Cyber Security Issues in Smart Meter and Their Solutions

Fatemeh Halim, Salman Yussof and Mohd. Ezanee Rusli

College of Computer Science and Information Technology, Universiti Tenaga Nasional, Malaysia

Abstract
Smart meter is an essential component of a smart grid, which is the next generation power grid system. However, the use of smart meter poses many security concerns. Before smart meter can be widely deployed, these security concerns need to be identified and mitigated. This paper presents a review of cyber security issues related to a smart meter that have been identified by security researchers. The cyber security issues can be divided into three categories which are attacks on network, attacks on physical hardware and attacks on data. Solutions to some of these issues are also discussed. The paper ends with a discussion on security solutions that can be implemented to further secure a smart meter system.

Key words:
Smart meter, cyber security, security issues, security solutions.

1. Introduction

The electrical power system currently used by many companies around the world has remained almost the same way for decades. With the increase in electrical power demands, issues such as voltage sags, blackouts, and overloads have increased dramatically. Furthermore, the current electrical power system releases a lot of carbon emissions. The United States' power system alone takes up 40% of the country's carbon dioxide emissions [1]. Smart grid is the next generation of power delivery infrastructure that is expected to improve the electrical power delivery system and solve many of the current problems in power delivery. The term smart grid refers to the electricity delivery system improved with digital technology. Many nations such as the USA, Europe, Canada, China, Australia, and South Africa are now modernizing their power grids using smart grid technology. They believe that the power delivery system does not only need to be reliable, scalable, manageable, and extensible, but it also needs to be secure, interoperable, and cost-effective.

A smart grid has four main components which are advanced metering infrastructure (AMI), supervisory control and data acquisition (SCADA), plug-in hybrid vehicle (PHEV) and communication protocols and standards. Smart meter is a component of AMI, which provides accurate measurement and automate remote reading of power consumption. Some smart meters can also interface with 'smart' home appliances and control them to operate in a power-efficient manner. All these capabilities are achieved through the use of two-way communication and advanced sensors [2]. Basically, there are two main communication functions performed by smart meters [3]. The first one is to send the collected data to the utility company and to receive operational commands from operation. The second one is to exchange data with equipment that supports home energy management system (HEMS) [4]. Moreover, there are two communication media which are commonly used by smart meters to transmit data to the utility company. These two media are a radio frequency (RF) and power line carrier (PLC).

Due to smart meter data collection and communication abilities, it may become a target for malicious attackers who may benefit from stealing or manipulating the smart meter data. To protect from these malicious attackers, all communications between smart meters and utility companies need to be secured. Furthermore, software and network security mechanism should be in place to properly protect the smart meter data. On top of that, smart meters must be installed at secure locations so that they cannot be easily tampered with physically.

In this paper, cyber security issues of smart metering and their solutions are discussed. The remainder of the paper is structured as follows. In Section II, we have a closer look at the smart meter technology and the specification of a smart meter. In Section III, the various types of smart meters, security attacks are discussed. Section IV presents a number of solutions proposed by security researchers to protect smart meters from cyber-attacks. Section V concludes the paper.

2. Overview Smart Meter

Smart grid is considered as the next generation of today's power grid technology, and smart meter is one of its main components. If the power company embarks on smart grid implementation, smart meters will need to be installed at every house and premise. A smart meter can provide more accurate billing, enable the utility company to remotely connect/disconnect power to the building, monitor power usage of individual household devices, and able to report the consumption of energy to both customer and the utility company. Smart meters may also provide a termination function for utility companies to remotely terminate the

Manuscript received March 5, 2018
Manuscript revised March 20, 2018

power supply of a premise. Hence, these abilities make it an interesting target for security attackers.

2.1 Smart meter specifications

Basically, a smart meter has a network interface as well as sensors. These basic components are inside a cover that is sealed with a flag-style tamper seal to protect the meter. The meter also contains a Microcontroller Unit (MCU), which allows it to control inputs and outputs, to keep track of time and to store data in RAM, ROM, EEPROM or Flash. Through this ability to control, modify and compute data, the smart meter can run smart appliance applications [5]. The MCU also saves logs of important meter activities [6]. Smart meters additionally have an Analog Front End (AFE) that can receive analog data and convert it to digital data and pass it to the microcontroller. Smart meters are also equipped with memory component that can be in the form of a flash memory and LCD component to display data [6]. There are two smart meter standards; one is from the American National Standards Institute (ANSI) and another one by the International Electro Technical Commission (IEC). Fig. 1 shows examples of ANSI and IEC smart meters.

Fig. 1 Examples of IEC and ANSI smart meters

2.2 Benefits of smart meters:

There are many benefits of using smart meters and these benefits can be classified into three groups.

i. Benefits to the utility company

The utility company mainly benefits from the smart meter by having a much-improved billing service. Meter reading, through which the utility company knows how much to charge the customers, can now be done remotely and automatically. A smart meter does not only provide a timelier and more accurate billing service, but it also reduces cost because the company no longer needs to hire people to travel to each house and take meter reading manually. Smart meter also allows the power company to manage its operation more efficiently. It allows the overall energy usage to be monitored and this in turn enables a better control over power peak and distribution. A smart meter can also assist in troubleshooting if there is a problem and this can reduce the time required to restore power or fix a customer's problem. Finally, since the customers can also see their power consumption through the smart meter, it will make them more aware of their energy usage and indirectly this will educate the customers to better manage their energy consumption (i.e. avoid peak hour, use power-consuming appliances when the electricity price is low and etc.). If all customers can do this, the cumulative effect of this would surely benefit the utility company as well.[7,8,9,10].

ii. Benefits to consumers

The consumers mainly benefit from smart meter in terms of financial saving. Customers can know when their electricity costs more, and then they can change their respective activities to non-peak times. By changing their consumption behaviour, they can decrease their energy cost. Therefore, the customer can manage their energy consumption effectively. For example, by using smart meter, consumers may choose to switch/delay using equipment with high power consumption at peak hour to off-peak hour that has lower electricity cost. Accurate billing can also be considered as another benefit for customers because an accurate measurement can be taken remotely [7]; [8]; [9]. Therefore, consumers can get instant or daily details, which enables them to change their energy consumption if necessary. In addition, better quality of supply such as fewer power interruptions, and faster power restoration are also part of the benefits that the consumers may gain by using smart meter [10]; [11]. This is because with the use of smart meter, data gathering and minor maintenance can be done remotely without having to wait for scheduled maintenance. Therefore, many problems can be identified and resolved faster.

iii. Benefits to the government

The use of smart meter can benefit the government and the nation by contributing to a greener environment and enhances its economy. As mentioned earlier, the use of smart meter can help to reduce energy consumption. By having lower energy consumption, the CO2 emission is also subsequently reduced and this contributes to a greener environment. By increasing the awareness of consumption pattern, this can lead to of energy consumption, and it can be a good way to save energy for both consumers and the utility company [7]; [9]. Furthermore, since smart meters can be accessed remotely, utility company does not have to send staff to read the meter. This can decrease the emissions from driving and also reduce fuel consumption [10]. Another significant benefit that can be gained from a smart meter is the creation of jobs for the deployment of smart meters in terms of manufacturing, installation, and maintenance of the meters and related infrastructure such

as communication hardware and software services, information technology and business analysis [10].

2.3 Smart grid and control system architecture

A typical smart grid metering and control system, as shown in Fig. 2, contains a group of meters/sensors and controllers/actuators that interconnect with a substation/data concentrator, a client, and several third-party entities. At the metering service provider side, the central Head End System (HES) collects metering data from terminal nodes situated at the locations of the prosumers (Fig. 3). The terminal nodes include smart meters, gateways and data concentrators. The data concentrators are used to gather and forward data sent between the HES and the terminal nodes. Communication between the different entities is achieved through the use of various wired or wireless links such as PLC, DSL, WiFi, ZigBee, GSM/UMTS/LTE, or even satellite communication. A smart grid metering and control system includes a network, which gathers data and controls the transfer of electricity [12]; [13]; [14].

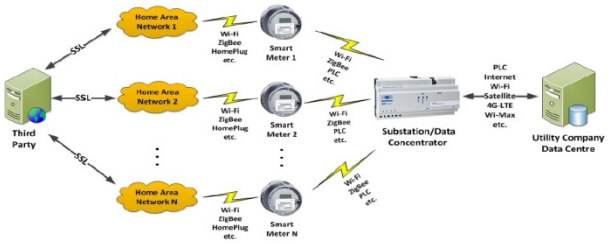

Fig. 2 Architecture of a typical smart grid metering and control system [12].

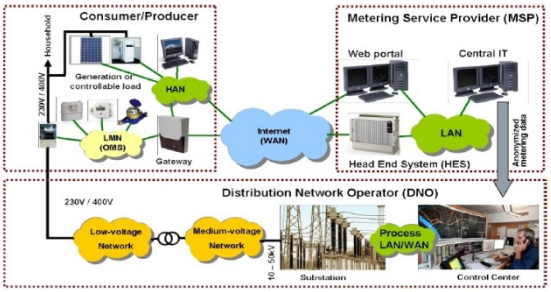

Fig. 3 Smart metering system overview [13].

3. Cyber Security Issues in Smart Meter

For a system to be considered secure, it must fulfil the four security requirements which are confidentiality, integrity, availability and non-repudiation [15]. Most security issues can undermine at least one of these security requirements. For example, an attacker may be able to masquerade as a legitimate meter data management system, and thus able to gain access to confidential information. This would also enable the attacker to change control commands, deny access to the legitimate system, and cause the system to not receive critical data [15]. The most important aspect with regard to security of smart meter is the network communication. This is because smart meters must send data to the utility company and it is important that the data do not get manipulated or tampered during transmission in smart grid [16]. Furthermore, since smart meters are connected to the smart grid, many attacks on smart grid can also affect smart meters due to this connectivity.

Security in smart meter covers both software and physical security. However, software security is more difficult to address because it cannot be physically seen or inspected. As such, security flaw in software would be difficult to detect. In many cases, a security flaw in software can only be detected once an incident occurred such as an attacker able to gain access to the smart metering system and steal data from the smart meter [17]. In order to prevent such data theft, security mechanisms such as using encryption, digital signature, firewall, access control and trusted platform need to be implemented in the software and the communication infrastructure.

There are various smart meter security issues that have been identified by researchers. These security issues can be categorized into three categories which are attacks on network, attacks on physical hardware and attacks on data. Table 1, 2 and 3 summarize existing research work on these three categories respectively. Some discussion on selected smart meter security issues are given in the sub-sections below.

3.1 Attacks on network

Two main communications media, wired and wireless can be used for data transmission between smart meters and power utility companies [18]. Low-cost infrastructure and the ease of establishing a connection in the difficult and unreachable areas are the advantages of using wireless communication. Therefore, wireless communication between smart meters and utility companies is an easier way to establish communication compared to wired communication. However, potential security problems related to networking in smart meters are mostly due to the use of wireless network. Table 1 highlights security attacks on network that can threaten smart meters, as well as their possible solutions.

ZigBee, which is based on IEEE 802.15.4, is a wireless technology commonly used in smart meter [18]. ZigBee has many security issues and vulnerabilities which can be exploited by attackers to access smart meter and its data. The most famous attack is the KillerBee attack which can

be performed on ZigBee and IEEE 802.15.4 networks. ZigBee is actually a framework and a set of tools that can be used to eavesdrop a ZigBee network, perform replay attack, attack the cryptosystems, as well as perform various other security attacks [19]. Interference or modification of network communications is also another threat on smart meter network system [20]. Attacks on network can occur when attackers compromise the gateway board by opening a network port to send malicious data, or injecting malicious codes into the memory of a smart meter [21]. The impact of this attack may be in the form of shutting down the entire grid, something that could cause downtime in the electricity supply throughout the entire system [1]. Security attacks in the network can also affect the physical equipment in the system such as by shutting down servers, damaging network components or causing the smart meter to stop working. Therefore, wireless network interface used in smart meters may potentially cause a serious security risk. WiFi is another wireless network technology commonly used in a smart metering system. Similar to ZigBee, WiFi is also prone to security risks. For example, enormous numbers of WiFi networks are completely open to sniffing [22].

Many network attacks that can be performed on a computer network can also be performed on a smart meter network. One example is the black hole attack, which is a routing attack where a malicious node advertises itself by sending a fake route reply as having the shortest path to all nodes in the environment. As a result, all traffic will be sent through this node and the node would then drop all the packets that it receives, which causes the packet to not reach the intended receivers. In smart meter network, black hole attack can be performed between an access point and a smart meter [23]. Other security attacks that can compromise the smart meter network are the Gray hole and Sybil attacks [23]. The gray hole attack is similar to the black hole attack in the sense that a malicious node attempts to get all the packets to go through it. However, it would not drop packets all the time. It can either drop packets with a certain probability, drop packets destined to only certain destination nodes or behave maliciously only for a certain time duration [24]; [25]. A gray hole attack may also behave in a manner which is a combination of the above, thus making its detection even more difficult [26]. In Sybil attack, a malicious node impersonates a large number of 102 on-existent nodes, which makes it appear as if numerous malicious nodes are conspiring together. This attack aims at subverting the reputation system used by peer-to-peer networks such as the smart metering network.

According to [27], wireless ad-hoc network is also currently used for enabling smart metering communication. Nowadays, cell phones with ad-hoc-network-enabled have been used as an instrument to display information and allow users to control appliances in their homes remotely. Hence, it is also reasonable to deploy smart meter facilities for mobile phone. Users can also access the smart meter remotely using the same concept [28]. Various research works have reported that wireless ad-hoc networks are vulnerable to various attacks such as passive eavesdropping, active interfering, impersonation, and denial-of-service [28]. Most of the time, the attacker's aim is to access metering data and privacy information. Thus eavesdropping and changing the data sent over the network have become the more popular attacks [29]. Other attacks that are commonly performed on an ad-hoc network include the black hole, gray hole, wormhole, flooding and churning attacks.

Another common way of attacking the smart meter network is to attack its routing process. Data collected by the smart meter must be transmitted to the utility company. However, this data transmission can be interrupted by various kinds of routing attacks such as altering and replaying routing data, creating routing loops, repelling traffic and producing false error messages [30].

Network attacks can also be performed by accessing network components such as Multi Utility Communication (MUC), which is the communication module in the smart meter. Once the attacker gains access illegally to a system along the communication path, he can hijack the communication between MUC and utility servers or attempt a man-in-the-middle attack such as DNS cache poisoning [31]. Another component that can be targeted is the Target of Evaluation (TOE), which is an electronic element, including hardware and software/firmware used for gathering, storing and transferring of meter data from one or more meters to one or many utility companies via the gateway [32]. Through the TOE, an attacker can try to fake internal user data or the time synchronization function [32]. The gateway is also another component that is of interest to attackers because it can reveal profile data when compromised [33].

Other security issues in smart meter can be caused by the Internet infrastructure problems such as attacks on network hardware, software or protocols [14]. An example of this would be the denial-of-service attacks (DoS) and the distributed DoS (DdoS) attacks, which are very common in the Internet. DoS/DdoS attack is also considered as a cyber-physical attack where the attack can have an effect on a physical hardware [31]. In both Denial of Service (DoS) and Distributed Denial of Service (DdoS) attacks, servers or network resources will be unavailable to users. With respect to smart meter, DoS/DdoS attacks can delay or drop sensing/control signals [34]. As the AMI is connected to the public Internet, it is vulnerable to DdoS attacks in general.

Different areas connected to the power grid may have different vulnerability to the DdoS attacks. For instance, compared with smart meters in residential homes, the AMI at a large industrial site may be well protected, physically and/or logically, by a carefully optimized demilitarized zone (DMZ) to considerably decrease the chance of success of a DdoS attack. Different neighborhoods may also be more or less vulnerable depending on their broadband connectivity, position of connecting tools, and proximity to the attacking hosts [35].

3.2 Attacks on physical hardware

Table 2 shows several cyber-physical attacks which can threaten a smart metering system. To launch a physical attack, hackers must first exploit access points in the network and then launch an attack that could cause physical harm to the system [36]. For example, attackers can send malicious data to destroy the physical system such as draining the battery or remotely connecting/disconnecting meters [37]. It is also possible for attackers to gain control over certain devices. This enables them to shut down certain appliances within a household, for instance, the refrigerator or washing machine [9]. Another type of physical attack would be to obtain sensitive information by physically tampering the smart meter. As an example, attackers can gain access to the smart meter board through the JTAG interface on the smart meter and reprogram the JTAG interface. This will cause the key components of a smart meter, including keys, privacy data and other information to be compromised [38]. Currently, the electric power control system does not have adequate measures to guarantee protection against malicious physical or cyber-attacks, which makes them highly vulnerable [34].

3.3 Attacks on data

According to [39], there are two types of data transmitted by a smart meter; one is the power consumption value of the last slot in the current slot and the other is the smart meter reading in the current slot. Smart meter data which include private information and consumers' electricity activities are collected, recorded and stored in databases. These databases may be shared with, or fall into the hands of criminals, blackmailers, corrupt law enforcer, cyber hackers of wireless communications, power company workers, and other anonymous parties who may perform malicious actions that are detrimental to the occupants of the premises where the smart meter is located.

For the duration of the last decade, countrywide deregulation has changed the electricity market in the United States from a traditionally controlled market to an economical one. Locational Marginal Prices (LMP) are usually used to control day-ahead and real-time price by numerous regional transmission organizations [40]. Some attackers can launch an attack by manipulating data from a set of meters with the goal of influencing revenues of a real-time consumption price [40]. Malicious attackers can affect real-time consumption price in two ways. One is by manipulating the meter readings which can directly affect the quantity of electricity usage. The other way is by manipulating meter readings which will affect the Locational Marginal Prices (LMP) calculation [40].

Table 3 shows several attacks on data and existing solutions to thwart such attacks. For example, ciphertext-only attack (COA) can deduce the decryption key or plaintext from the ciphertext by eavesdropping database. Another attack called the known plaintext attack (KPA) works by obtaining pairs of plaintext and the cipher text. Attackers can then gain these pairs by reading the meter and then eavesdrop the encrypted value sent by the meter. Chosen plaintext attack (CPA) can select plaintext and the corresponding ciphertext. The hacker can then control power consumption, and then eavesdrop on the encrypted value sent by the meter [17].

The most significant attacks that threaten information privacy are intrusion or modification of network communication, illegal access to stored data, masquerade or man-in-the-middle attacks and malicious software which mainly target smart meter firmware or control systems [20]. Wireless networks are also easily sniffed by attackers and may be vulnerable to Man-in-the-Middle attacks [41]. Man-in-the-middle attacks can snoop and modify data during transmission, which jeopardize data integrity [41].

Table 1: Attacks on Network

Cyber Security Attacks / Issues	Solutions / Remedial Actions
Spoofing one of the devices and sending a forged message to another device [11]. Spoof private information [42]. IP spoofing and DNS spoofing [41].	The occurrence of spoofing attack can be detected by measuring energy consumption, packet delivery ratio, node degree and link utilization [11]. For WiFi network, use TKIP (Temporal Key Integrity Protocol) for authentication [43]. Use Secure Shell (SSH) protocol for remote login [41].
Rainbow and interference attacks [42].	Novel attestation mechanism called the One-way Memory Attestation Protocol (OMAP) can detect and avoid network attacks such as Rainbow and interference attacks [42].
Attack to the gateway in smart meter to steal profile data [33].	Use GridPriv together with German BSI's Protection Profile (PP) [33].
KillerBee attacks in ZigBee and IEEE 802.15.4 networks [19].	Tools to enable network attacks detection such as open ear, ZB war drive [22].
Sniffing and injecting network traffic [22]. Sniffing on WiFi network [22].	Tools to enable network attacks detection such as open ear, ZB war drive [22].
Gray hole, Sybil attacks [23]; [19].	By creating dedicated paths between the source (smart meter) and the sink node (access point) that collects information [23].
Black hole attacks [11]; [24].	DPRAODV (Detection, Prevention, and Reactive AODV) prevents security threats of black holes by informing other nodes in the network of the attack [24]; [44]. Minimum transmission energy (MTE): route messages based on the the energy of the transmitters which can detect black hole, spoofing and selective forwarding attacks [11].
Eavesdropping of private information [43].	Encrypt data before transmission using encryption standard such as AES [43].
TCP/IP attacks [43].	Use Secure Sockets Layer (SSL)/Transport Layer Security (TLS) for Internet communication [43].
Privacy attacks to metering data launched from the network [29].	Use anonymity services to help protect privacy. For example, smart metering data can be separated into low frequency attributable data (data used for billing) and high frequency anonymous technical data (data used for demand side management) [12]. Secure escrow protocol to securely anonymize the ID of frequent metering data sent by a smart meter [12].
DoS and DDoS attacks [31]; [1].	Anomaly detection, network supervision and active management of Internet connection [31]. Adopt TCP/IP, VPN (IPsec), SSH, SSL/TLS [1]. Intrusion detection and firewalls [1]. For WiFi network, use TKIP (Temporal Key Integrity Protocol) for authentication [43].
Network attacks in wireless ad-hoc network [45].	Multiple certificate authorities (CAs) distributed over the network, each with a periodically updated share of the private key [45].

Table 2: Attacks on Physical Hardware

Cyber Security Attacks / Issues	Solutions / Remedial Actions
Local cyber-physical attacks at a smart metering location, for example, manipulating the measured energy consumption [46].	An embedded real-time anomaly detector that can cover both the cyber and physical domains [46].
Cyber-physical attacks on the smart grid [20].	Model the attacks using Petri nets for analysis [20].
Functions like remote connect/disconnect meters and outage reporting may be used by unwarranted third parties [1].	Secure meter maintenance [1]. Delete unauthorized changes on meter [1]. Authorize all accesses to/from AMI networks [1].
Physical attacks such as battery change, removal, and modification [1].	Secure meter maintenance [1].
Injecting malicious codes into the memory of a smart meter [42].	OMAP (One-Way Memory Attestation Protocol) can detect memory modification attacks due to malicious code injection [42].

Table 3: Attacks on Data

Cyber Security Attacks / Issues	Solutions / Remedial Actions
Manipulated data [40].	Implement security index to detect manipulated data [40].
False data injection (FDI) [47] which results in a lower energy consumption reading for the attacker and a higher reading for the others in a neighborhood.	Use a hybrid IDS (Instruction Detection System) to detect FDI [47].
Checksum forgery attack, which attempts to compute a checksum on the memory before the smart meter sends the checksum [42].	Attestation mechanisms to detect checksum forgery attack [42].
Cyber-attacks in control and commands, and bulk data [41].	Use asymmetric key cryptography such as elliptic curve digital signature algorithm (ECDSA) to encrypt any control/commands like remote disconnect/connect and real-time pricing changes [41].
Parallel checksum computation attack, which attempts to speed up checksum computation in order to perform another illegal operation during extra time [42].	Attestation mechanisms to detect parallel checksum computation attack [42]. Force sequential execution in checksum computation. [42].
Privacy problem such as illegal access to stored data, masquerade or man-in-the-middle attacks and malicious software [20].	Using a trusted third party (TTP) to protect privacy of smart meter [48]. Multi-resolution wavelet delegation method using multiple keys to encrypt [49]. Data can be stored in an LDAP drive identity management solution [50]. Using homomorphic encryption can corroborate smart meter data privacy [12]. Use Shamir Secret Sharing (SSS) to protect data privacy [51]. Use encryption scheme such as AES or Rabin [43]; [41]; [38].
Eavesdropping of messages sent by smart meter using known plaintext attack (KPA), chosen plaintext attack (CPA) and ciphertext only attack (COA) [17].	Use SSMP (Secure Smart Metering Protocol) which uses four cryptographic protocols with multiple keys to prevent eavesdropping [17].

4. Mitigating Cyber Security Attacks In Smart Meters

In this section, possible solutions or remedial actions to the security attacks described in the previous section will be presented. Similar to the security attacks, the solutions will also be categorized into three categories.

4.1 Mitigations for attacks on network

Communication performed by smart meters must use secure protocols such as IPSec (Internet Protocol Security), SSL (Secure Socket Layer) /TLS (Transport Layer Security) and SSH (Secure Shell), encryption, firewalls, user access control mechanisms, and secure physical locations to avoid unauthorized tampering or penetration [1 ; 32; 52]. IPsec protocol uses encryption technology to provide data confidentiality, integrity, and authenticity between all nodes in a network communication. Another protocol that can also be used to protect data across a network is C12.22 standards for protocol specification for interfacing to data communication networks (communicating smart metering data across a network) [12]. There are also attestation mechanisms such as one-way memory attestation protocol (OMAP) which can detect attacks and prevent network attacks such as rainbow and interference attacks [42].

Different neighbourhoods can also be more or less vulnerable depending on their broadband connectivity, the status of connecting equipment and proximity to attacker sites. The DdoS attack can be mitigated in different ways depending on its specific form. For example, flooding attacks can be mitigated by router throttling, while low-rate TCP attacks can be mitigated by monitoring for the periodic attack signatures and concomitant filtering of flagged traffic. These abilities can also be used to allow only trusted and authorized traffic into the network [35].

In the communication network, one of the most important components is the gateway. The gateway security is always a concern and therefore a reliable gateway time is necessary. To achieve a reliable gateway time and avoid, detect, or mitigate attacks on a gateway' time, the Germany BST's protection profile (PP) can be used for the gateway of a smart metering system [33]. The smart meter gateway (SMGW) can support intrusion prevention systems (IPS) and packet filtering (Firewall) which can monitor and filter the network traffic [53]. TOE is another security module proposed to be used by the gateway where it can function as a cryptographic provider [32].

4.2 Mitigations for attacks on physical hardware

Attacks to physical hardware can come in various forms such as tampering of the smart meter equipment or an attack that can damage smart meter equipment. [47] Proposed a CONSUMER attack model that is designed to detect the attack of equipment on the consumer's side. Other methods include the use of location-based keys and employing a cryptographic related method to avoid malicious node attacks [47]. [52] Proposed a solution for high voltage/frequency tampers. For instance, ferrite beats, capacitor line filters and physically large SMD resistors, electrostatic devices can produce spikes/voltages in the range of 35KV. The smart meter ASIC should have highly tolerant I/Os. Some board design methods such as using ferrite beads, capacitor line filters, and physically large SMD resistors can help to defend the meter electronics from numerous forms of electromagnetic charges.

An important part of a smart meter is the real time clock (RTC) and there are security attacks that try to access the RTC to change the real time. One way to do this is by sending malicious codes. To prevent malicious codes from changing the real time clock (RTC) settings, locked registers can be used where they need to be unlocked before they can be written [52].

An embedded anomaly detection model can also secure cyber and physical domains in smart meters [46]. For example, one solution for cyber-physical attacks is the clustering-based anomaly detection algorithm [46]. Another solution is embedded real-time anomaly detector which can cover both the cyber and physical domains [46]. It has been shown that the algorithm is able to efficiently detect numerous kinds of attacks without emitting any false positive [46].

[54] Presented the rat-group attack which exploits the weaknesses of smart meters in the cyber world but spreads the attack to the physical world to obtain direct economic profits. Game theory is then applied to analyse this attack. The analysis results suggest that the power company should follow an open protection policy, such as disclosing the defence parameters for all users (the potential attackers), which results in less loss in the attack.

4.3 Mitigations for attacks on data

Personal data in all forms must be protected from unauthorized occupation, copying, disclosure, access, use, loss or theft [1]. One way to protect important data is by limiting access. Meaning that, only authorized people can have access to data resources [55] Smart meter records fine-grained consumption profile of electricity and report it to the utility company who bills the consumer consequently. It is of utmost important that this consumption profile data does not leak to those who are not supposed to see them. A novel data checking technique which is based on holomorphic encryption can be a good solution to protect privacy information [39].

Multi-resolution wavelet delegation can be a method to secure smart meter privacy database against attacks, by using multiple keys to encrypt the data [49]. Intrusion detection system (IDS) and remote attestation are two mechanisms which are used to protect the privacy of customers [6]. A trusted third party (TTP) can be used to protect the privacy as well [48]. For example, smart meter sends their data using some form of encrypted communication to the TTP. The power company would then obtain the data that they require, which is normally in the form of aggregated data, from the TTP. According to [12], in Europe, the European Commission recommends using anonymity services to help protect privacy. For example, smart metering data can be divided into low-frequency attribute-able data (data used for billing) and high frequency anonymous technical data (data used for demand-side management). In this case, the main challenge resides in anonymizing the high-frequency data, which are required for efficient grid functionalities, while making sure that the reliability, the effectiveness and the security of these functionalities are not compromised.

Privacy can also be compromised by the attacker monitoring the power usage of a building. To prevent this, a technique using battery can be employed. When batteries charge and discharge, this technique can control and avoid the detection of appliance power signatures using sophisticated algorithms for Non-Intrusive Load Monitoring (NILM) [56]. More recently, a new technique called Combined Heat and Privacy (CHPr) which uses frame thermal, rather than chemical energy storage, can make it look like someone is always at home. This technique uses a partial demand flattening to eliminate a large majority of power variations [56].

Shamir Secret Sharing (SSS) is a method in cryptography for distributing a secret between groups of participants. When a secret is encrypted using SSS, the secret can only be reconstructed when the shares are combined together. Individual shares are of no use on their own. Therefore, the SSS scheme is appropriate to perform privacy-preserving collection of smart meter data [51].

With regard to data privacy, much could be possible just by giving careful attention to the stream of information through a business, and careful attention to how it is utilized. For example, if client data is stored in an LDAP-driven identity management solution, then the use of virtual directory solutions instead of replicating the entire LDAP source will offer the chance to limit the data that is approved over to the applications and users that consume

customer data. With this, the underlying OMC data is stored in one place, and the users of the data are stored in another place. Another advantage of this solution is that only the data for the consumers who are being managed at that time is accessible instead of having data about all clients available at all times [50].

Some attacks in database happen because of encryption or authentication control/commands vulnerabilities. Encryption and authentication are critical cryptographic methods for a smart grid to protect data integrity and confidentiality [57]. Asymmetric key cryptography such as elliptic curve digital signature algorithm (ECDSA) can be used to encrypt any control/commands like remote disconnect/connect and real-time pricing changes [43;52]. In addition, revocation management can be used to handle strong authentication of devices and data [22]. All security protocols need one cryptography method to encrypt the data [41]. Encryption structures can be based on symmetric key cryptography like AES, DES or asymmetric key cryptography such as RSA [57]. 128-bit AES cipher is common in smart metering and is frequently used in the communication between smart meters and collection units. Since the data is encrypted, this prevents eavesdropping [43;52]. In the same fashion, using key exchanges based on Elliptic Curve Cryptography (ECC) can offer a high level of security [41]. Another method that can be used to secure smart meter network is the Secure Smart Metering protocol (SSMP) which relies on the security of its four cryptographic protocols to securely produce keys for each network device and issue key sharing between network devices [17].

5. Conclusion

This paper presents an overview of cyber security issues that can occur in smart meter deployment. We categorized the smart meter security issues into three categories which are attacks on network, attacks on physical hardware and attacks on data. For each category, a number of security issues and attacks that have been identified by security researchers were discussed. This is followed by the discussion on the mitigation techniques proposed by researchers to prevent or mitigate the security attacks highlighted. Even though many mitigation techniques have been proposed, not all the security issues or attacks are addressed. Further research works are still needed to further improve the state of security of smart metering system.

References

[1] Liu, J., Y. Xiao, S. Li, W. Liang, C.L.P Chen," Cyber security and privacy issues in smart grids," IEEE Communications Surveys & Tutorials, 14(4): 981 – 997, 2012.

[2] Barenghi, A., Breveglieri, L., Fugini, M., & Pelosi, G, Smart Power Grids Security," Smart Meters and Home Gateway Scenarios," Proceeding of the IX Conference of the Italian Chapter of AIS, 2013.

[3] Mohassel, R.R., A. Fung, F. Mohammadi, K. Raahemifar, "A survey on advanced metering infrastructure. International Journal of Electrical Power & Energy Systems," 63: 473 – 484, 2014.

[4] Isamu, K., and S. Sekiguchi, 2013. Technologies Supporting Smart Meter Networks. FUJITSU Sci. Tech. J, 49(3): 307-312.

[5] Elmenreich, W., and D. Egarter," Design guidelines for smart appliances," Proceeding of the Tenth Workshop on Intelligent Solutions in Embedded Systems (WISES), pp: 76 – 82, 2012.

[6] Molazem, F," Security and Privacy of Smart Meters: A Survey," 2012. [Online]. Available: http://blogs.ubc.ca/computersecurity/files/2012/04/FMolazem_SurveyFaridMolazem.pdf. [Accessed: April-2012]

[7] Zheng, J., D.W. Gao, L. Lin," Smart meters in smart grid: An overview," Proceeding of IEEE Green Technologies Conference, pp: 57 – 64, 2013.

[8] Benzi, F., N. Anglagi, E. Bassi, L. Frosini," Electricity smart meters interfacing the households," IEEE Transactions on Industrial Electronics, 58(10): 4487 – 4494, 2011.

[9] Elmaghraby and Losavio, Elmaghraby, A.S. and M.M Losavio," Cyber security challenges in smart cities: safety," security and privacy. Journal of Advanced Research, 5(4): 491 – 497, 2014.

[10] Doris and Peterson, Doris, E. and K. Peterson,"Government Program Briefing: Smart Metering," National Renewable Energy Laboratory, 2011 [Online]. Available : http://www.nrel.gov/docs/fy11osti/52788.pdf

[11] Kaplantzis, S. and Y.A. Sekercioglu," Security and smart metering," Proceeding of the 18th European Wireless Conference (EW), pp: 1 – 8, 2012.

[12] Fan and Gong, Z., P. Kulkarni, S. Gormus, C. Efthymiou, G. Kalogridis, M. Sooriyabandara, Z. Zhu, S. Lambotharan, W.H. Chin," Smart grid communications: Overview of research challenges, solutions, and standardization activities," IEEE Communications Surveys & Tutorials, 15(1): 21 –38, 2013.

[13] Von Oheimb, D," IT Security architecture approaches for Smart Metering and Smart Grid. Smart Grid Security," 7823: 1 – 25,2013..

[14] Fróes Lima and Portillo Navas; Fróes Lima, C.A. and J.R. Portillo Navas. "Smart metering and systems to support a conscious use of water and electricity energy. Energy, "45(1): 528 – 540, 2012.

[15] Cleveland, Cleveland, F.M., " Cyber security issues for advanced metering infrastructure (AMI)," Proceeding of IEEE Power and Energy Society General Meeting – Conversion and Delivery of Electrical Energy in the 21st Century, pp: 1 – 5, 2008.

[16] Depuru, S.S.S.R., L. Wang, V. Devabhaktuni," Smart meters for power grid: Challenges, issues, advantages and status," Proceeding of IEEE/PES Power Systems Conference and Exposition (PSCE), pp: 1 – 7, 2011.
[17] Kim et al, Kim, S., E.Y. Kwon, M. Kim, J.H. Cheon, S.H. Ju, Y.H. Lim, M.S. Choi, "A secure smart-metering protocol over power-line communication," IEEE Transactions in Power Delivery, 26(4): 2370 – 2379, 2011.
[18] Vehbi et al, Gungor, Vehbi C., Dilan Sahin, Taskin Kocak, Salih Ergut, Concettina Buccella, Carlo Cecati, and Gerhard P. Hancke, "Smart grid technologies," Communication technologies and standards." IEEE transactions on Industrial informatics 7, no. 4 (2011): 529-539, 2011.
[19] Stelte and Rodosek, Stelte, B., and G.D Rodosek," Thwarting attacks on ZigBee-Removal of the KillerBee stinger," Proceeding of the 9th International Conference on Network and Service Management (CNSM), pp: 219 – 226, 2013.
[20] Chen, T.-M, J.C. Sanchez-Aarnoutse, J. Buford," Petri net modeling of cyber-physical attacks on smart grid," IEEE Transactions on Smart Grid, 2(4): 741 – 749, 2011.
[21] Vigo, R., E. Yuksel, C.D.P.K Ramli," Smart Grid Security A Smart Meter-Centric Perspective," Proceeding of the 20th Telecommunications Forum (TELFOR), pp: 127 – 130, 2012.
[22] Travis, G.S, S. Bratus, R. Melgares, R. Speers, and S. W. Smith," Api-do: Tools for exploring the wireless attack surface in smart meters," Proceeding in System Science (HICSS), 45th Hawaii International Conference on, pp. 2133-2140, 2012.
[23] Bennett, C., and S.B. Wicker," Decreased time delay and security enhancement recommendations for AMI smart meter networks," Proceeding of Innovative Smart Grid Technologies (ISGT), pp: 1– 6, 2011.
[24] Payal and Swadas, Raj, Payal N., and Prashant B. Swadas, "Dpraodv: A dyanamic learning system against blackhole attack in aodv based manet," arXiv preprint arXiv:0909.2371 , 2009.
[25] Saravanan et al, Jaisankar, N., R. Saravanan, K.D. Swamy,"A novel security approach for detecting black hole attack in MANET," Information Processing and Management. 70: 217 – 223, 2010.
[26] Jawandhiya, P.M., M.M. Ghonge, M.S. Ali, J.S. Deshpande," A survey of mobile ad hoc network attacks," International Journal of Engineering Science and Technology, 2(9): 4063 –4071, 2010.
[27] Farooq and Jung, Farooq, H. and Low Tang Jung," Performance analysis of ad-hoc routing protocols in smart metering infrastructure," Proceeding of IEEE Science and Information Conference (SAI), pp: 871 – 874, 2013.
[28] Dusit, N., L. Xiao, P. Wang," Machine-to-machine communications for home energy management system in smart grid," IEEE Communications Magazine, 49(4): 53 – 59, 2011.
[29] Saed, M., N. Al Holou, K. Daimi," Centralized Smart Meter-to-Collector Communications Security," Proceeding of the International Conference on Digital Security and Forensics (DigitalSec2014), pp: 8 – 14, 2014.
[30] Fenjun, L., Bo Luo, Peng Liu," 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.
[31] Chinnow, J., K. Bsufka, A.D. Schmidt, R. Bye, A. Camtepe, S. Albayrak," A simulation framework for smart meter security evaluation," Proceeding of IEEE International Conference on Smart Measurements for Future Grids (SMFG), pp: 1 – 9,2011.
[32] Kreutzmann, H., S. Vollmer, N. Tekampe, A. Abromeit," Protection profile for the gateway of a smart metering system. German Federal Office for Information Security," Tech. Rep, 2011.
[33] Stegelmann, M., & Kesdogan, D," Gridpriv: A smart metering architecture offering k-anonymity," In Trust, Security and Privacy in Computing and Communications (TrustCom) IEEE 11th International Conference on (pp. 419-426). IEEE, 2012.
[34] Govindarasu, M., A. Hann, P. Sauer," Cyber-physical systems security for smart grid. Future Grid Initiative White Paper," PSERC (Power System Engineering Research Center) publication, 2012.
[35] Ma, C.Y.T., D.K.Y. Yau, N.S.V. Rao," Scalable solutions of markov games for smart-grid infrastructure protection," IEEE Transactions on Smart Grid, 4(1): 47 – 55, 2013.
[36] Kantarci, M.E. and H.T. Mouftah," Management of PHEV batteries in the smart grid: Towards a cyber-physical power infrastructure," Proceeding of the 7th International Conference of Wireless Communications and Mobile Computing Conference (IWCMC), pp: 795 – 800, 2011.
[37] Al Abdulkarim, L. and Z. Lukszo," Information security assurance in critical infrastructures: Smart metering case," Proceeding of First International Conference Infrastructure Systems and Services: Building Networks for a Brighter Future (INFRA), pp: 1 – 6, 2008.
[38] Yaghmaee, M.H., Q.A. Frugh, M. Bahekmat," Monitoring approach for detection compromise attacks in smart meter," Proceeding of 22nd International Conference and Exhibition on Electricity Distribution (CIRED), pp: 1 – 4, 2013.
[39] Yukun, N., T. Xiaobin, C. Shi, Y. Kai, B. Zhiyong," A security, privacy protection scheme for data collection of smart meters based on homomorphic encryption. IEEE EUROCON," pp: 1401 – 1405, 2013.
[40] Jia, L., R.J. Thomas, L. Tong," Malicious data attack on real-time electricity market," Proceeding of IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp: 5952 – 5955, 2011.
[41] M. Arora, "Advanced Metering: Ecosystem, Security threats and Counter measures," Freescale Semiconductor, 2013. [Online]. Available: https://aroramohit.com/articles/2016/2/15/advanced-metering-ecosystem-security-threats-and-counter-measures
[42] Song, K., D. Seo, H. Park, H. Lee, A. Perrig,"OMAP: One-way memory attestation protocol for smart meters," Proceeding of the Ninth IEEE International Symposium on Parallel and Distributed Processing with Applications Workshops (ISPAW), pp: 111 – 118,2011.
[43] Ghansah, I, "Smart Grid information assurance and security technology assessment," California energy commission, 2010. [Online]. Available: http://www.energy.ca.gov/2013publications/CEC-500-

2013-056/CEC-500-2013-056.pdf. [Accessed: December-2010]
[44] Jaisankar, N., R. Saravanan, K.D. Swamy, "A novel security approach for detecting black hole attack in MANET," Information Processing and Management. 70: 217 – 223,2010..
[45] Alomari, A," Implementing Rsa Algorithm For Fully Distributed Certificate Authority In Manet," Journal of Information Systems & Operations Management, 7(1) , 2013.
[46] Raciti, M. and S. Nadjm-Tehrani," Embedded cyber-physical anomaly detection in smart meters. Critical Information Infrastructures Security, 7722: 34 – 45, 2013.
[47] Chun, L., and N. Ansari," CONSUMER: A Novel Hybrid Intrusion Detection System for Distribution Networks in Smart Grid," IEEE Transactions on Emerging Topics in Computing, 1(1): 33 – 44, 2013.
[48] Bohli, J.-M, C. Sorge, and O. Ugus," A privacy model for smart metering," Proceeding of IEEE International Conference on Communications Workshops (ICC), pp: 1– 5, 2010.
[49] Engel, D," Wavelet-based load profile representation for smart meter privacy," Proceeding of the IEEE PES Innovative Smart Grid Technologies (ISGT), pp: 1-6, 2013.
[50] Shein, R, "March. Security measures for advanced metering infrastructure components," In 2010 Asia-Pacific Power and Energy Engineering Conference, 2010.
[51] Rottondi, C., Verticale, G., & Kraus, C," Secure distributed data aggregation in the automatic metering infrastructure of smart grids," In Communications (ICC), IEEE International Conference on (pp. 4466-4471). IEEE, 2013, June.
[52] M. Arora,' Advanced Metering: Security threats, Challenges and Counter measures', Freescale Semiconductor, 2010. [Online]. Available: https://aroramohit.com/articles/2016/2/15/advanced-metering-security-threats-challenges-and-counter-measures
[53] Sikora, A," Implementation of Standardized Secure Smart Meter Communication," Proceeding of the 35th International Telecommunications Energy Conference 'Smart Power and Efficiency' (INTELEC), pp: 1 – 5, 2013.
[54] Shange, Ming, Jingqiang Lin, Xiaokun Zhang, and Changwei Xu, "A game-theory analysis of the rat-group attack in smart grids," In Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 2014 IEEE Ninth International Conference on, pp. 1-6. IEEE, 2014.
[55] Shahinzadeh, H., and A. Hasanalizadeh-Khosroshahi," Implementation of Smart Metering Systems: Challenges and Solutions," TELKOMNIKA Indonesian Journal of Electrical Engineering, 12(7): 5104 – 5109, 2014.
[56] Dong, C., D. Irwin, P. Shenoy, J. Albrecht," Combined heat and privacy: Preventing occupancy detection from smart meters," Proceeding of IEEE International Conference Pervasive Computing and Communications (PerCom), pp: 208 – 215, 2014.
[57] Wang, W., and Z. Lu," Cyber security in the smart grid: Survey and challenges," Computer Networks, 57(5): 1344 – 1371, 2013.

Fatemeh Halim is a Master student in field Security networking computer in UNITEN university in Malaysia in departments of Information Technology, 6 years experiences about networking computer and Cisco (CCNA, CCNP).

Salman Yussof is an Associate Professor at the College of Information Technology, Universiti Tenaga Nasional, Kajang, Malaysia. He received his Bachelor of Science degree and Masters of Science degree in Electrical and Computer Engineering from Carnegie Mellon University, USA, in 1999. In the same year, he was accepted as a faculty member at the College of Information Technology, Universiti Tenaga Nasional. While working as a faculty member, he pursued his PhD study in the same university and eventually received his PhD in 2010. His research interests include next generation Internet technologies, network security and security for critical infrastructure. He is a member of IEEE.

Mohd Ezanee Rusli is a Senior Lecturer at the College of Information Technology, Universiti Tenaga Nasional, Kajang, Malaysia. He received his PhD Degree in 2012 from Massey University, NZ, MSc in 2002 from UMIST, UK and BSc from Southampton University in 1999. His research interests are embedded system, networking, image processing and wireless network. He is a member of IEEE and ACM