119, 2010. Article (CrossRef Link)

[25] F. Aloul, A. Al-Ali, R. Al-Dalky, M. Al-Mardini, and W. El-Hajj, "Smart Grid Security: Threats, Vulnerabilities and Solutions," *International Journal of Smart Grid and Clean Energy*, vol. 1, pp. 1-6, 2012. Article (CrossRef Link)

[26] F. Skopik, Z. Ma, T. Bleier, and H. Grüneis, "A Survey on Threats and Vulnerabilities in Smart Metering Infrastructures," *International Journal of Smart Grid and Clean Energy*, vol. 1, pp. 22-28, 2012. Article (CrossRef Link)

[27] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A Survey on Cyber Security for Smart Grid Communications," *IEEE Communications Surveys & Tutorials*, vol. 14, pp. 998-1010, 2012. Article (CrossRef Link)

[28] V. Aravinthan, V. Namboodiri, S. Sunku, and W. Jewell, "Wireless AMI Application and Security for Controlled Home Area Networks," *Proceeding of the IEEE Power and Energy Society General Meeting*, pp. 1-8, 2011. Article (CrossRef Link)

[29] M. M. Fouda, Z. M. Fadlullah, and N. Kato, "Assessing Attack Threat Against ZigBee-based Home Area Network for Smart Grid Communications," *Proceeding of the International Conference on Computer Engineering and Systems (ICCES)*, pp. 245-250, 2010. Article (CrossRef Link)

[30] M. M. Fouda, Z. M. Fadlullah, N. Kato, L. Rongxing, and S. Xuemin, "A Lightweight Message Authentication Scheme for Smart Grid Communications," *IEEE Transactions on Smart Grid*, vol. 2, pp. 675-685, 2011. Article (CrossRef Link)

[31] B. Lichtensteiger, B. Bjelajac, Mu, x, C. ller, and C. Wietfeld, "RF Mesh Systems for Smart Metering: System Architecture and Performance," *Proceeding of the 2010 First IEEE International Conference onSmart Grid Communications (SmartGridComm)*, pp. 379-384, 2010. Article (CrossRef Link)

[32] W. Dong, L. Yan, M. Jafari, P. M. Skare, and K. Rohde, "Protecting Smart Grid Automation Systems Against Cyberattacks," *IEEE Transactions on Smart Grid*, vol. 2, pp. 782-795, 2011. Article (CrossRef Link)

[33] A. Hahn and M. Govindarasu, "Cyber Attack Exposure Evaluation Framework for The Smart Grid," *IEEE Transactions on Smart Grid*, vol. 2, pp. 835-843, 2011. Article (CrossRef Link)

[34] H. Khurana, M. Hadley, L. Ning, and D. A. Frincke, "Smart-Grid Security Issues," *IEEE Security & Privacy*, vol. 8, pp. 81-85, 2010. Article (CrossRef Link)

[35] P. McDaniel and S. McLaughlin, "Security and Privacy Challenges in The Smart Grid," *IEEE Security & Privacy*, vol. 7, pp. 75-77, 2009. Article (CrossRef Link)

[36] H. Yi, L. Husheng, K. A. Campbell, and H. Zhu, "Defending False Data Injection Attack on Smart Grid Network Using Adaptive CUSUM Test," *Proceeding of the 45th Annual Conference on Information Sciences and Systems (CISS)*, pp. 1-6, 2011. Article (CrossRef Link)

[37] X. Le, M. Yilin, and B. Sinopoli, "False Data Injection Attacks in Electricity Markets," *Proceeding of the First IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pp. 226-231, 2010. Article (CrossRef Link)

[38] L. Husheng, L. Lifeng, and R. C. Qiu, "A Denial-of-Service Jamming Game for Remote State Monitoring in Smart Grid," *Proceeding of the 45th Annual Conference on Information Sciences and Systems (CISS)*, pp. 1-6, 2011. Article (CrossRef Link)

[39] A. Bartoli, Herna, x, J. ndez-Serrano, M. Soriano, M. Dohler, A. Kountouris, and D. Barthel, "Secure Lossless Aggregation for Smart Grid M2M Networks," *Proceeding of the First IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pp. 333-338, 2010. Article (CrossRef Link)

[40] L. Fenjun, L. Bo, and L. Peng, "Secure Information Aggregation for Smart Grids Using Homomorphic Encryption," *Proceeding of the First IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pp. 327-332, 2010. Article (CrossRef Link)

[41] D. Pan and Y. Liuqing, "A Secure and Privacy-Preserving Communication Scheme for Advanced Metering Infrastructure," *Proceeding of the IEEE PES Innovative Smart Grid Technologies (ISGT)*, pp. 1-5, 2012. Article (CrossRef Link)

[42] K. Sungwook, K. Eun Young, K. Myungsun, C. Jung Hee, J. Seong-ho, L. Yong-hoon, and C. Moon-seok, "A Secure Smart-Metering Protocol Over Power-Line Communication," *IEEE Transactions on Power Delivery*, vol. 26, pp. 2370-2379, 2011. Article (CrossRef Link)

[43] D. P. Varodayan and G. X. Gao, "Redundant Metering for Integrity with Information-Theoretic Confidentiality," *Proceeding of the First IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Gaithersburg, pp. 345-349, 2010. Article (CrossRef Link)

[44] Y. Ye, Q. Yi, and H. Sharif, "A Secure and Reliable In-network Collaborative Communication Scheme for Advanced Metering Infrastructure in Smart Grid," *Proceeding of the IEEE*

Wireless Communications and Networking Conference (WCNC), pp. 909-914, 2011. Article (CrossRef Link)

[45] S. McLaughlin, D. Podkuiko, and P. McDaniel, "Energy Theft in The Advanced Metering Infrastructure," *Critical Information Infrastructures Security - Lecture Notes in Computer Science*, vol. 6027, pp. 176-187, 2010. Article (CrossRef Link)

[46] E. Ayday and S. Rajagopal, "Secure, Intuitive and Low-cost Device Authentication for Smart Grid Networks," *Proceeding of the IEEE Consumer Communications and Networking Conference (CCNC)*, pp. 1161-1165, 2011. Article (CrossRef Link)

[47] M. G. Rahman and H. Imai, "Security in Wireless Communication," *Wireless Personal Communications*, vol. 22, pp. 213-228, 2002. Article (CrossRef Link)

[48] J. Choi, I. Shin, J. Seo, and C. Lee, "An Efficient Message Authentication for Non-repudiation of the Smart Metering Service," *Proceeding of the First ACIS/JNU International Conference on Computers, Networks, Systems and Industrial Engineering (CNSI)*, pp. 331-333, 2011. Article (CrossRef Link)

[49] H. Alzaid, E. Foo, and J. G. Nieto, "Secure Data Aggregation in Wireless Sensor Network: A Survey," *Proceeding of the Sixth Australasian Conference on Information Security (AISC '08)*, pp. 93-105, 2008.

[50] A. Perrig, J. Stankovic, and D. Wagner, "Security in Wireless Sensor Networks," *Communications of the ACM*, vol. 47, pp. 53-57, 2004. Article (CrossRef Link)

[51] J. Fadul, K. Hopkinson, C. Sheffield, J. Moore, and T. Andel, "Trust Management and Security in the Future Communication-Based "Smart" Electric Power Grid," *Proceeding of the 44th Hawaii International Conference on System Sciences (HICSS)*, pp. 1-10, 2011. Article (CrossRef Link)

[52] A. Bartoli, J. Hernandez-Serrano, M. Soriano, M. Dohler, A. Kountouris, and D. Barthel, "Secure Lossless Aggregation Over Fading and Shadowing Channels for Smart Grid M2M Networks," *IEEE Transactions on Smart Grid*, vol. 2, pp. 844-864, 2011. Article (CrossRef Link)

[53] D. R. Raymond and S. F. Midkiff, "Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses," *IEEE Pervasive Computing*, vol. 7, pp. 74-81, 2008. Article (CrossRef Link)

[54] "*Cryptographic Nonce,"* Available: http://en.wikipedia.org/wiki/Cryptographic_nonce

[55] E. Quinn, "Privacy and the New Energy Infrastructure," *University Colorado Law School - Center for Environmental and Energy Security (CEES) Available at SSRN 1370731*, pp. 1-41, 2009. Article (CrossRef Link)

[56] J. M. Bohli, C. Sorge, and O. Ugus, "A Privacy Model for Smart Metering," *Proceeding of the IEEE International Conference on Communications Workshops (ICC)*, pp. 1-5, 2010. Article (CrossRef Link)

[57] S. Brinkhaus, D. Carluccio, U. Greveler, B. Justus, D. Löhr, and C. Wegener, "Smart Hacking for Privacy," *Proceeding of the 28th Chaos Communication Congress (28C3)*, 2011.

[58] D. Gram, "*Smart Meters Raise Privacy, Health Concerns in Vt.,"* Available: http://www.boston.com/news/local/vermont/articles/2011/11/14/smart_meters_raise_privacy_health_concerns_in_vt/

[59] G. Kalogridis, F. Zhong, and S. Basutkar, "Affordable Privacy for Home Smart Meters," *Proceeding of the Ninth IEEE International Symposium on Parallel and Distributed Processing with Applications Workshops (ISPAW)*, pp. 77-84, 2011. Article (CrossRef Link)

[60] NIST, "Guidelines for Smart Grid Cyber Security: Privacy and the Smart Grid - Potential Privacy Impacts that Arise from the Collection and Use of Smart Grid Data," *National Institute of Standards and Technology (NIST)*, 2010. Article (CrossRef Link)

[61] S. Ozdemir, "Concealed Data Aggregation in Heterogeneous Sensor Networks using Privacy Homomorphism," *Proceeding of the IEEE International Conference on Pervasive Services*, pp. 165-168, 2007. Article (CrossRef Link)

[62] S. Ozdemir and Y. Xiao, "Hierarchical Concealed Data Aggregation for Wireless Sensor Networks," *Proceeding of the Embedded Systems and Communications Security Workshop in Conjunction With IEEE SRDS*, 2009.

[63] A. Molina-Markham, G. Danezis, K. Fu, P. Shenoy, and D. Irwin, "Designing Privacy-Preserving Smart Meters With Low-cost Microcontrollers," *Proceeding of the Financial Cryptography and Data Security*, pp. 239-253, 2012. Article (CrossRef Link)

Muhammad Daniel Hafiz Abdullah is a tutor at Faculty of Computer Science and Information Technology, Universiti Putra Malaysia (UPM). He obtained his Diploma (Electronic Engineering) and B.Sc (Computer Science) from UPM in 2002 and 2006 respectively. He completed his Master degree in Universiti Teknologi Malaysia (UTM) in the area of Computer Science. Currently he is pursuing his Ph.D at Universiti Putra Malaysia in Faculty of Computer Science and Information Technology. His research interests include the smart grid, wireless network security and applied cryptography.

Zurina Mohd. Hanapi received her first degree in BSc. Computer and Electronic System from the University of Strathclyde, Glasgow, UK in 1999. The author then received her master degree in MSc. Computer and Communication System Engineering from Universiti Putra Malaysia (UPM), Selangor, Malaysia in 2004 and Ph.D from the Universiti Kebangsaan Malaysia (UKM) in 2011. Currently she is a senior lecturer in the Department of Communication Technology and Network, Faculty of Computer Science and Information Technology, UPM. She had published more than 20 papers in the cited journals and conferences in the area of security and wireless sensor network. Her current research interests are on security, routing, wireless sensor network, wireless network, distributed computing, and cyber-physical-system. Dr. Hanapi is a member on Malaysian Security Committee Research (MSCR) and IEEE.

Zuriati Ahmad Zukarnain is an Associate Professor at the Faculty of Computer Science and Information Technology, University Putra Malaysia (UPM) Malaysia. She is the head for High Performance Computing Section at Institute for Mathematics and Research (INSPEM), University Putra Malaysia. She received her PhD from the University of Bradford, UK. Her research interests include: Efficient multiparty QKD protocol for classical network and cloud, load balancing in the wireless ad hoc network, quantum processor unit for quantum computer, Authentication Time of IEEE 802.15.4 with Multiple-key Protocol, Intra-domain Mobility Handling Scheme for Wireless Networks, Efficiency and Fairness for new AIMD Algorithms and a Kernel model to improve the computation speedup and workload performance. She has been actively involved as a member of the editorial board for some international peer-reviewed and cited journals. Dr. Zuriati is currently undertaking some national funded projects on QKD protocol for cloud environment as well as routing and load balancing in the wireless ad hoc networks.

M. A. Mohamed received his B.Eng in Electronic Systems Engineering, M.Sc in Computer Systems Security, and Ph.D in Mathematical Cryptography in 1997, 2003, 2011 respectively. Currently, he is a senior lecturer at the Faculty of Computer Science and Information Technology at Universiti Putra Malaysia. His research interests include cryptography and network security.