# Smart Grid Metering Networks: A Survey on Security, Privacy and Open Research Issues

Pardeep Kumar *Member, IEEE* , Yun Lin *Member, IEEE*, Guangdong Bai, Andrew Paverd *Member, IEEE*, Jin Song Dong, and Andrew Martin *Member, IEEE*

***Abstract*— Smart grid (SG) networks are newly upgraded networks of connected objects that greatly improve reliability, efficiency and sustainability of the traditional energy infrastructure. In this respect, the smart metering infrastructure (SMI) plays an important role in controlling, monitoring and managing multiple domains in the SG. Despite the salient features of SMI, security and privacy issues have been under debate because of the large number of heterogeneous devices that are anticipated to be coordinated through public communication networks. This survey paper shows a brief overview of real cyber attack incidents in traditional energy networks and those targeting the smart metering network. Specifically, we present a threat taxonomy considering: (i) threats in system-level security, (ii) threats and/or theft of services, and (iii) threats to privacy. Based on the presented threats, we derive a set of security and privacy requirements for SG metering networks. Furthermore, we discuss various schemes that have been proposed to address these threats, considering the pros and cons of each. Finally, we investigate the open research issues to shed new light on future research directions in smart grid metering networks.**

***Index Terms*—Smart grid communications, smart metering, security, privacy, research directions.**

## I. Introduction

SMART grid (SG) networks are envisioned to be the next evolutionary step of power supply networks [1]. These networks typically include several advancements that will improve the efficiency and reliability and provide uninterrupted energy supply to homes and businesses. In addition, SG also includes various renewable energy sources (e.g., solar, wind, etc.), distributed generation (DG) and distributed storage (DS) [2]–[6]. As shown by market research [7], the SG market is projected to grow $20.83 billion in 2017 to $50.65 billion by 2022. This market shift has therefore generated significant interest from governments, industries and academia. The main abbreviations are summarized in Table I.

SG networks consist of different domains, including (i) bulk generation, (ii) energy transmission, (iii) energy distribution, (iv) customers, (v) operation, (vi) market and (vii) service provider, as shown in Fig. 1. The upper domains, i.e., bulk generation, energy transmission, energy distribution and customer are primarily connected by two-way energy flow (illustrated with black solid lines). These upper domains are managed and controlled by the underlying domains, i.e., operation, market and service provider, via two-way information flow (illustrated with red dotted lines) [8]. This two-way flow of energy and data will enable new functionality between the consumers and utilities in the SG.

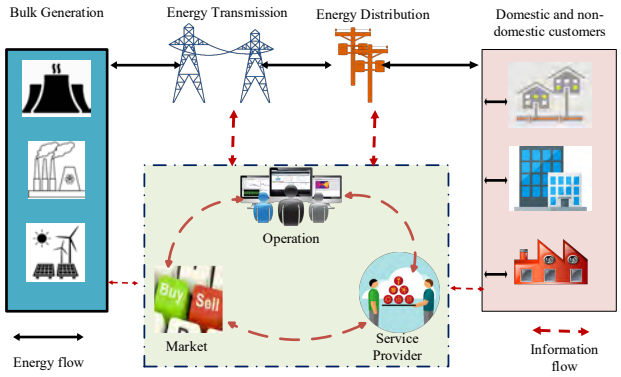


Fig. 1. A high-level conceptual model of the SG [8] [9] [10].

To realise the aforementioned domains, one of the main infrastructures is smart metering that will not only help to evaluate the status of a power grid but also to manage those distributed resources. It is anticipated that a large number of heterogeneous devices (e.g., smart meters, sensors, etc.) will be deployed between consuming points and monitoring and controlling centers [11]–[13]. The term smart metering system defines an intelligent electronic device that measures energy usage data, with more precise information than a traditional meter, and sends and receives data via two-way communication [14]. As a result, smart metering networks equipped with the information and communication technology (ICT [15]), and working together with intelligent sensors allow utility companies to manage and control the SG. Despite the control and management capabilities of smart metering, the collected metering data can be used by automated and intelligent systems to enable new applications. These applications may include load management programs, DG and DS control systems and billing [13], [16], [17].

However, the mass dependence on ICT and smart metering network technologies also open up several threat surfaces, especially when the utility companies integrate several automated applications. A report published by the United States Computer Emergency Readiness Team (US-CERT) warns that

P. Kumar is with the Department of Computer Science, Swansea University, Swansea, United Kingdom, (email:pardeep.kumar@swansea.ac.uk)

Y. Lin is with the School of Computing, National University of Singapore, Singapore, (email:llmhyy@gmail.com)

G. Bai is with the School of Information and Communication Technology, and the Institute for Integrated and Intelligent Systems, Griffith University, Australia, (email: g.bai@griffith.edu.au)

A. Parerd is the Microsoft Security Response Centre, Microsoft Research Cambridge, United Kingdom, (email: andrew.paverd@ieee.org)

J.S. Dong is with the School of Computing, National University of Singapore, Singapore, (email: dcsdjs@nus.edu.sg)

A. Martin is with the University of Oxford, Oxford, United Kingdom, (email: andrew.martin@cs.ox.ac.uk)

the advanced persistent threat activities are targeting energy sectors [18]. Recent studies reveal that the energy companies can be predominantly subjected to targeted attacks [19], [20]. A targeted attack on the SG metering network could potentially lead to slowdown or shutdown of the power grid systems, and cripple the utility delivery systems. Exploitation of vulnerabilities in the SG metering network could affect individual consumers, as well as infrastructure such as substations and control centers [21]. Moreover, a threat is not only limited to the SG metering network security but it can raise many privacy issues for end-customers. For instance, a smart meter usually sends energy reports every 15/30 minutes periodically over wireless communication. An eavesdropper can intercept such reports to invade the privacy of consumers, for example, what time the property is occupied or empty [22] [23]. As a result, the individuals' private life patterns can be inferred or can be used for criminal purposes.

Following the aforementioned issues, security and privacy issues recently have been the subject of extensive research because the public safety, and the national economy and security are rely heavily on the energy networks. Although security and privacy weaknesses are continuously being discovered in the network technologies, protocols, and devices used in the energy systems, the significance of threats to system level security, threats or theft via services, and threats to privacy are not always fully understood in SG metering networks. In the following subsection, we discuss recent survey papers in this field, and point out the distinguishing features and main contributions of our work.

### *A. Existing Work*

Recently, several survey papers have been conducted on the security and privacy issues in SG domain, as follows.

**Security:** In 2013, Wang-Lu analyzed security challenges in the SG network, including transmission and distribution subsystems, AMIs, and HANs [24]. The authors presented the security requirements and thoroughly evaluated network threats with case studies. Moreover, the research mainly considered cryptographic countermeasures including authentication and key management in various SG domains. This paper includes detailed analytical analysis including several traditional protocols (e.g., distributed network protocol) in the energy domains. Nevertheless, since 2013, extensive novel and advanced security methods have been published and those need to be explored.

In 2014, Komninos et al. presented smart grid and smart home security [21]. The authors mainly considered the interaction between the smart home and SG environments, and classified their security risks. The paper discussed some representative threats and evaluated theoretical impacts from smart home to smart grid and vice versa. The authors provided a survey of the available literature as the security countermeasures and included the SG's ongoing activities over the period of 2009 – 2013. Though, Komninos et al. reviewed several papers from the viewpoint of security countermeasures including privacy, the critical analysis of these schemes (if any) were not discussed.

TABLE I
ABBREVIATIONS AND DESCRIPTIONS

| **Abbreviation** | **Description** |
|---|---|
| ARP | Address Resolution Protocol |
| AES | Advanced Encryption Standard |
| AMI | Advanced Metering Infrastructure |
| ABE | Attribute-Based Encryption |
| AVISPA | Automated Verification of Internet Security Protocols and Applications |
| BOC | Back Office Compromise |
| CR | Cognitive Radio |
| CIA | Confidentiality, Integrity and Availability |
| CI | Critical Infrastructure |
| DCU | Data Collector Unit |
| DPI | Deep Packet Inspection |
| DoS | Denial of Service |
| DNO | Distribution Network Operator |
| DSS | Distribution Sub-Station |
| DR, DRAS | Demand Response, and Automation Server |
| DG, DS | Distributed Generation, and Distributed Sources |
| DSR | Dynamic Source Routing |
| ECC | Elliptic Curve Cryptography |
| ECDSA | Elliptic Curve Digital Signature Algorithm |
| FHE | Full Homomorphic Encryption |
| HVE | Hidden Vector Encryption |
| HAN | Home Area Network |
| HEMS | Home Energy Management System |
| HMI | Human Machine Interfaces |
| HWMP | Hybrid Wireless Mesh-Routing Protocol |
| IBC | Identity-Based Cryptography |
| ICS | Industrial Control System |
| ICT | Information and Communication Technology |
| IED | Intelligent Electronic Device |
| IoT | Internet of Things |
| KDS | Key Distribution Server |
| LTE | Long-Term Evolution |
| MPS | Main Power Supply |
| MAC | Medium Access Control |
| MDMS | Meter Data Management System |
| MITM | Man-In-The-Middle |
| NAN | neighbourhood area network |
| OIP | Optimal Inspection Point |
| PREP | Path Reply |
| PMU | Phasor Measurement Unit |
| PHEV | Plug-in Hybrid Electric Vehicles |
| PREQ | Proactive Path Request |
| PUF | Physically Unclonable Function |
| PLC | PowerLine Communication |
| PKI | Public Key Infrastructure |
| RFID | Radio Frequency Identification |
| RTU | Remote Terminal Units |
| SG, SM | Smart Grid and Smart meter |
| SMI | Smart Metering Infrastructure |
| SCADA | Supervisory Control And Data Acquisition |
| SVM | Support Vector Machine |
| TLS | Transport Layer Security |
| TTP, TRE | Trusted Third Party, and Remote Entity |
| TPM, TU | Trusted Platform Module, Transmission Unit |
| US-CERT | United State Computer Emergency Readiness Team |
| VPN | Virtual Private Network |
| WSN | Wireless Sensor Network |

TABLE II
COMPARISON WITH OTHER SURVEYS

| | Security issue | Privacy issue | Real attack incidents | Threat-I | Threat-II | Threat-III | Pros of countermeasures | Cons of countermeasures | Paper covered |
|---|---|---|---|---|---|---|---|---|---|
| [24] | √ | ND | ND | √ | ND | ND | √ | ND | 2008–2012 |
| [21] | √ | √ | ND | √ | LD | LD | √ | ND | 2010–2014 |
| [25] | √ | √ | ND | LD | LD | LD | √ | ND | 2010–2016 |
| [2] | ND | ND | ND | ND | ND | ND | ND | ND | 2008–2015 |
| [26] | √ | ND | ND | √ | ND | ND | √ | ND | 2009–2016 |
| [23] | | √ | ND | LD | LD | √ | √ | √ | 2007–2014 |
| [27] | ND | √ | ND | ND | ND | LD | √ | ND | 2008–2015 |
| [28] | √ | √ | ND | LD | LD | LD | √ | ND | 2007–2014 |
| [29] | LD | LD | ND | LD | ND | LD | √ | ND | 2010–2015 |
| [17] | LD | LD | ND | LD | LD | LD | LD | ND | 2010–2018 |
| Ours | √ | √ | √ | √ | √ | √ | √ | √ | 2010–2018 |

Threat-I: Threats to system level security; Threat-II: Threats or Theft via services; Threat-III: Threats to privacy; √ - Detailed Discussion; LD - Limited Discussion; ND - No Discussion

Tan et al. discussed security advances in SG over the period of 2010 – 2015 [25]. The authors covered the data driven approaches, e.g., data generation security, data acquisition security, data storage security, data processing security and security analytics in the SG networks. They thoroughly analyzed the suitability of various security analytics techniques, e.g., statistical methods, data mining and visualization. These techniques can be employed in data analytics to ensure security of the SG networks. However, Tan et al. did not consider whether the proposed techniques have negative implications and other complexities from the viewpoint of the SG networks.

In [2], the authors surveyed smart electicity meter data intelligence techniques for future energy systems. Alakhakoon and Yu first discussed the key aspects of the smart metering process, and the interest of different stakeholders. The authors then briefly discussed the smart metering tools, including support vector machine, and fuzzy logic. These tools can be used to achieve metering intelligence, and to support stakeholder applications, e.g., consumer profiling and load forecasting. The security and privacy issues were briefly discussed in the paper, but they were not the main focus of the paper.

In 2016, He and Yan focused on the cyber physical attacks in the SG [26]. Similar to Wang-Lu's survey, the authors discussed the attack scenarios on the energy generation, transmission, distribution, and electricity markets. In addition, the authors pointed out some of the significant defence mechanisms including protection, detection and mitigation. The survey does not provide details (e.g., pros and cons) of the defence techniques.

In 2018, Stellios et al. [30] discussed the Internet of Things (IoT) enabled cyberattacks in several critical infrastructures (CIs), e.g., industry, smart grid, transportation, and healthcare. The authors modeled a threat vector that can be used against IoT devices. The threat vector includes *critical* IoT enabled attacks and *verified* attacks in the CI systems. In addition, the paper pointed out the hidden IoT enabled attack paths in CIs and services. The authors discussed very detailed cyberattacks in CIs. However, descriptions of their mitigations and solutions are at a high level.

**Privacy:** Finster and Baumgart conducted a survey on privacy-aware smart metering [23]. The authors first formulated significant problems concerning privacy in smart metering: (i) metering for billing, and (ii) metering for operations. Furthermore, they discussed several countermeasures, such as billing via trusted party, cryptography, anonymization, and aggregation in order to provide data privacy to the consumers. The paper includes threats and schemes that were published mainly over the period from 2007 to 2014.

Another work focused on the shortcomings of smart meter data privacy and their solutions [27]. The survey covered the following use cases: (i) billing, (ii) operations, and (iii) value-added services. The authors mainly covered the research results from 2008 to 2015. In addition, the authors in [23] and [27] mainly discussed privacy concerns without considering insecure networks. For instance, as the smart meter data travels through insecure networks, consumers' privacy can be breached at network level. In addition, the detailed security issues are not the scope of both surveys.

In 2014, Mohassel et al. presented a survey on advanced metering infrastructure (AMI) [28]. They discussed the basic concepts of AMI and briefly presented the physical and cyber security challenges including privacy. The paper addressed limited but significant security and privacy requirements in the AMI network. However, the authors neither included detailed threat model and discussion on the state-of-the-art security schemes nor presented the privacy-preserving schemes. In the same vein (in 2016), Yasin presented a survey on smart metering and SG communication [29]. However, the survey papers presented in [28] [29] mainly focus the literature published from 2008 to 2014. In 2018, Wang et al. presented a review of smart meter data analytics, methodologies and challenges in many of smart metering key applications [17]. However, security and privacy issues are not the main goal of the review paper.

### *B. Comparison with our survey*

The previous surveys have their own advantages. Some of the work presented in [21], [25], [26], and [30] categorized many of security issues, for instance smart grid to home and vice versa, security analytics, physical and cybersecurity, and IoT enabled attacks in CIs, respectively, in SG. None of the existing survey covers recent real-time attack incidents on the

energy networks, except the work presented in [30]. Other works [23], [27] and [28] focus on privacy in SG metering networks and present high level solutions with limited analysis. In contrast to the existing survey papers, this survey provides up-to-date activities of rapidly advancing research on SG metering network security and privacy. Moreover, most of the existing survey papers do not consider the detailed threat taxonomy by categorizing it in terms of (i) threats to system level security, (ii) threats and/or theft via services, and (iii) threats to privacy. Moreover, we have pointed out various security and privacy requirements that can be considered from the very beginning of the SG metering network design. In addition, this survey provides an analysis of previously published schemes which are proposed as the security and privacy countermeasures, and includes their pros and cons. Table II summarized a comparison between the existing survey papers and our paper.

### C. Our Contribution

Our work makes the following new contributions:

- **A comprehensive view of security and privacy concerns:** Security and privacy are relevant albeit independent concerns in the SG metering network. We discuss the relationship between security and privacy in SG metering networks. By providing such a comprehensive view, we aim to shed light on how a SG security protocol can be designed with regard to these respective concerns.
- **Detailed taxonomy of SG attacks:** We provide a detailed and hierarchical taxonomy of SG metering attacks, considering the attack surface of SG communication and the attack intentions. The taxonomy includes the most up-to-date literature to the best of our knowledge.
- **A comprehensive study for security and privacy goals and corresponding solutions:** We summarize several security and privacy goals in SG metering networks. In addition, we provide comprehensive reviews on various existing solutions (with their pros and cons) which claimed to address different security and privacy goals.
- **Future research directions:** Based on our study, we identify further research problems to be addressed, along with their early solutions and future directions.

### D. Organisation of the paper

The overall organisation of this paper is shown in Fig. 2. To facilitate the discussion (in Section III – X), we summarize the background of SG metering network in Section II. In Section III, discusses real attack incidents on the energy networks and smart metering networks. These incidents reveal the lack of adequate protection in SG metering networks. To explore the security and privacy issues, we define a threat model and a threat taxonomy that aim to understand several threats in SG networks in Section IV.A, Section IV.B, respectively. Then following the extensive literature from the industry and academia, Section IV.C defines the principal security and privacy requirements for SG metering networks. Based on Section IV, we broadly explore the threat taxonomy (i.e., threats to system level security, threats to services and threats

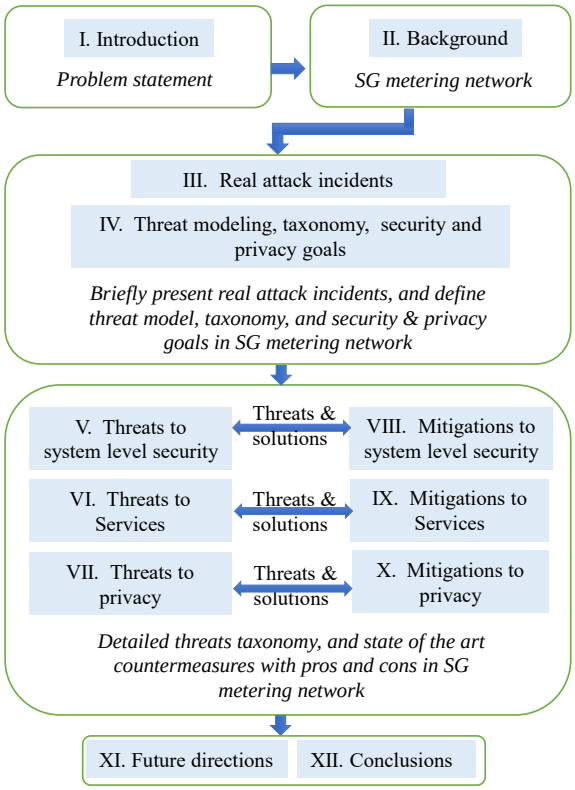


Fig. 2. Overall organisation of the survey paper.

to privacy) in SG metering network in Section V – VII. Following Section V – VII, we provide comprehensive reviews of various schemes (with their pros and cons) that have been proposed to enhance security in the SG networks, while maintaining privacy in Section VIII – X. In Section XI, we discuss open (research) issues that need to be explored for the future directions and conclusions are drawn in Section XII.

## II. Background of Smart Grid Metering Networks

The overall success of a SG and its emerging paradigms are mainly fostered by the advanced metering infrastructure (AMI) or smart metering infrastructure (SMI). Note that AMI and SMI are used interchangeably. The SMI not only improves the value added services for the customers, but also develops the remote control functionality from the utility side (i.e., control center) to smart meters. Moreover, the SMI could lead the opportunities to make plug-in hybrid electric vehicles to vehicle-to-grid application as the distributed renewable energy sources. As shown in Fig. 3, the SG metering network is a wide network and it consists of several technologies, as follows.

### A. Smart Meter – Consumer side

The SG is assumed to be incorporated with a variety of smart functionalities, e.g., dynamic pricing, demand response, outage notification, power connect/disconnect, theft detection, communication with other smart devices and so on [32] [28]. To accomplish these functionalities, a smart meter plays one of the important roles. Note that the SMI is not only limited to smart electricity meters, but it also includes smart gas and water meters. A smart meter is typically installed at the

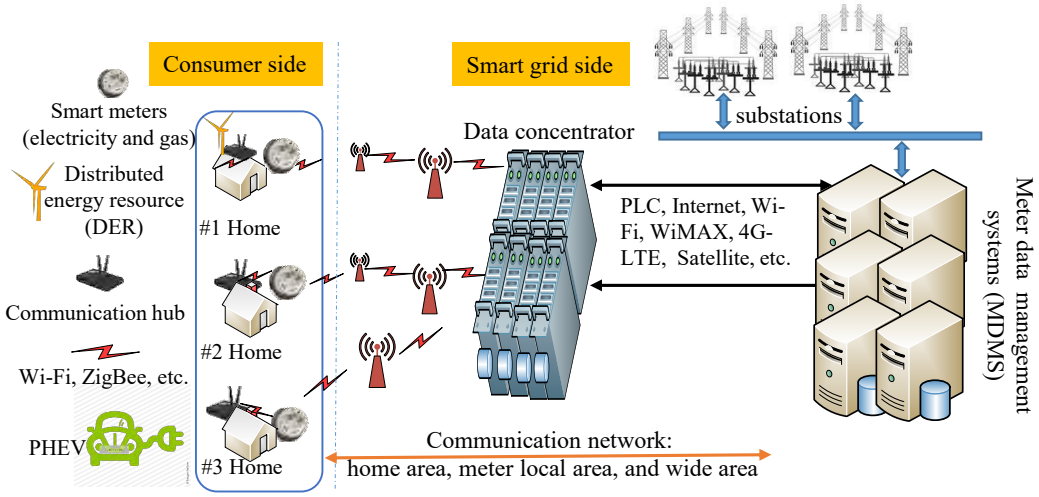


Fig. 3. SG metering network and its components [31].

consumer's premises for measuring, storing, displaying and transmitting the energy uses to the utility companies. However, a latest smart meter is integrated with the following metrology computation blocks, as follows. (i) It comprises of *solid state electronic (hardware and software)*, essentially integrated with a micro-controller system with inbuilt memory that stores energy consumption readings, performs post-processing, and manages control commands and/or alert messages. (ii) An *analog to digital* converter provides an instantaneous footprint of energy uses and power factor. It can also measure the phase current and voltage. (iii) In order to connect with external devices, a smart meter is usually integrated with several *interface units*, e.g., universal asynchronous receiver transmitter, and serial peripheral. (iv) A *display unit* is a regulatory requirement that an end-user can see the consumption report for the billing and energy controlling purposes. (v) A *real time clock (RTC)* provides tariff information in the duration of an hour, a day, a month and a year for data analysis, billing and demand-response purposes. Moreover, the RTC can be utilized in wireless network for the time synchronous purposes. (vi) *Communication*: a smart meter is enabled with two-way communication capability (via wireless/wire-line) for transmitting meter data to the utility, and for receiving control commands from the utility. Alternatively, a smart meter may connect with a communication hub that further connects the appliances within a home and the outer world via the communication networks, as discussed in Section II.B.

### *B. Smart Grid Metering Communication Networks*

A communication network is an enabling technology in order to realize the SG metering networks. As depicted in Fig. 3, a communication network can be divided into following three classical networks.

#### *B.1 Home Area Network (HAN)*

From the utility perspective, the HAN is a group of appliances, entertainment systems, lighting systems, energy storage and generation (solar, wind etc.), electric vehicles. In addition, a home display together a controller provides an interactive user interface which uses for energy control and device maintenance purposes. Within the HAN, a smart meter acts as a home gateway that collects energy consumption reading, sends collected readings to control data center and executes control commands that are received from the utility.

In a typical HAN, the information flows between the smart meter and appliances are not continuous, therefore, each device data rate may vary from 10 to 100 Kbps. The data rate also depends on the number of devices and their distances. Therefore, assuming small distances in the HAN, wireless technologies can be one of the potential solutions that provide many features, e.g., automatic network configuration. Few of home automation technologies are as follows: IEEE 802.15.4 (e.g., ZigBee and Zwave [33]), operates at 2.4 GHz, data rate up to 250 Kbps, and covers up to 50 m. The potential merits of IEEE 802.15.4 include wireless communication, low cost, low power consumption and the flexibility. The demerits of IEEE 802.15.4 are as follows: (i) IEEE 802.15.4 does not provide enough security like WiFi based secure system, and (ii) IEEE 802.15.4 supported devices have low bandwidth [28] so that they cannot be useful in high stream multimedia data.

Another prominent HAN technology is IEEE 802.11 (WiFi), data rate up to 54 Mbps and it can cover up to 300 m. The merits are low-cost deployment and high flexibility. The demerits of IEEE 802.11 are high interference and power consumptions. In addition, following the technical specifications from [34], the advanced smart meters shall be integrated with both IEEE 802.15.4 and IEEE 802.11.

#### *B.2 Meter Local Area Network (MLAN)*

The meter local area network refers to communication between the smart meter and the data concentrator. The MLAN network is mainly located: (i) at the energy distribution domain, which comprises of the data concentrators, and (ii) at the field area networks including many automated devices, e.g., monitors, re-closers, switches, capacitor controllers, etc.

MLAN typically communicates over the powerline communication (PLC) which uses existing wireline connections to

send data from one node to other nodes. The PLC operates at two different data rates called, narrowband PLC (NB-PLC) and broadband PLC (BB-PLC). The NB-PLC can send up to 500 Kbps, operate at 500 kHz frequency and cover up to 150 km distance. Whereas BB-PLC can send up to 200 Mbps, operate at 2 – 30 MHz, and cover up to 1.5 km. Currently, in many countries (e.g., Italy, France, Britain and China) a PLC based technology has been the main choice for communication between the smart meters and data concentrators. The main merits of PLC are low cost, ubiquitous nature, and low deployment cost as it can make use of available communication infrastructure. The demerits of PLC are as follows: higher signal loss, interference and complex routing.

In the SMI, wireless mesh network has been proposed and deployed widely. Each smart mesh meter collects own data and becomes a router for other smart meters to send consumption usage data to the data concentrator. A mesh network can operate up to 900 MHz through unlicensed radio. The Internet is used to connect the smart metering mesh network to the distributed data concentrators which are usually located few kilometers away. Moreover, a mesh network can be a self-formed and self-healed network that can easily tolerate the network faults. For instance, when one smart meter can no longer operate, the rest of the meters can still communicate with each other either directly or through one or more intermediate meters. The main merits of mesh network are as follows: it provides cost effective solution with dynamic self-organization, self-healing, and significant scalability services. The demerits of mesh network are network fading and interference. Each smart mesh meter needs to send messages and acts as a router, which causes high complexity of each smart meter to go up high.

### *B.3 Wide Area Network (WAN)*

In the SG metering network, a WAN is known as the highest-level network that provides connectivity between multiple data concentrators and the utility control center. The WAN is also recognized as a core network through which enormous SMI data, control commands and signals are transmitted and received. In order to provide communication in WAN, several potential technologies can be employed, e.g., IEEE 802.16 (i.e., WiMAX), IEEE 802.20 (MobileFi), PLC, IEEE 802.11 (WiFi) and IEEE 802.15.4 (ZigBee).

The viability of WiMAX for Smart Grid Last Mile (SGLM) communication is shown in [35]–[37]. It provides data rate up to 128 Mbps for downlink and 28 Mbps for uplink, and covers up to 48 km. As shown in [38], WiMAX can provide real-time connectivity, control and a high speed communication with low latency to support multimedia services as an effective facility to mobile workers in SG metering networks.

MobileFi (IEEE 802.20) is a mobile broadband wireless access technology that ensures the reliability, low latency, and high bandwidth. In addition, MobileFi can provide high mobility up to vehicular speed of 250 kmph and can transmit variable real time data from 1 Mbps to 20 Mbps. The MobileFi can be deployed in substation monitoring, and electric vehicle charging system through the distributed renewable generation. More details on the recent communication technologies for the SG can be found in [39]–[46].

## *C. Meter Data Management System (MDMS)*

In the SG metering network, typically information are collected via the communication technologies from the consumers' systems (i.e., smart meters). These information are stored to the utility servers, also called *meter data management system (MDMS)*.

The collected data allows various activities in a power grid, e.g., network controlling and monitoring, operational management, billing, etc. For more details, please refer to [23], [27], [47]–[49].

## *D. Advanced applications in SG metering network*

The SMI enables various enhanced applications in the energy distribution automation system (i.e., accurate modelling of load information [50], [51]), and data management system. Examples of advanced applications in SMI are as follows.

### *D.1 Demand Response using SG metering network*

Through the load management systems, the utility companies can detect peak load demand and control them via the demand-response (DR) program. In DR programs, the SM enables a customer to act as an active participant in overall grid load management via controlling energy use within the HAN [52], [53]. Consumers wish to voluntarily lower their normal consumption either during the peak time network congestion or based on the events when energy prices are high [52].

Nevertheless, the successful implementation of a DR program relies upon an efficient two-way communication system between the DR consumer and the utility. A generic DR architecture is shown in Fig. 4.

- The utility first defines a DR event – the peak-time when customers' electricity demands need to be shifted (from on-peak to off-peak times) depending on their preferences. Then, a DR-request packet including dynamic price signals is sent from the DR automation server (DRAS) to the DR customer via the SG metering network.
- The end-users who intend to alter the timing (or wish to reduce electricity consumption), communicate back to the utility with their DR-response packet including their requested price, load shift and timing.
- Home energy management system (HEMS): In a home, the HEMS system is a (software and hardware) system that is accountable for managing and controlling several functionalities, e.g., utility bill tracking, real-time metering, equipment management, and so on.

### *D.2 Outage Notification using SG metering network*

Many SG systems enable the endpoints to send a "last gasp" message to utility to inform that an outage has happened in a SM and it is out of power. Such a function can help the whole grid system efficiently respond to the outage condition. Fig. 5 shows the sequence diagram, describing how such last

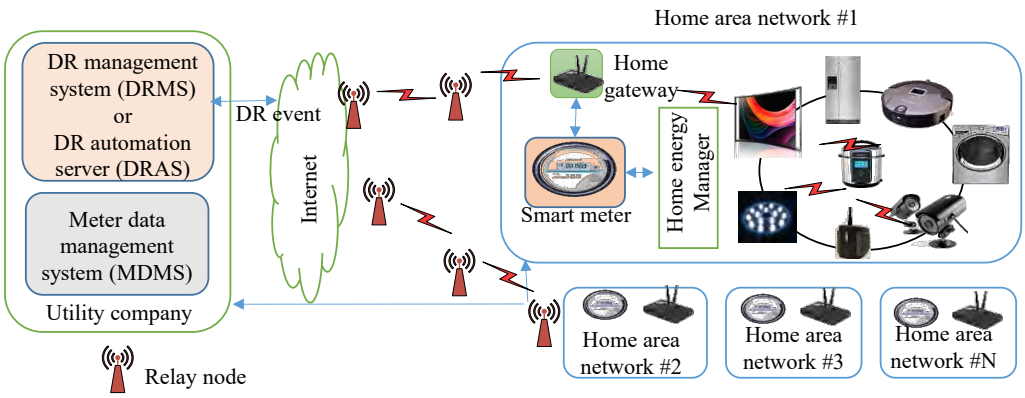


Fig. 4. Demand response program flow of information.

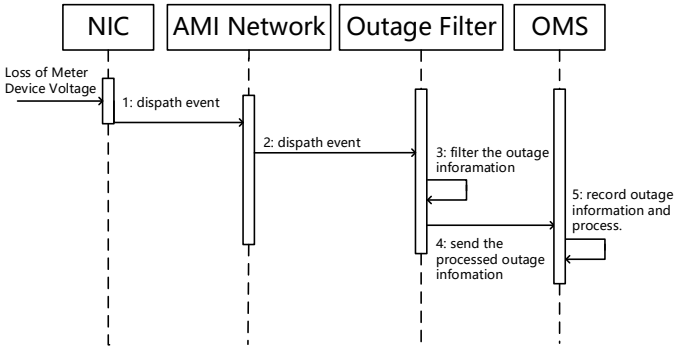


Fig. 5. Outage Notification Scenario [54]

gasp transmission functionality works. There are four entities involved in the outage notification scenarios:

- **Network Interface Component (NIC)**: The entity represents network interface to endpoint metering device.
- **AMI Network**: The entity represents the network of AMI, which is responsible for measuring, collecting, analyzing energy usage, and communicating with metering devices.
- **Outage Filter (OF)**: The entity provides filtering information for the "last gasp" information from AMI to Outage Management System, which helps to filter noise and short-term outages.
- **Outage Management System (OMS)**: The entity is a system used to improve the response to reported outages and expedite power restoration of the homes.

In Fig. 5, the entities interact with each other to fulfill the goal of outage notification as follows. NIC can detect a zero voltage (i.e., loss of voltage) in some smart meters. Afterwards, it sends a last gasp information to SMI Network and AMI Network routes the OF (step 1, 2). When OF receives the transmitted data, it filters the data according to specific filtering rules (step 3). If the data is valid after applying filtering rules, the OF sends a message to OMS (step 4).

Finally, OMS updates the received messages and updates the status of the corresponding device (step 5).

## III. Attacks in the Power Sector and Smart Metering Networks

As the popularity of vulnerabilities on the power grids has been risen during past few years, it is necessary to briefly elaborate the real-world attack incidents in energy sectors. In addition, we discuss the serious consequences caused by the insecurity on energy network, for instance energy companies, renewable energy resources, and customer side SMI.

### A. Attacks on energy companies

The energy company is considered as one of the most vulnerable critical infrastructures. For instance, on December 23, 2015, three Ukrainian power distribution companies known as "Oblenergos" experienced coordinated cyberattacks that resulted in a power blackout in the region [55]. The attack impacted approximately 250,000 customers and lasted blackout for several hours. The attack began through a phishing email containing a *malware-rigged attachment* (e.g., documents and excel sheets). When users opened the Word Documents and Excel spreadsheets in the companies' business network, the dropped *BlackEnergy3 malware* will lurk around and that steals legitimate user credentials. It is believed that during the attack, the attackers have *stolen* the VPN secret parameters to control the ICS network. Moreover, the electronic media reported that the attackers remotely accessed the tools to control the HMI and pulled the breakers [62]. Precisely, the VPNs appear to lack of robust *authentication*, e.g., *two-factor or three-factor authentication*. The attackers can use a variety of common techniques to infiltrate the energy companies' systems, such as *KillDisk malware* that deletes selected files on computer systems and renders systems inoperable. Moreover, the attacker uploaded a *malicious framework* via *communication channels* to the gateway devices at substations to knock the system down [26]. Once again on December 17, 2016, Ukrain suffered from another power outage, which is also attributed to the cyberattacks [19], [20].

Candid Wueest [56] reported that a division/section of the Austrian and German power grid was *unexpectedly misdirected* via a *control command* which results the power grid nearly knock down. In this case, a status request query (i.e., *test command*) was mistakenly forwarded/transmitted from

TABLE III
SUMMARY OF RECENT VULNERABILITIES LEADING TO REAL-WORLD CYBERATTACK INCIDENTS

| **Targeted entities** | **Cyber vulnerabilities** |
|---|---|
| Ukrainian power distribution | Authentication violated, malicious framework uploaded, VPN credential stolen [55] |
| Austrian and German power grid | A control command misdirected that led to distributed denial of service attack (DDoS) [56] |
| Renewable energy | A remote attacker can reach out solar panels and SMs and spoof (network) configurations and meter parameters [57] |
| Renewable energy | A remote attacker can inject malicious script to the 442SR wind turbine [58] |
| Smart metering | A puppet attack can result to potential denial of service (DoS) attack and other routing attack in wireless mesh nodes [59] |
| Smart metering | Reverse engineering may lead to electricity usage fraud or may lead to other privacy concerns about the individuals [60] |
| Smart metering | Compromising smart meter communication can lead to monetary effects [61] |

a newly installed Germany gas plant network, finding its way to the Austrian energy power control and monitoring network systems. Moreover, the query produced too many response messages, which yielded even more data queries that successively flooded the control network. Such queries are also called self-inflicted *distributed denial of service* (DDoS) attack. However, to freeze this attack, the division of the monitoring and control system had to be separated and disconnected. Similarly, there are various types of cyberattack incidents (e.g., stuxnet, night dragon and shamoon/disttack) that target different CIs. More details can be found in [56].

### *B. Attacks on renewable energy resources*

Locus Energy offers solar panels based renewable energy systems. However, in 2016, a *command injection vulnerability* in energy solar panels was reported in ICSA-16-231-01 [57]. The research reported that a remote attacker *with low skill* can not only exploit a (PHP) vulnerability to reach out solar panels and smart meters but he/she can *spoof* the network configurations and meter's parameters out. However, to mitigate this vulnerability, the company has produced a firmware update for almost 100K devices.

XZERES is an energy company which mainly maintains and provides wind turbine based renewable energy systems. However, two independent researchers identified the vulnerabilities in a system called "442SR wind turbine". They claimed that by *injecting malicious scripts*, the 442SR wind turbine can be remotely controlled [58]. Similarly, other renewable resources vulnerabilities are reported for the wind turbine in ICSA-15-162-01A [63], the eSolar Light in ICSA-15-160-02 [64]. More research on cyber security assessment of distributed energy resources can be found in [65].

### *C. Attacks on Metering networks*

As reported in [59], the AMI may be utilized as an entry point to damage network functionality in the power grid. Yi et al. discovered a new cyber threat (called *puppet attack*) for the smart meters [59]. The attack can cause a *denial of service* (e.g., *packet flooding*, and *resource exhaustion* – in the terms of energy and bandwidth) for smart meters using wireless mesh network topology. Precisely, in the AMI network, a normal node can be selected as a puppet node, which is mainly controlled by an attacker. This puppet node not only receives packets from the neighbouring nodes, but it can flood bogus packets to AMI network. Such bogus packets can exhaust the *bandwidth* and the *node energy*. The authors claimed that the puppet attack is more difficult to detect than a flooding attack. Consequently, the AMI network performance can drop seriously down. As described by the authors, this newly discovered puppet attack has the ability to cause a "collapse of the network" and it is "hard to discover the malicious node".

At the Black Hat Europe conference of 2014, Alberto and Javier proved blatant security weaknesses of smart meters. The authors argued that by exploiting the reverse engineering, meters can be shutdown and/or an electricity consumption *theft* and *fraud* can be performed over the power line communication networks [60]. In addition, Alberto and Javier also claimed that by *exploiting the hardware*, an attacker can get the encryption keys (e.g., a master key). Then anyone can have full network control over a big area, i.e., to turn on/off lights remotely. A malicious user can use the master key to obtain the power consumption information of a neighbouring house (to determine) "if someone is in the house". Such information leakage can certainly raise privacy issues.

Tellbach-Li presented cyber-attacks on smart meters in a household nanogrid [61]. The authors developed and simulated a network model for a nanogrid, which is closed to a real-world scenario. The model includes a complete household with the SM and the nanogrid. In this study, several cyber-attacks were mounted into the SM to study the effects of different attacks on a household nanogrid. Tellback-Li's claimed that by compromising *SMs communications*, *integrity*, *confidentiality* and *availability*, attacks can cause *monetary effects* on the grid. Finally, Table III summarized the list above mentioned incidents.

**Lessons**: It can be noticed that with the growing usage of ICT, the energy sectors become vulnerable to security and privacy attacks. The lack of adequate protection against coordinated attacks could be catastrophic. For instance, the attack incidents on energy companies, renewable energy resources and metering networks serve as prominent instances to demonstrate the significant consequences in energy networks. Such vulnerabilities can also impact in many ways, ranging from benign disruption to act of sabotage, threatening individual live to economic fraud and even more the national security threats. Moreover, these attacks point the urgency to improve the resilience of next-generation power grid where a massive number of heterogeneous smart meters, sensors, and control systems will be inter-connected via several technologies.

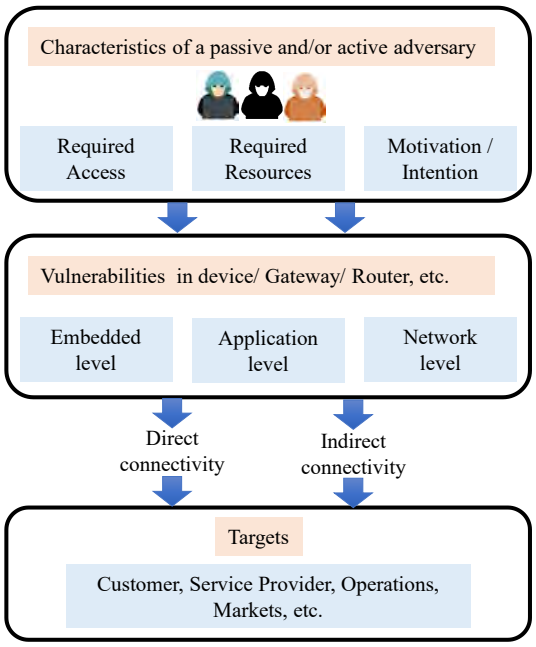


Fig. 6. A high-level threat model in SG metering network.

## IV. Threat Modeling and Taxonomy, and Security and Privacy Goals in SG Metering Networks

Following Fig. 3, the SG metering network favors the interoperability and remote management and control of several entities, including consumers, data concentrator systems, etc. These entities unfortunately might be vulnerable to various cybersecurity attacks. The inter-connectivity of those entities, together with their inherent constraints, enables several threat vectors targeting the SG metering network systems, services, applications, etc. The threat vector defines a procedure that a threat agent used to cripple down the target. This section first defines the threat model, and then presents the threat taxonomy in SG metering networks. Finally, we point out the security and privacy requirements that can be considered in the designing of SG metering networks.

### A. Threat modeling in SG Metering Networks

In order to understand the threats in SG metering network, we must briefly discuss the involved entities, and examine their interactions for mounting attacks. Fig. 6 shows the high-level adversary model, including adversaries, vulnerabilities and targets. The threat model followed in this paper is conceptually adopted from [30].

#### A.1 The Adversary

The adversary is a threat agent (or a group of agents) that aims to cause substantial harm to a target system by exercising powerful attacks. A threat agent may include hackers, cyber-criminals, legitimate consumers, etc. As shown in Fig. 6, an active or passive attacker can be modelled as follows.

1) *Required access to SG metering network*: It means that what type of access to SG metering network is required, for instance *physical access* or *logical access*, to mount an attack.

In *physical access*, if an attacker has direct access to the target systems then we call it an *insider*. More precisely, an insider can have direct access to the proximity of a system and that may be enough to mount an attack. On the contrary, if an attacker that has no direct physical access to a target system then we call it *outsider*. An outsider can gain knowledge by tampering other devices to mount the attack.

In *logical access*, an attacker can connect logically to the target systems via the available insecure components or interfaces (e.g., open ports). These components might be inherently vulnerable to threats [66].

2) *Required resource*: To mount an attack, the required capabilities mean the ability to use the resources, e.g., high resources (such as advanced equipments) or low resources (such as cheap devices). In addition, other factors include technical skills (e.g., expert or non-expert), knowledge, and time, to exercise the attack.

3) *motivations/intentions*: The motivation of attackers is typically include: (a) intended to cause disruption or destruction of SG metering network systems (we call it *strong motivation*); (b) gain access to the system that benefits to adversary, e.g., energy theft threat, financial losses; and (c) the fact that an attacker may have different intentions, such as intend to know the life pattern of the individuals and whether the property is occupied or not. All these intentions lead to privacy issues.

#### A.2 Vulnerabilities in SG metering network

In the SG metering network, a number of heterogeneous systems will be deployed. In our modeling, the system (e.g., smart meter, gateway, router, sensors, and so on) is one of the facilitators of the attack. In most of studies (e.g., [59], [60], [61]), a system is one of the weakest points in a threat chain, and is an entry point for the attacker. An adversary can explore and detect plenty of the weakest links/features of a target system to mount the attacks on SG metering network. Few of these weakest links can be regarded as follows, *embedded vulnerabilities*, *application vulnerabilities*, and *network vulnerabilities*.

1) *Vulnerabilities in the embedded systems*: In [60], [61], a number of vulnerabilities in the embedded hardware have been reported in SG metering systems, e.g., *lack of tamper protection*, *weak encryption module* and *algorithm*, *hardware design flaws*, etc. In addition, numbers of embedded software flaws have been discussed in the smart metering systems, such as bugs in [67], [68], malware and lack of software update in [69]. Utilizing these software vulnerabilities, an attacker can pose huge impacts on the smart metering network, and on the consumers, e.g., a black out in home.

2) *Vulnerabilities in the applications*: An application deals with metering data management and other value added services (e.g., automated billing and demand response program) for the consumers. However, exploiting *software flaws* and *accidental misconfiguration*, an attacker may lead to cyber threat, e.g., inappropriate data delivery scheduling from millions of smart meters, as discussed in [70].

3) *Vulnerabilities in the networks*: In SG metering network, a device (including meter, gateway, and/or router) is connected via the network and communication protocols. However, the network level protocols can be explored to mount many of attacks, as demonstrated in [59]. As an example, numbers of networking and communication protocols, e.g., IEEE 802.11.x

( i.e., mesh network, WiFi), IEEE 804.15.4x (i.e., ZigBee, Zwave, etc.) are reported to contain security vulnerabilities [71], [72]. A recent study reveals how an attacker can exploit compromised smart meters to inject, modify, delete data, to the gateway or router in SG metering network [73]. In addition, the *lack of key management* techniques of symmetric keys and/or public keys in the network and communication protocols completely exposure to the attacks (e.g., no data integrity, no confidentiality and lack of authentication).

### *A.3 The targets in SG metering networks*

Exploiting the aforementioned vulnerabilities, an attacker may target the actual targets but not limited to, e.g., customers, service providers, and market. Nevertheless, the actual target and attack may depend on an attacker's motivation and/or intention. In the SG metering networks, the targets are typically interconnected with the heterogeneous systems via the network and communication technologies. In our high-level threat model (refer to Fig. 6), we regard the interconnection between the systems and targets, as *direct connectivity*, and *indirect connectivity* [30]. Based on the connections, an attacker may exercise an attack to a target, as follows.

1) *Direct connectivity between a system and target*: In this attack, a system and target both together have a direct connection, such as physical and/or logical connections. If a system is installed in a physically secured premisses (e.g., a smart meter, which is installed in a building area network), then it can be referred as a *direct physical connection* between a system and target. Whereas, if a system is installed inside or outside in a physically secured premisses then it can be referred as a *direct logical connection*. For instance, a router/gateway may be installed either inside or outside in a physically secured location in the NAN [74].

2) *Indirect connectivity between a system and target*: To enable novel business models, the metering network requires new transformations, for instance "bring your own device (BYOD)" policies. Precisely, the consumer may buy and install (untested) demand-side response ready systems (e.g., smart thermostat) from an untrusted manufacturer [75]. However, such a system may connect with a target in an indirect and non obvious way. This indirect connection path can pose high risk, and can be used to mount the attack on advanced applications, such as demand response programs.

## *B. Threat Taxonomy in SG Metering Networks*

Based on the attack model over multiple entities and their inter-connections via communication technologies (as shown in Fig. 3), we grouped the threat taxonomy into mainly three categories, as shown in Fig. 7 [76], [77]:

- Threats to system-level security: An attacker may attempt to take down (partially or fully) the SG metering network. For details refer to Section V. The countermeasures for threats to system-level security are presented in Section VIII.
- Threat or theft to services: An adversary may aim to steal services in the SG metering applications, such as billings, etc. For details refer to Section VI. The countermeasures for threat or theft to services are presented in Section IX.

TABLE IV
LATENCY ASSOCIATED WITH APPLICATIONS [80]

| **Time latency** | **Applications** |
|---|---|
| $\leq 4ms$ | Protective relaying (to detect defective circuits) |
| $Subseconds$ | To monitor device state in WAN |
| $Seconds$ | Controlling substation, and feeder management |
| $Minutes$ | Continuous checking uncritical device and pricing |
| $Hours$ | Energy usage unit and wholesale-market pricing |
| $Days$ | Long-term monitoring (e.g., microgrid information) |

- Threats to privacy: An attacker may intent to target to compromise the confidentiality of consumers' sensitive data over insecure systems or networks. For details refer to Section VII. The countermeasures for threats to privacy are presented in Section X.

## *C. Security and privacy goals in SG Metering Networks*

### *C.1 Security goals*

The SG metering network is a mission critical infrastructure – consisting of major elements, such as information technology (IT), ICS and communication infrastructures. These elements are being employed to send command information across the energy networks, and to report usage/consumption, price, billing, and DR programs among the energy companies and end-consumers. The SG metering network therefore requires new expansions and methodologies to deal with the IT, ICS and network infrastructure and their incorporation with the physical devices, machines, equipments and end-consumers [78]. This paper points out following security goals that should be considered from the early design of SG metering network. Note that the goals are directly adopted from [21], [79]–[81].

- **Availability**: Based on consumption usage data (i.e., SM) in the HAN, the utility supplier's is now able to balance and manage the bulk generation and consumption. In this regard, the SMs reports are significantly important for the energy feedback purposes [82]. Therefore, the availability of SMs data has become crucial for the SG metering network reliability. Note that availability requirements may vary based on the applications, such as the protective relaying requires $\leq 4$ *ms* (time) latency to detect defective lines and circuits. Therefore, data availability is one of main design goals in the SG metering network. Table IV summarizes the applications that require different time latency [80] or data availability.
- **Integrity**: A SM typically sends consumption data periodically to the utility servers via data concentrators. Though the data concentrator may be physically secured from an outside access, its various interfaces with other entities make it vulnerable to be attacked. Integrity provides assurance that the data and control commands have not been altered or modified without authorization. A loss of integrity will cause destruction of information, and will lead to incorrect decision regarding controlling and managing the SG metering network.
- **Confidentiality**: It is a security dimension which analyses whether some specific data should be shielded from

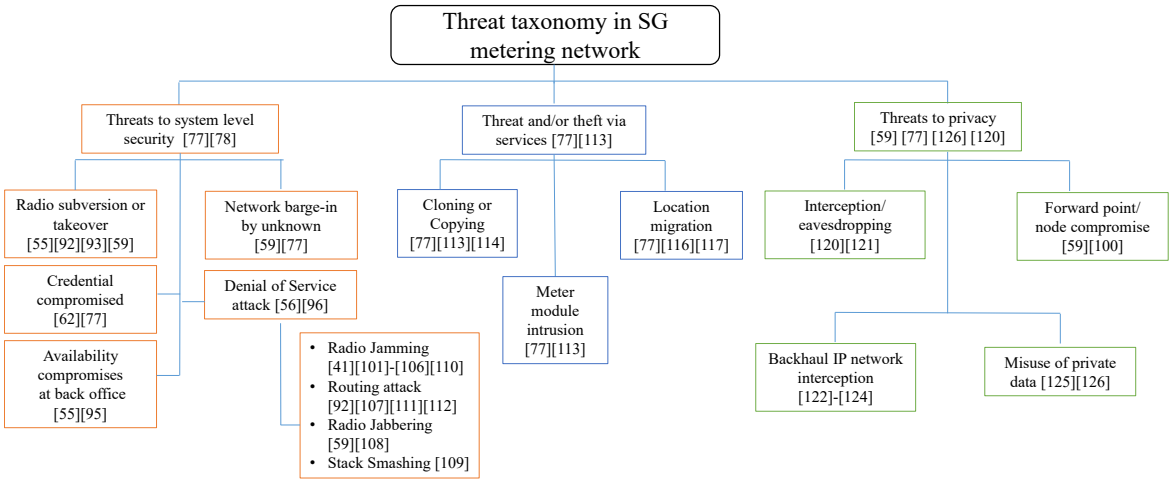


Fig. 7. Threat and/or attack taxonomy in SG metering network.

being disclosed by unauthorised entities. It is the least critical dimension when considering grid communications reliability but a very important one for end consumers. Confidentiality is intrinsically linked to the privacy of end-customers, as consumption usage data can reveal the life pattern of individuals. At the utility servers, therefore consumption usage data shall be kept confidential.

- **Authentication or identification**: SG metering network comprises of millions of entities. Therefore, there is an immense need for making sure that someone or something really is who or what claims to be. Authentication or identification is a logical method for proving the legitimacy and identification of an entity, such as end-user, meter, etc. A SG metering application must be integrated with a strong authentication mechanism that can identify and discard unauthorized connections and commands. In addition, an authentication scheme should also meet the high-efficiency, tolerant to attacks, and support multicast in the SG metering [24].
- **Non-repudiation**: Considering the vast scale of SG metering network, non-repudiation property can detect that an individual had performed some false actions, for example, energy theft by the consumers, and now he/she denies to take the responsibility of the action.
- **Access control**: Numerous stakeholders will share consumption usage data, which depends on the interest of their applications, such as demand supply, load management, etc. However, these stakeholders are required to enforce adequate authorization policies, so that customers data can not be accessed without permission [83].
- **Accountability and auditing**: Periodic accountability and auditing are paramount requirements to further validate the security mechanisms for the SG metering network systems. Despites, there may exist some security breaches but the periodic accountability procedure will help out to detect who is responsible for that breach. Essentially, for the thorough analysis of the SG metering network and their information systems, accountability will make the systems accountable and traceable [84].

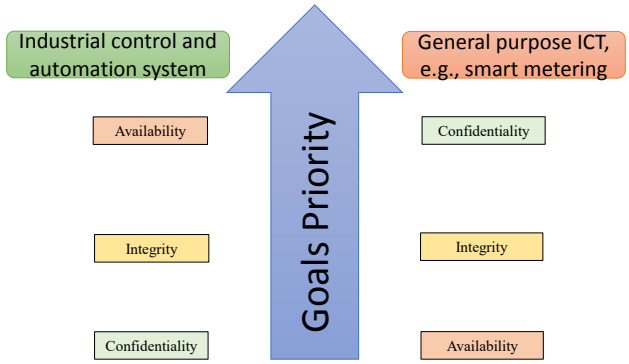


Fig. 8. Security goals in smart metering network.

Noteworthy, in a SG, security goals have different priorities for the different domains, e.g., ICS (i.e., grid automation and control system) and ICT (i.e., general purpose systems – smart metering), as depicted in Fig. 8. To ensure the operational reliability in SG, the priority order is AIC (i.e., availability, integrity and confidentiality). Availability and integrity are given the highest priority goals because ICS systems are main driving forces for the grid automation, human and equipment safety, and environmental impacts. On the contrary, confidentiality is at the top priority in the general purpose ICT processes or in the AMI network. The common known fact is that the consumption usage data is sensitive for an individual, since it can provide knowledge about individual's habits, e.g., if someone is on the vacations or watching TV.

### *C.2 Privacy goals*

In the SG metering network, many of devices (e.g., meters, sensors, actuator, etc.) exchanges their messages across the grid infrastructure via the communication technology and protocol. However, such devices significantly expand huge amount of messages (e.g., control commands, consumption data, and other relevant information) in the different domain in SG, as shown in Fig. 1. For an analogy, the energy suppliers currently collect one month reading per consumer/home. If they start collecting consumption information each minute, the monthly reading per consumer will expend to over 43,000

readings. Indeed, the expanded readings from the consumers help to improve an even distribution among the energy production and consumption, but also bring an array of privacy concerns. For instance, within a given home or other property (i.e., building), the smart metering data will give much more precise picture on individual behaviour, activities, and the time patterns associated with the individual activities. Moreover, the fine-grained energy consumption usage data may even show the total number of personnels in a home or building, which could also reveal the pattern of when the property is empty or occupied. Therefore, the main question is how the consumption usage data can be collected without revealing the privacy of individuals and still be able to useful for practical purposes, e,g., billings, demand-supply, and other operations. Note that this subsection will focus on the communication privacy in SG metering network. This paper discusses the following properties for privacy, which are directly adopted from [85]–[88].

- **Anonymity**: As shown in literature – "*Anonymity is the state of being not identifiable within a set of subjects, the anonymity set*" [89]. Privacy properties such as *consumer-to-utility anonymity* aim to make an entity anonymous from others, even from a peer.
- **Unlinkability**: In this, the data/information are not sufficiently linkable among two entities in a system. From the broad perspective, unlinkability is paramount property that needs to be implemented at different level such as, home area network (smart meter, sensor, home gateway, etc.) and field area network (i.e., data concentrator and substations that are located in cloud or SG servers) [86].
- **Undetectability:** From a SG metering network perspective, entities (e.g., machine, device, equipment, data, application, user) or their information/data could be an interest of a malicious user/adversary to detect or infer knowledge about the entity or data. Therefore, the item/data should be undetectable to the adversary. Furthermore, the undetectability property can be further divided into two forms: zero undetectability and maximum undetectability. For the details, readers may refer to [90].
- **Unobservability**: With this property, an outside observer cannot tell whether communication takes place or not – i.e., an uninvolved entity (e.g., an outside observer) cannot sufficiently distinguish whether a targeted entity (smart meter) had executed certain messages or other actions on interest, for instance, sending consumption messages, demand-bidding messages, paying bills, or logging in.
- **Pseudonymity**: "*A pseudonym is an identifier of a subject which is different from the subject's real names*" [89]. In grid communication, many stakeholders can access the consumption data from the smart meters, therefore, a smart meter must have several identifiers (i.e., pseudonmity). These identifiers only be possessed by the dedicated entities those are communicating or exchanging messages with the smart meter.

## V. Threats to System level Security in SG Metering Network

In a SG metering network, smart meters are to be installed on the individual premises that will likely be part of the AMI network. A smart meter transmits/receives data and many other pieces of sensitive information among the dedicated data concentrators, control centers, and customers. However, an attack on system level security can take down a part of or the whole power grid. For example, assume a SG metering network as shown in Fig. 3 – a malicious agent or a group of agents (e.g., insider or outsider) may try to alter the program instructions in smart meters, and deliberately modify alarm thresholds. Such agents may send an unofficial signal (e.g., a disconnect meter command) impersonating the utility to the millions of smart meters or to other load control devices in the energy grid. These attempts may result in damage to machine, unusual shut-off of power operations or even crippling of control equipment. In the SG model (see Fig. 1), such attacks may influence the roles of *Customer*, *Service Provider* and *Operations*. As depicted in the threat taxonomy in SG metering network (refer to Fig. 7), the threats to system-level security can be further divided into followings:

### A. Radio subversion or takeover

This threat aims to control/take one or more radio channels to intercept RF communication modules, so that the intercepted radio channels "belong" to the attacker. As shown in Fig. 3, the smart meter or data center and/or data concentrator talks wirelessly utilizing various means of communication technologies. Over the wireless radio, an attacker can manipulate the smart meter dynamics in order to inject malicious code (e.g., control command/firmware). For instance, at the consumer side, the manipulated control command might effect mainly meter's metrology board. If a control command/alert message is replaced with the malicious intention, then an attacker can attempt to jeopardize the availability of devices by flooding further fake commands at large scale, such as, home appliances or other devices. By doing this an attacker can takeover on homes, buildings, and societies. Moreover, if an attacker takes control on radio communication, he/she will be able to issue disconnect commands (again and again) to millions of meters since there is no adequate way of checking the authenticity and integrity of these commands [91], [92].

Considering the grid side, the recent real incident on the Ukrainian power revealed that the attacker uploaded a *malicious framework* to the gateway devices at substations in order to knock the system down [55]. Such threats can have serious financial implications for the end-users, utilities, and other entities in the SG metering network [93]. Consequently, this threat (i.e., radio subversion) is assumed to be highly severe (e.g., loss of availability and integrity), since unauthorized entity can takeover either on grid side or on consumer side, or on both side together.

### B. Credential compromise

In order to harm the SG metering network, the cyber criminals can obtain large volumes of credentials for the purpose

of system control at the utility side. For example, in the Ukrainian power cyber attack, it is believed that the attacker compromised/stole VPN's (weak) credentials and reached the ICS, and remotely accessed the tools to control the HMI [62]. Here, the weak credentials means weak authentications, poor access control policies defined and weak passwords that might have been used to break the system. Typically, credentials check the legitimacy of identity of an entity on the network and system, and then let that entity access communication network, such as, VPN, access point, communication module/meter and operation and management system [76]. The compromised systems' credentials, therefore, enable an attacker to plan coordinated attacks on the weakest link of the power plants. Consequently, blackout the societies are potentially high risks on the national security, and so on. The impact of this threat can be catastrophic or higher.

### C. Availability compromises at back office

Consider the utility side network (please refer to Fig. 3), a perpetrator (e.g., insider or outsider) would take illegal access to computers by exploiting social engineering attacks (i.e., this also known as back office compromise). For instance, according to the Wall Street Journal, cyberspies have ever gained access to the U.S. electrical grid computers. Moreover, the attackers left out (malicious) software programs that could be exploited for one or more threats, as reported by the current and former national-security officials [94]. In a recent attack on the Ukrainian power distribution companies, as the official documents and spreadsheets, when clicked or opened, dropped a BlackEnergy3 malware, as reported in [55]. The tremendous capabilities of malwares, such as BlackEnergy3 and KillDisk, may pose major necessary threats (e.g., information leakage, access control violation) to corrupt or overwrite the master boot records, databases, power control servers and so on. As a consequence, the impact could be catastrophic or high and may lead to financial losses.

### D. Network barge-in by unknown

In the SG metering network (Fig. 3), different entities usually exchange messages and/or information via the single-hop or multi-hop communications. For instance, (i) consumer side: a smart meter forwards consumption usage via single or multipath routing to the upper layers; (ii) grid side – load management program: a demand response (DR) manager sends DR signal via multi hop communication (using relay node) to the end-users, as shown in Fig 4. For single or multihop communications, wireless relay nodes are used to exchange the information/control commands in AMI network. Usually these relay nodes are unguarded. Routing data therefore through the public network (i.e., relay node) is considered one of the weakest point (or anomalous activity point) to be attacked. It is possible that a rogue relay node can make available for absolute access to the adversary who may aim for anomalous activities, such as message modification, man-in-the-middle and packet analysis threats [59]. Such anomalous activity can disrupt or mislead the communication modules at the utility to meet the varying demand of the end-users (i.e., house, factory, and so on) without being detected. For example: (i) for the personal interest, an ill-intention adversary (a factory rival) may set up a rogue communication module in the smart metering network routing path to piggyback radio traffic (requested energy) from the factory side over the mesh network infrastructure. (ii) Malevolent user attempts to disrupt communication modules via unofficial (transmission or reception) channels or uses an "unknown" routing to intercept (e.g., puppet attack [59]) traffic in the SG metering network. (iii) Typically, the control center sends control commands to the substations – any tampering with routing either on control command or packet address can lead to false alarm, system outage, etc. Moreover, an attacker may undertake to modify the control command packets to assume a different role, e.g., manufacturer of energy, consumer of energy, or distributor of energy, etc. Such threats may severely effect degradation of functional capability or may lead to major damage to network availability and integrity.

### E. Denial of Service

In this threat, a malicious activity can weaken or downgrade the operational performance of the whole SG metering network from its anticipated operations. An attacker can exploit the inherent vulnerabilities of network at different layers to take down the communication performance. These threats result low to high impact in all or part of the network becoming unserviceable (or unavailable). For instance, a misdirected control command leads to DoS attacks and about to take down the Austrian utility network [56]. In [95], Asri-Pranggono evaluated the impacts of DoS attacks (e.g., flooding attack) on the AMI network. DoS attacks can be further categorized as follows.

- **Radio frequency (RF) spectrum jamming**: The wireless communication technologies are one of the main components in realisation of a SMI. For instance, cognitive radio (CR) particularly is highly promoted to deploy in the SG network that can utilize all possible spectrum resources [41] [109]. However, incorporation of CR technology (at physical (PHY) layer) in SG will also bring new security challenges [104] [105]. A recent research [103] proposes a new attacking strategy (i.e., spoofing and jamming) in CR network using power distribution by applying dynamic programming in wireless SG. This research focuses on attacking at super users (SUs) and reduces SU's spectrum availability and transmission performance. In addition, the authors claimed that the attack success probability in CR technology is always higher within the power constraint. However, the main objective of a jamming threat is to jeopardize the communication among the smart meters and utilities via a radio emitter device. This is the most common attack on the physical layer that prevents signal from being received. Typically these attacks can have two different classes: i) *proactive jamming*, it can transmit high-energy noise signals consistently to squeeze a wireless channel completely (i.e., whether there is data on the communication channel) and put all the nodes in non-functioning mode. (ii) *reactive*

TABLE V
SUMMARY OF THREAT TO SYSTEM LEVEL SECURITY IN SG METERING NETWORK

| **Threat to system level security** | | | | |
|---|---|---|---|---|
| ***Threat*** | | ***Description*** | ***Security goals compromised*** | ***Threat impact*** |
| Radio subversion or takeover [91] [92] [96] | | An attacker can manipulate SMI dynamics over the wireless radio through *Unauthorized RF interception*, *Eavesdropping*, *Malicious code*, and *Replay attack* | Availability, authenticity, availability, integrity, Authenticity, availability | High |
| Credential compromised [62] [76] [97] | | Over insecure metering network, an attacker can control the systems at grid side via: *Stolen credential*, and *Integrity violation* | Authenticity, access control Integrity | High |
| Back office compromise [55] [98] | | An insider can misuse smart metering systems (e.g., computers) by exploiting social engineering attacks, such as: *Illegal access*, and *Disrupt system* | Authenticity, confidentiality Availability, access control, accountability | High |
| Network barge-in by unknown [59] [99] | | Routing SM data through public network (i.e., relay node) can cause *Traffic analysis*, *Message modification*, and *MITM* | Confidentiality Availability, integrity, Authenticity | High |
| Denial of Service threats [56] [95] | RF Spectrum [100]–[105] | A jammer can squeeze the SMI network when it senses an active radio channel is labelled as occupied, thus cause *Jamming*, *Spoofing*, and *Delay in delivery* | Availability, Integrity Availability | Low to High |
| | Routing [91] [106] | Routing in SMI is vulnerable to several DoS attacks: *Neglect and Kill packets*, *Misdirection*, *Spoofing*, *Replay, Control traffic, and MITM* | Availability Availability, integrity Confidentiality, authenticity Availability, integrity Authenticity | Medium to High |
| | Jabbering [59] [107] | A malfunctioning smart meter can be co-opted to transmit so much traffic as: *Flooding*, and *De-synchronization* | Availability Authenticity, availability | Low to High |
| | Stack smashing [108] | The application layer of SMI may vulnerable to *Memory overload*, and *System crashing* | Authenticity Availability | Low to High |

**Low** - means the limited effect that put down the single entity functionality to minor damage to assets, minor harm to individuals by compromising one or more security goals. **Medium** - means the significant adverse effect that degradation of a single entity functional capability to significant damage to assets, significant harm to individuals by compromising one or more security goals. **High** - means the severe adverse effect that degradation of a single entity functional capability to the fairly high damage to infrastructure, substantial financial loss, and major damage to societies by compromising one or more security goals [21].

*jamming*, firstly, it keeps silent and overhears on certain channels. Secondly, once it overhears the wireless messages are being triggered within the transmission range then it can launch DoS attack. The active adversary can firmly squeeze transmission and reception using the high RF signals, which can deliberately damage the information flow in smart metering infrastructure as follows. Consider a demand response manager initiates a demand response event for the consumers. In this scenario, (i) a jammer can squeeze the network when it senses an active radio channel is labelled as occupied, since a message (an event) is being sent from a sender (i.e., demand response manager); and (ii) the consumer device (i.e., smart meter) might be deliberately precluded from receiving event packets that are sent from sender [100]. Consequently, the smart meter (i.e., receiver) always waits for the data packets. In addition, Namboodiri et al. have pointed out how a jammer can temporarily/permanently connect or disconnect AMI messages by spoofing packets [101]. For WSNs, Yang et al. [102] proposed a novel attack called "learning-based jamming (LearJam)". The LearJam has two-phase design: (i) learning phase, and (ii) attacking phase. Authors claimed the LearJam can achieve successful attacks, and can reduce the network's throughput considerably. In summary, such RF jamming attacks can escalate potential damages or endure concerns to the network performance of two-way communication in smart metering network.

- **Routing attacks**: Routing is vulnerable to DoS attack, e.g., selective forwarding, black hole, etc. For example, consider the multihop communication in AMI – if a node is compromised then it can broadcast a "hello" message and can represent itself as the shortest path to other nodes. Consequently, all the neighbouring nodes traffic get directed to the compromised node and thus pose DoS attack to mislead the meter data. Moreover, Lin et al. demonstrated if the forged data is injected in the routing path (by an attacker), it can cause disproportionation of the demand and supply patterns that will escalate the prices for the energy distribution – consequently the energy distribution process will be disrupted [106]. In [91], Kaplantzis-Sekercioglu discussed how selective forwarding attack can be the interest of attackers. In this attack, an attacker can include himself/herself (e.g., man-in-the-middle) in the data flow path of interest. Then the attacker may choose not to forward selective packets and drop them to cause a black hole effect in the end-to-end packet delivery of smart meters or demand response program. A variant of this attack is that the adversary only drops packets coming from specific sources (e.g., HAN or utility center, referring to Fig. 3) or drops packets in a random fashion, whilst reliably forwarding other packets [91]. Another routing threat is to kill packets – by killing packets (e.g., trip-off/control commands), an attacker can cause routing to crash or become unavailable. Moreover, considering a DR program (referring to Fig. 4),

an attacker can kill the DR program packets/signals so that the consumers cannot participate to the DR program. The packet killing threats, thus, can damage the integrity of the SG metering network. More information on routing protocols and challenges in power grid network can be found in [110], [111].

- **Jabbering**: Jabbering can control end-to-end links. In this attack, a malicious smart meter is co-opted to transmit so much traffic (i.e., flooding and de-synchronizing) that other nodes cannot communicate. For example, Yi et al. have shown how the flooding attack can severely downgrade the resources via transmitting fake control signals, in the smart metering networks [59]. In de-synchronized attack, a malevolent adversary may disturb the communication link that has been established among two legitimate entities (i.e., HAN and utility company data center, referring to Fig. 3) by re-synchronizing their transmission. Moreover, this attack is also called puppet attack, whereby an attacker can act as a puppet node, and can transmit attack messages. Upon receiving the attack messages, the puppet node will be firmly taken over by the adversary. Consequently, the puppet node floods more messages to the other neighbouring nodes to take down the network communication performance and drain the node energy. Moreover, the authors demonstrated that puppet attack can take down 20-10 % of message delivery ratio that could be a serious concern for the SG metering network [59]. Consequently, network bandwidth and performance can be disturbed. In addition, it can exhaust the device resources (battery depletion). In another research [107], Wang et al. discussed transport layer protocol security implications in the power grid synchrophasor data communication. More details can be found in [107].
- **Stack smashing**: The attack is mainly applicable to the application layer. It is a procedure – to damage or crash the application or device's operating system by the means of overloading/overwriting the memory buffers with more (bogus) data as compared to the size of the memory-buffer (especially in resource hungry devices). Therefore, the sensitive data will be revealed, lost/corrupted by the attackers. Moreover, in [108], the authors demonstrated that software applications in SG domain are potentially weak such that a room may be opened for DoS attacks.

In Table V, we summarize security goals violated in the system level threats including their impacts.

## VI. Threats or Theft via SG metering Services

In addition to different types of attacks to system level security against the SG metering network, the energy companies may face other potential threats that can result in the theft of metering services, as shown in Fig. 7. For instance, preventing a SG metering network operator from collecting revenues [76], [112]. In such threats, an individual smart meter (or a group of smart meters) within a geographical location, intentionally sends incorrect report of the consumption usage data to the energy company. Precisely, a customer may reduce his/her amount to pay in the bill by executing a demand reset operation after the first number of billing cycles [112]. The rate of theft seems not too big, although the cumulative effect on the energy companies will be very significant. From the perspective of SG model (see Fig. 1), such an attack type can influence the roles of *Customer*, *Market*, *Service Provider*, and *Operations*. The main threats in this category are as follows [76], [112], [117]:

### A. Cloning a smart meter

As the SMs are manufactured by different companies, with the collaboration of an insider (i.e., employee) – an attacker can have an opportunity to access the binary image of keys, IDs, and framework of the smart meter and can clone a smart meter. Such cloning threats provide adversaries with the capability of impersonating or masquerading other legal smart meters. Precisely, with cloning a smart meter, a perpetrator can change a meter or radio channel ID with the duplicate copy such that the fabricated meter can lower own electricity bill or can send zero usage report. Moreover, as reported in [118], the attacker can sell meter design for own benefits. Such cloned meter may have low to high impact. For instance, if a number of cloned meters start sending fake readings to the utility company then the utility company may have a big revenue loss [113].

### B. Meter module compromise/intrusion

An energy theft (by means of a meter compromise) is usually referred to as non-technical loss to the utility company [114]. An attacker can make such theft by meter bypassing, meter compromising and tampering, and/or defective meters. Moreover, a modern smart meter is integrated with the communication module, which can be disconnected with an ill-intention such that the meter stops sending consumption report to the utility. A perpetrator may attempt to separate communication module into the pieces in order to shift the usage information (from higher to lower), to report zero usage of power or to forge the demand. In another threat, considering the billing scenario, a mischievous customer can replay the previous consumption messages to the utilities, to make the financial loss. As a result, this threat can pose major impact. Moreover, as the new green energy systems (e.g., solar, wind) are emerging, the end-users can play an active role as energy producer and they can sell energy to the utility company when demands are surpasses the supply. A malevolent consumer can alter the messages, by the means of increasing and decreasing the number of green energy units that to be sent (or reversed) for billing, as reported in [112].

### C. Location migration

To make frauds (i.e., message modification, billing frauds, etc.) in SMI services, one of the possible ways to change the meter location [115]. For instance, to cut down the reported consumptions and related (consumption) bills, a malicious customer can change the meter from a site that asks high usage price with the meter from a site that takes considerably low

TABLE VI
SUMMARY OF THREAT OR THEFT OF SERVICES IN SG METERING NETWORK

| **Threat and/or theft of services** | | | |
|---|---|---|---|
| Threat | Description | Security goals compromised | Threat impact |
| Clone a smart meter [76] [112] [113] | Clonning a SM may lead to many attacks: *Impersonation, Masquerade*, and *Malicious code* | Availability, confidentiality<br>Confidentiality<br>Availability, integrity | Low to High |
| Meter module compromise [114] | A compromised SM may utilize to mount: *Replay attack*, and *Eavesdropping* | Authenticity<br>Authenticity, availability | High |
| Location migration [115] [116] | An ill-intention attacker can change SM's location by: *Message modification*, and/or *Traffic analysis* | Confidentiality<br>Availability, integrity | Low to Medium |

usage price, as discussed in [76], [116]. In addition, PHEV can be charged at different locations with malicious intentions. Inaccurate billing or unwarranted service will disrupt operations of the market.

Table VI summarizes the security goals compromised in theft of service threats and their impacts.

## VII. THREATS TO PRIVACY IN SG METERING NETWORK

Privacy issues are one of the main concerns in the smart metering network. Consider a demand response program where the smart meter data and demand response (DR) program signals (e.g., program type including demand-bidding, location, etc.) are exchanged over the public networks via two-way wireless communication. It is highly possible that an unauthorized user can intercept or alter smart meter messages (and DR program signals) while the messages/signals are in transit. In SG metering network, the message alteration or leakage could have fatal outcomes for the targeted household that the messages belong to. Such threats therefore can reveal the personal (identifiable) information to the unauthorized entities. From the perspective of SG model (see Fig. 1), such an attack type can influence the roles of *Customer*, *Market*, *Service Provider*, and *Operations*.

Table VII summarizes the security goals compromised in privacy/confidentiality threats and their impacts. The privacy threats may arise as:

### A. Interception/eavesdropping

The most common threat to the individuals' privacy – consumption load tracing when the user data in transit [119]. Unauthorized interception on the communication channels could allow an attacker to intercept wireless packets. For instance, an attacker (i.e., MITM) may collect consumer's electricity usage preference and deduce the consumer's daily routine and other personal information. As a result, this threat may have major impacts (high) on the individual privacy. As another example, consider a demand response automation server (as shown in Fig. 4), initiates a DR event containing program type, date and time of the DR program, pricing, geo-location, and consumers list via public channel. By eavesdropping, an adversary can collect such information and pose serious threats to customer privacy as discussed in [120]. Eavesdropping on a DR program may not be a severe issue, because although it is vulnerable to the privacy threats, eavesdropping on a DR program may not happen regularly. Nevertheless, such program needs to be protected from eavesdropping and replay attacks.

### B. Forwarding point compromise

Confidential information (e.g., billing and bidding) can be revealed if a forwarding entity/node (e.g., a data collector unit) in the network topology (e.g., mesh infrastructure) is compromised (as shown in [59]). As a consequence, it can forward smart meter packets toward an attacker or unauthorized individual. Furthermore, such compromised forwarding point can pose significant impacts to many use cases. For instance, as shown in Fig. 4, a demand response automation server sends the system load status program (i.e., a DR event) to the consumers. The load status program contains many useful information, such as event identifier, facility identifier, date and time, shed data in kWh, event type (Day-Ahead or Day-of [126]), and load for the consumers (heating, ventilation and air conditioning (HVAC), and so on). However, the compromised forwarding point can forward such information to unauthorised node, and can invade privacy of the customers. Moreover, by exploiting medium access control (MAC) frame address field, an honest but curious neighbour (i.e., a spoofing attacker), can deliberately impersonate as the legal forwarding node to collect consumption usage from the neighbouring meters to learn their life patterns. To achieve this, an attacker can send bogus address resolution protocol (ARP) messages to the smart meters, as discussed in [99].

### C. Backhaul IP network interception

Usually, an utility company uses the backhaul IP network for data aggregation and other operation controls. In the backhaul network, network configuration vulnerabilities may be exploited due to the weak authentication. Moreover, an IP packet can be easily tampered since packet encryption is optional. Therefore, packet spoofing on the source and destination addresses, packet disruption, and substation command resetting, to list a few instances of how devices and machines can be misconfigured at the network and transport layers. These misconfigurations can lead to potential threats to sensitive data [100]. For example, an attacker can alter the destination address and transport sequence when the billing and bidding messages are in transit. Consequently, such data can leak the consumers' privacy as data aggregated at the data concentrators that utilized the backhaul network, as discussed in [121]–[123]. These unauthorised backhaul network interceptions may lead to significant damage to infrastructure, asset, financial loss, and harm to a household privacy.

TABLE VII
SUMMARY OF PRIVACY/CONFIDENTIALITY THREATS IN SG METERING NETWORK

| **Privacy/confidentiality threats** | | | |
|---|---|---|---|
| Threat | Description | Security goals compromised | Threat impact |
| Radio Eavesdropping [119] [120] | SMI data can be leaked over the wireless radio through *Unauthorized RF interception, Eavesdropping* and *MITM* | Authenticity, confidentiality, integrity<br>Confidentiality, Authenticity | High |
| Forwarding point compromise [59] [99] | In SMI network, a rouge forwarding point can be utilized for *Spoofing, Unauthorized forwarding*, and *Message modification* | Confidentiality<br>Authenticity, Confidentiality integrity | Low to Medium |
| Backhaul network interception [121]–[123] | In the public backhaul network, an attacker may control SMI data and device: *Unauthorized aggregation, Address spoofing, and Malconfiguration* | Authenticity<br>Confidentiality, integrity, authenticity<br>Authenticity, integrity | High |
| Misuse of data [124] [125] | At the back end server, the misused of SMI data may cause *Data breach* | Privacy violation | Low to Medium |

### *D. Misuse of private data*

For privacy threats, many researches have considered the privacy issues that arise when the fine-grained consumption information is sent/aggregated directly to/by the distribution network operator (DNO)/energy suppliers, even though this may be the legitimate mode of operation of the system (i.e., no external attacker) [124], [125], [127]. Even if the DNO/supplier is trustworthy, there is also the subsequent threat of a data breach at the DNO, which could reveal this private consumption information to other stakeholders (such as consumer electronic companies). For instance, consumer electronic companies may use utility databases where the consumption information are stored. Having access to such databases, the consumer electronic companies may start following individuals to promote their products, which may be not the interest of the consumers.

## VIII. COUNTERMEASURES TO SYSTEM LEVEL SECURITY FOR SG METERING NETWORK

To protect the SG metering network from threats to system level security (as shown in Section V), this section discusses extensive state-of-the-art papers including their pros and cons. We first discuss the mitigations for radio takeover, credential compromise, and back office compromise. Second, we present the countermeasures for network barge-in by the unknown, and finally, the possible solutions for detecting and mitigating DoS attacks are discussed.

**Radio subversion or takeover mitigations**: In general, an attacker can gain access over wireless communication and can modify, inject, replay old messages to the smart meters or to the data concentrator. To provide a secure framework, Caropreso et al. proposed an open source framework for (customized) smart meters [128]. The framework is based on a client-server architecture, where a smart meter acts as a client and a gateway acts as a server. To mitigate the wireless communication threats (e.g., radio eavesdropping), the authors employed the traditional openSSL protocol that establishes a TLS-based secure communication over the wireless channels between the client and the server. Further, the authors evaluated the data traffic and performance evaluation, and claimed that the proposed framework is semantically secured. Nevertheless, the proposed framework lacks a threat model, such that it is not easy to justify whether the framework is secure against replay attack, message modification attack, etc. In addition, the framework is limited to the customized smart meters, which may not be always practical as the smart meters are typically manufactured by the different manufacturers.

Similarly, Vaidya et al. proposed a secure scheme that authenticates control command in the smart grid infrastructure [96]. Based on ECC, the scheme utilized an interactive on-the-fly verification and/or key agreement for the participating entities over the wireless communication in a HAN. The idea is as follows – the authors assumed that the involved entities (e.g, home device, mobile, and gateway) first need to pre-compute the cryptographic coupons and then prove their legitimacy using the coupons. The authors utilized three-party authentication (i.e., mobile, home device, and gateway), and claimed that their scheme is secure against impersonation and MITM attacks. In addition, an attacker cannot forge the control command within the HAN.

The scheme may require high computational and communicational costs due to a large number of message exchanges between the involved parties (user, smart meter, and gateway).

**Credential compromise mitigations**: As the SMI is one of key components in SG environment, a data concentrator is one gateway to the WANs that include the SG control center [129]. However, due to the lack of adequate access control mechanisms or policies, an attacker may control VPN, HMI, and ICS, and may compromise the credentials [62].

In [129], Hasan et al. proposed a cloud-centric collaborative security service architecture dedicated to AMI. The architecture provides, security as a service, including network security monitoring, encryption key management and security assessment. The geographically distributed architecture comprises of the following entities. (i) A WAN consists of AMI concentrators and a control center. (ii) An AMI concentrator integrated with a traffic monitoring unit, upstreams the data to the WAN. It forms a NAN with SMs to collect data from consumers. (iii) SMs are located at the consumers sites, e.g., homes and buildings, and upstream consumption usage data to the NAN. The authors introduced a concept of distributed data centers to enable security services for the AMI concentrators. These data centers (and/or security servers) are connected with the backbone network in a client-server manner. A dedicated VPN tunnel is assigned for each client/server pair and the security servers are running over the clouds.

Though, the architecture proposed in [129] claimed security

TABLE VIII
SYSTEM LEVEL MITIGATION APPROACHES FOR RADIO TAKEOVER, CREDENTIAL COMPROMISE, AND BACK OFFICE COMPROMISE IN SG METERING NETWORK

| Threat | Applications | Wireless/ Wired | Involved entities | Test-bed/ Simulation | Security Goals | Descriptions | Ref. |
|---|---|---|---|---|---|---|---|
| RT | Data management | Wireless | SM, NAN | Simulation | 3,4 | ***Pros:*** open source framework, client-server architecture, uses openSSL, evaluated traffic and performance analysis ***Cons:*** lack of threat model, and lack of proper security analysis. | [128] |
| RT | Data management | ZigBee/ WiFi | SM, Mobile, head-end | – | 3,5 | ***Pros:*** presented a zero-knowledge identification scheme, on-the-fly key agreement, protection against impersonation and MITM attacks. ***Cons:*** required high computational communicational costs that may cause availability issues | [96] |
| CC | SMI, substation management | unspecified | SM, HAN, NAN, WAN | Simulation | – | ***Pros:*** proposes a cloud-based architecture, mathematical simulations, overall latency is minimized. ***Cons:*** lack of threat model and security analysis, lack of VPN security, encryption key management is not implemented, may vulnerable to several attacks | [129] |
| CC | Substation management | unspecified | substation, control center | Simulation | 3,4 | ***Pros:*** proposes a data-centric access control framework, utilizes fully homomorphic encryption, bloom filter, secure against MITM and spoofing attacks. ***Cons:*** if the broker is compromised then what will be the (negative) impact, bloom filter is subjected to high false positive rate. | [130] |
| BOC | Substation management | – | — | – | – | ***Pros:*** suggested black and white listing connections, inbound/ outbound logging and monitoring, and end-to-end secure framework. ***Cons:*** the authors did not proposed any solution. | [98] |

RT: radio takeover; CC : credential compromise; BOC: back office compromise; – : no proof of concepts/simulations;
**Security goals** – 1 : Availability; 2 : Integrity; 3 : Confidentiality; 4 : Authentication; 5 : Non-repudiation; 6: Authorization; 7 : Accountability;

services, there is an implicit assumption that an integrated traffic management unit demands a predefined criteria to discover potential anomalies. The criteria is never defined. In addition, the proposed scheme is a mathematical model, such that it may have several practical issues from the security service perspectives. For instance, encryption key management over VPNs is neither discussed nor implemented.

Based on publish/subscribe model, Duan et al. proposed a new framework that enables a secure and adequate access control in smart grid [130]. The proposed secure framework can be applied to many scenarios in SG metering network, e.g., event analysis, human machine interface, remote control, alarm control, etc. The authors utilized a fully homomorphic encryption and the publisher's private key to publish data securely and utilized the bloom-filter based encoded control policies to mitigate the credential compromise threats. With the attribute-based access control policies, the encrypted data can only be accessed by subscribers who are granted privileges. The framework includes three entities, subscriber, publisher, and broker. The scheme invokes, when a subscriber generates its query and sends it to the publisher. Upon receiving the query, the publisher translates the query to attribute-based access control policy and encrypts the query, and then sends it to the broker for verification. The framework requires each subscribing query must be authenticated via the broker before it granted access to the system credentials. The framework has been justified as a safeguard against two attacks, e.g., MITM attack and spoofing attack.

Indeed, the framework may provide security against the credential compromise attacks. Nevertheless, the framework does not account the (negative) impact of the framework in smart grid domain if the broker is compromised. The broker always needs to be online otherwise the framework would not be useful in practice. Moreover, a bloom filter is typically subjected to high false positive rate that may cause encoded policies to be forwarded unnecessarily.

**Back office compromise mitigations**: Recently, back office has been compromised using the potential malware, e.g., BlackEnergy, as shown in [55], [98]. Such attack could affect the end-user data and normal back office operations in SG metering networks, e.g., billing, credit rating, and so on [131].

In order to mitigate back office threats in SG, Khan et al. [98] suggested protection strategies against the back office compromise attacks with a particular focus on the BlackEnergy malware, as follows. (i) *Black and white listing connections*: In this, the external Internet Protocol (IP) addresses can be listed as a black-list (i.e., untrusted source) and white-list (i.e., trusted source). Essentially, it is not possible to make the black-list for those of unforeseen future updates of malware. However, the white-list of trusted and reliable destination can be managed, specially for the dedicated smart meters, field devices, data concentrators, and control centers, etc. (ii) *Inbound/outbound logging and monitoring*: As packets are transmitted and received using bi-directional communication, inbound/outbound packet monitoring and logging is possible in SMI for each entity, e.g., smart meter, data concentrator, field device, and control center. (iii) *End-to-end security mechanisms*: To prevent the SG metering systems from such malware, an end-to-end security mechanism may be an effective solution without including the key distribution centers.

***Summary***: In Table VIII, we summarize all the proposed countermeasures for the radio takeover [128] [96], credential compromise [130] [97], and back office compromise [98] in the terms of applications, communication mode (i.e., wireless/wired), involved entities, test-bed/simulation, security and privacy goals, and descriptions with pros and cons.

***Lessons Learned***: We discuss the lessons learned while reviewing the state of the art schemes. The aforementioned proposals are the imperative efforts as they can deal with the radio takeover, credential compromise and back office

compromise threats. However, the cons can have tremendous negative impacts on legitimate entities and this (negative) impact should be further examined.

*Radio takeover mitigations* – In [128], the authors proposed to establish a secured connection between a SM and NAN gateway by employing the openSSL protocol. In 2018, Guido Vranken reported a security issue in the key establishment in the TLS handshake, which uses Diffie-Hellman's based ciphersuite. During the handshake process, an attacker can make use of a malicious server to send a large prime number to the client device over the public (i.e., wireless/wired) network, as shown in [132]. This large prime may induce the client to spend an immoderately long period of time establishing a secret key for such large prime numbers. As a consequence, this immoderately long period could be exploited in a DoS attack at the client. Considering the cyber attacks on the Ukrainian power distribution, such very large prime value can be alarming, and/or be a potential target for an attacker if he/she takes over on radio communications. Therefore, a careful design of security scheme is still paramount. In contrast, Vaidya et al.'s scheme [96] provides security to control command but requires high communicational and computational costs.

*Credential compromise mitigations* – Approaches such as cloud-centric collaborative security service architecture did not discuss *how* and *what* policies should be defined to detect the anomalies and *how* to manage the keys for VPNs. In [130], indeed the bloom filter based encoded control policies can provide protection from credential compromise threats. However, in real practice, a bloom filter is generally subjected to (high) false positive rate that may lead encoded policies to be forwarded unnecessarily to, e.g, human machine interface, acquisition and estimation systems.

*Back office compromise mitigations* – Khan et al. suggested many ways to mitigate back office compromise attacks for real-time controlling and monitoring in SG [98]. Few of the mitigation mechanisms are: black and white listing, and inbound/outbound monitoring. These solutions can be applied to SG metering network, but it is hard to discuss the practicality and lessons learned of the suggested countermeasures as they are not implemented in the real world SG scenarios.

**Network barge-in by unknown mitigations**: In practice, the entities in the smart grid will exchange data over wireless mesh network in single-hop or multi-hop manner [110], [111]. Routing and message forwarding, therefore, are paramount services for end-to-end communications in smart metering, system monitoring and controlling, etc. As discussed in the attack taxonomy (i.e., Network/routing barge-in by unknown), an ill-intention adversary can mount several DoS attacks on the routing path. For example, malicious routing information/node can be injected/planted into the routing path of a network (such as, a puppet attack). As a consequence, inconsistencies in the SM network operations may occur. However, numerous schemes have been presented to improve routing security in smart grid [99], [133]–[141], as shown in Table IX.

There are proposals for wireless mesh networking in AMI networks that targeted on NAN applications. For example, Saputro-Akkaya proposed a secure piggybacking-based address resolution protocol (ARP) in [99]. The protocol utilized for IEEE 802.11s-based AMI network. The work addressed potential flooding issues in the ARP and proposed an efficient mechanism to solve those issues. The authors specifically utilized two types of packets: (i) proactive path request (PREQ) packet, and (ii) path reply (PREP) packet in AMI network. Mesh path is enabled via the path discovery protocol, which is defined by a default and mandatory hybrid wireless mesh-routing protocol (HWMP). The idea of this scheme is to piggyback the ARP packets (i.e., PREQ and PREP) while the route is being searched in the context of AMI. As the authors mentioned during the process of piggybacking of the ARP packets, it is very likely that a PREQ packet may be exposed to the possible ARP cache poisoning attacks. To overcome this attack, the authors computed a signature (i.e., elliptic curve digital signature algorithm (ECDSA)) to each piggybacked packet to authenticate the messages. However, the use of per-piggybacked packet cryptographic signature induced overhead to an intermediate router, when it is receiving several thousands of PREQ request from the smart meters in the meter local area network (MLAN).

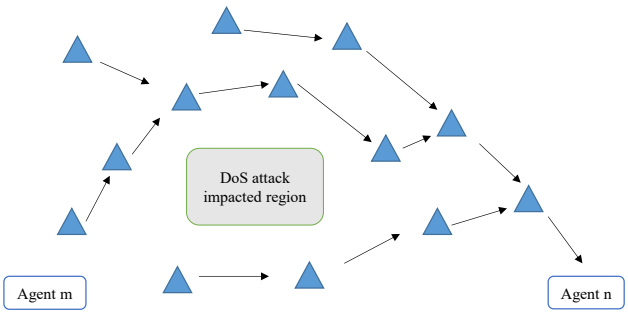

Fig. 9. Data flocking – bypassing DoS region in multiphop routing [143].

A secure scalable routing and data aggregation (SRDA) approach has been evaluated for wireless meter network by Wan et al. [133]. To determine the best routing path, the authors first introduced the inter-domain proxy and intra-domain proxy concepts. The inter-domain proxy is a smart meter that aggregates data between the different MLAN. Whereas, the intra-domain proxy that collects meter data within the MLAN. The identity-based cryptography (IBC) mechanism is being used (for wireless smart meter) to issue and update the routing information in a secure manner. The trusted public key generator (PKG) is employed to generate system parameters for the SRDA. The proxy re-encryption mechanism is designed to preserve data privacy. Although the authors claimed that a software-defined network based secure architecture has been utilized for securing routing, there is a lack of details about the proposed SRDA. For instance, it is not described how IBC is being implied on the control and data planes of SDN architecture in the SRDA [133]

In another work [134], Wei-Kundur described a resilient multicast routing called "GOAliE" for smart grid applications. The approach utilized publish—subscribe paradigm and flocking theory where a phasor measurement unit (PMU) message-flock traverses from agent $m$ to $n$ in multihop manner while bypassing DoS region, as shown in Fig. 9. To bypass DoS impacted region, the authors employed agent-interaction

TABLE IX
SYSTEM LEVEL MITIGATION APPROACHES FOR NETWORK BARGE-IN BY UNKNOWN IN SG METERING NETWORKS

| Ref. | Comm. mode | Involved entities | Routing metrics | Routing mode | Sec. & Pri Goals | Descriptions |
|---|---|---|---|---|---|---|
| [99] | 802.11s wireless mesh | SM, gateway | PDR, E2ED, throughput | multi-path | 2, 4 | ***Pros:*** addressed issues of ARP flooding; proposed secure ARP scheme; utilized piggybacking concepts; three-way handshake is required; and added signature to each packet; and performed integrity and authentication for PREQ and PREP; secure against spoofing attack and MITM attack. ***Cons:*** overall high communication overhead for resource-hungry SM. |
| [133] | Wireless | SM, data concentrator | scalability, EE | unspecified | 3,4,5 | ***Pros***: a secure routing and data aggregation approach; presented the identifier-based cryptography mechanism; SDN based secure architecture; scalable and energy-efficient; and addressed confidentiality, mutual authentication, non-repudiation and secure against MITM. ***Cons:*** lack of security details on data and control planes in SDN. |
| [134] | 802.16 WiMax | – | PDR, LTC | multi-hop | 1 | ***Pros:*** resilient multicast routing for smart grid applications; resilient distributed multicast data delivery; and protection from DoS attack. ***Cons:*** the approach is not practical if synchronous data needs to be delivered within time [142]. |
| [135] | 802.15.4 wireless | SM, consumer, distribution | LTC, REL, overhead | multi-path | unspecified | ***Pros:*** suggested SPEED routing protocols; evaluated communication performances, i.e., latency, reliability, and overhead. ***Cons:*** security is out of scope for such critical smart grids. |
| [135] | 802.15.4 wireless | SM consumer, distribution | LTC, REL, overhead | multi-path | unspecified | ***Pros:*** discussed MMSPEED routing protocols; communication latency, reliability and overhead are evaluated. ***Cons:*** security is out of scope for such critical smart grids. |
| [140] | Wireless | SM, data concentrator, utility | packet loss | unspecified | 4 | ***Pros:*** investigated sinkhole attack; Enhanced RPL routing; node-to-node authentication; detected key-compromising attacks; utilized data mining. ***Cons:*** enhanced RPL does incur (high) packet budget; central database always needs to be online; lack of security analysis. |
| [141] | Wireless | – | $C_A$, $C_C$, $C_I$ | single-path multi-path | 1 | ***Pros:*** presented vulnerability assessment model; mitigating link insecurities, capitalized SDN framework. ***Cons:*** more complex to configure in cases of negative edge. |

PDR: packet delivery ratio; E2ED: end-to-end delay; LTC: latency; REL: reliability; EE: energy-efficiency; $C_A$: cost-on-availability; $C_I$: cost-on-integrity; $C_C$: cost-on-confidentiality; MITM : man-in-the-middle;
**Security and Privacy goals** – 1 : Availability; 2 : Integrity; 3 : Confidentiality; 4 : Authentication; 5 : Non-repudiation; 6: Authorization; 7 : Accountability; 8 : Anonymity; 9 : Unlinkability; 10 : Undetectability; 11 : Unobservability; 12 : Pseudonymity

based heuristic principles, as follows: flock centering, seeking goal, velocity matching, obstacle evasion, collision avoidance and behavioral transitions. In GOAliE, the authors considered traditional routing performance measurements such as, end-to-end latency budget, buffer overflow and packet deliver ratio. Through simulation, the authors demonstrated how the GOAliE utilizes the effective multicast routing algorithms to promote resilience in faulted power systems in the presence DoS attack on communication infrastructure. However, Masoumiyan et al. pointed out that the GOAliE strategy does not fit to synchronous data delivery, in [142].

A few proposals focus on low-cost wireless sensor network (WSN) in smart grid networks. For instance, Sahin et al. presented and evaluated quality of service distinguishing in two routing protocols (i.e., single path routing and multi path routing) in [135]. The authors assumed several numbers of low-cost sensor nodes are deployed from generation to consumer side. These nodes can enable various applications in smart grid, e.g., metering, monitoring and controlling, and dynamic pricing, energy management, and can communicate via single or multi hop networks. Sahin et al. highlighted performance evaluation for two routing protocols (SPEED and MMSPEED) considering communication latency, reliability and overhead. In addition, the authors pointed out that the secure routing is highly required in a SG domain, but lack of discussion on the possible solutions.

In SMI, the smart meters and control center communicate through the sink nodes. Following the routing threats, an attacker can take control over these sink nodes and use them to send malicious commands, for instance to turn off the power of the consumer premises. In [140], Taylor-Johnson developed secure communications against sinkhole attacks in smart grid metering networks. To set up a communication link over the low-power mesh network, the scheme uses the routing protocol for low-power and lossy networks (RPL) protocol, which is a routing protocol for the low-power and lossy networks. The RPL is based on distance vector routing protocol. Nevertheless, to mitigate sinkhole attack, the authors proposed modification in RPL addressing by utilizing encrypted authentication at each node-to-node link. In addition, the scheme also detected whether any key is compromised by using data mining techniques. To achieve encrypted authentication in RPL, the centralized key database, utility company key setup, and a static map were used. Note that the authors did not provide much details on the system setup. Nevertheless, each smart meter first generates own keys (i.e., public and privacy) on the system startup, and then inserts the key to the map, where the sink node could access them from the central database. The significant drawback is that the central database always needs to be online and could be the target of attacks. Moreover, lack of security analysis could be a major concern for usability of the proposed protocol.

Hammad et al. [141] enhanced communication security in smart grid by employing software defined network and achieved satisfactory quality of service by mitigating insecure communication links. The scheme takes advantage of three

different encryptions, where link security is attributed mainly built on security strength of the encryption algorithm. The authors defined (traditional) security metrics based on CIA (confidentiality, integrity and availability) threat model, as follows: $C_A$, $C_I$ and $C_C$ as the cost-on-availability, cost-on-integrity and cost-on-confidentiality, respectively. Here, cost-on means the weight that is scaling the individual attribute, which depends on the impact of considered threat model. However, selecting the optimal threshold value could be a challenge for the weighted-value since the trust decision is typically not defined in the scheme. Moreover, the scheme did not discuss the case of negative edges in the network. In another research [144], Mishra et al. discussed the packet-based attacks and studied the optimal inspection points (OIP) problem. In this paper, OIP finds many points for malicious attack detection in the smart grid applications, especially where each single packet or the network traffic is required to be inspected deeply. To achieve this, the authors introduced the concept of a set of OIPs that will perform the deep packet inspection (DPI) on each routing packet before sending the packet to the control center. However, such deep packet inspections may reveal the privacy of the consumption uses. More surveys on routing protocols in smart grid can be found in [110], [111].

***Summary:*** In SG metering networks, most of the schemes discuss a verity of attacks, e.g., secure to packet flooding attack [99], resilient to MITM attack [133], resilient to DoS attack [134], and sinkhole and spoofing attacks [140]. These proposed solutions mainly use two types of countermeasures, such as, cryptographic-based (e.g., [99], [133], [140], [141]) and networking-based (e.g., [134], [144]).

***Lessons Learned***: A smart meter data travels through multihop communications in the SM domain. Therefore, a route maintenance is important in SG metering network to enable the self-healing of faults. A routing protocol should be integrated with a security and privacy design in order to mitigate the public SG metering communication paths. Note that the cryptography based techniques ( [99], [133], [140], [141]) can protect from impersonation, masquerade, MITM, and integrity attacks. However, these techniques does not appear effective to detect other malicious attacks or malfunction due to the packet modification. Therefore, one of lesson is that a malfunction leads to many other attacks, e.g., sinkhole, packet forwarding, warmhole, etc. Second, the aforementioned proposed schemes come at the high cost of signature verification (for each packet). Moreover, following the schemes proposed in [142], [134] can lead to data synchronous problems in the smart grid domain. Therefore, both the schemes may not be practical for the energy feedback purposes in the load management applications.

Third, considering a packet-based detection approach, as proposed in [144], where each packet has to be scanned to detect the existence of potential attacks, if any, in the SG network. Scrutinizing each packet increases the time-consuming, thereby induced significant delays in throughputs. Moreover, such packet-based deep scanning on fine-grain energy consumption data may rise privacy issues. Thus, there is a critical need to rethink to design secure routing protocols with high performance evaluations from the real-time SG metering network viewpoint.

Finally, the privacy risks can also be emanated due to the data routing, which is typically done in a "store-carry-and-forward" mode. Nevertheless, majority of the proposed schemes have been neither designed nor implemented with a focus of privacy-aware routing in SMI that can mitigate the privacy risk in "store-carry-and-forward " mode. Such privacy violation can give the attacker unauthorized access to smart meter's requests, if the adversary is topologically close to a SM. We therefore believe that any communication (whether single-hop or multi-hop) paradigm used – a SG metering network must be supported with the possible aspects of privacy goals as pointed out in the Section IV.C (cf., privacy goals).

**Denial of Service attack mitigations**: As shown in Fig. 7, the denial of service (DoS) threats aim for malicious activities that weaken the operational performance from its anticipated operations, at various level of the network. In smart grid network, DoS threat could be even more disruptive as industrial control and automation systems are main driving forces for the grid automation. For instance, field devices (e.g., sensors, meters, phasor measurement units) are main components in the smart grid networks. To form a network, these devices usually utilized wireless mesh technology for exchanging information between the entities. However, a wireless mesh network is prone to routing-based DoS attacks as demonstrated in [59].

To mitigate DoS attack, Lee et al. [145] described and simulated a new mechanism to detect and monitor the misbehaviour of neighbouring mesh devices in a smart meter mesh network. The main idea of the scheme is to introduce a head node, which is similar to the data concentrator at the neighbourhood area network (NAN). The scheme suggested that a new device (smart meter (IEEE 802.11)) who intends to join the network, should be registered with the data concentrator. Upon registration, the identity of new node identity and location (i.e., X and Y coordinates) are verified and then a fresh session key is established among the head node and new node. Here, the head node is the local coordinator that contains the location information (in node information table) of the wireless mesh nodes (e.g., end-user smart meters). However, to monitor the misbehavior: (i) each node (e.g., A) not only continuously monitor its (two-hop) neighbouring nodes, but it counts incoming/outgoing packets from/to the monitoring nodes. (ii) Based on the pre-defined threshold value, the node A assures whether the incoming/outgoing messages are within the pre-defined value or not. If the determined value exceeds than the threshold value, then the node is compromised. To check the performance of the proposed scheme, a dynamic source routing (DSR) protocol is used and simulation results demonstrated that the routing misbehavior detection can be achieved by 97%.

However, the DSR protocol has inherent limitation that the packet size grows with route length to the source routing. The other major challenge is determining the threshold value. To deal with this, the authors proposed to employ automatic threshold revision process, which is based on the pre-defined time. This scheme may have some vulnerabilities. For instance, it assumed that if an attacker exploits the pre-defined

time based threshold value, then he/she can execute the attacks on automatic threshold revision process, which may increase significant packet loss rate.

Hu-Gharavi [146] suggested and simulated a new security (i.e., random key distribution) approach in wireless mesh network. To verify the mesh node (i.e., smart meter) authenticity, the authors utilized built-in (i.e., IEEE 802.11s) authentication protocol called "simultaneous authentication of equals (SAE)". Here, the authentication procedure is influenced by a single pre-shared key (and/or master key), which is known among other mesh nodes. However, a single discloser of key can easily violate security of the network, and can allow an unauthorized node to enter into the network (recall credential compromised in Section V.B). Therefore, the authors suggested a new countermeasure called "efficient mesh security association (EMSA)". The EMSA uses a key hierarchy to achieve as similar secure authentication as in the SAE. Note that since both the protocols (SAE and EMSA) are based on 4-way handshaking, DoS attacks can jeopardize the network. To mitigate DoS attacks, the authors proposed dynamic key distribution and key refreshment strategy. With the proposed strategy, the keys (including master session key) can be updated regularly (e.g., a week, a month or six months) before the master key expiration. The main shortcoming of the Hu-Gharavi's scheme is that a compromised node still can participate to the network until the master is valid for that particular duration. Moreover, Toor-Ma [147] pointed out that the scheme proposed in [146] is still vulnerable to the replay attack in EMSA.

Wireless communication networks for the smart metering network are potentially exposed to jamming threats. Several literature pointed out that jamming attacks pose constant DoS threat to smart grid applications [148], [102].

To mitigate jamming issues in smart gird applications (i.e., home metering and substation automation), Lu et al. [148] investigated two different types of jamming-resilient communication modes: (i) *Coordinated* link – two entities (i.e., a sender node and a receiver node) should possess a pre-shared unique secret key (e.g., code-frequency channel assignment) and this key should not be revealed to adversary. Note that, a sender is an intelligent electronic device (IED) that communicates with the gateway (i.e., receiver node) over the wireless communication. (ii) *Uncoordinated* link – in this link, the transmitter and receiver must select a frequency-code channel randomly to send/receive a packet. The message can only be received if both the sender and receiver have same channel, otherwise the message will be invalid. In addition, the authors evaluated the worst-case performance for jamming process and proposed a new system called "transmitting adaptive camouflage traffic (TACT)" system. The TACT consists of three types of traffics: (i) *routine traffic* for power monitoring and controlling purpose, (ii) *probing traffic* for measuring network performance, and (iii) *camouglage traffic* to balance the traffic load from the sender node to receiver node. Moreover, the authors suggested the implementation of the proposed TACT to every node, since it measures the delivery results of probing packets to adapt the number of camouflage packets in the network. Each camouflage packet is sent over a randomly chosen frequency/code channel. The system hence attains a trade-off between the message delay and the message delivery ratio. The main drawback of the TACT is the efficiency relies on homogeneous traffic rate of the all nodes, which however, may not be assured if there exists heterogeneous traffic rates.

In another research, Premarathne et al. [151] designed a secure and reliable cognitive radio (CR) sensor network in SG. The authors proposed to use a CR sensor, which is installed within a smart meter and it communicates over CR network to transmit the HAN data (i.e., consumption usages) to the field or neighbourhood area network. This research utilized a machine learning-based physical unclonable function (PUF) that generates secret keys and add noise to the keys. However, the noise needs correct error detection techniques that demand high computational resources, which are stringent in CR sensors. More research on CR in the SG can be found in [104], [109].

To achieve transport layer security, another so-called (java-based) open source framework (jOSEF) proposed in [149] with proof-of-simulation. The jOSEF provides an end-to-end secure link between the smart meter and the external market participant (EMP) in smart grid. This work mainly utilized the transport layer protocol based security mechanism that required user authentication of the clients against the smart meter gateway (SMGW). In the proposed framework, the SMGW is provided with cryptographic functions, e.g., public-private key generation module and digital certificates, and performed end-to-end transport layer security (TLS) between the SMGW and EMP. However, the jOSEF framework has the following drawbacks: (i) it does not support remote administration; (ii) it does not provide protection to the meter data that can raise privacy issues; and (iii) the jOSEF is implemented with only few security properties, such as password-based user authentication. Moreover, the paper does not provide how the security features have been covered and/or implemented.

In the same vein, Khaled et al. [150], addressed a study about secure (TCP/IP, i.e., transmission control protocol and internet protocol) communication in the power substation that supports smart metering communications. The authors have studied a substation automation that can remotely monitor and control the power distribution components via the smart meters. The authors specified a framework, namely, manufacturing messaging specification protocol (MMSP). The MMSP is utilized to communicate real-world data, and to control information between several devices in the SG. The MMSP traffic mainly secured at the application and transport layers via utilizing the X.509 certificates. Moreover, the authors analysed several cipher suite combinations, including key exchange, encryption and hashing, and their memory overhead, within the intra-network scenario. The security goals include data confidentiality, integrity violation detection, and packet-level validation for the SCADA system. Considering [107], TCP with TLS is vulnerable to attack, where an attacker can intercept the sequence counter (SC) because the SC in TCP evenly increment with each fixed data transfer. This vulnerability gives enough room to an attacker to inject the false data to a substation network.

***Summary***: In the SG metering networks, generally DoS at-

TABLE X
ROBUSTNESS TO DENIAL-OF-SERVICES IN SMART GRID METERING NETWORKS

| Ref. | Comm. wireless/ wire-line | Involve entities | Testbed/ Simulation | Descriptions |
|---|---|---|---|---|
| [145] | 802.11s wireless mesh | SM, NAN | Simulation | ***Pros:*** protection from DoS attack based on routing misbehavior; proposed neighbour nodes monitoring method; and used dynamic source routing between SM and data concentrator. ***Cons:*** packet size grows with route length due to the source routing. |
| [146] | 802.11s wireless mesh | SM, NAN | Simulation | ***Pros:*** identified SAE and EMSA DoS vulnerabilities; proposed a periodic key refreshment and distribution strategy for DoS attack; and employed tree-based routing. ***Cons:*** the proposed strategy still leads to the replay attack in EMSA, i.e., further leading to the DoS attacks, as shown in [147]. |
| [148] | 802.11s/ wireless | – | Simulation | ***Pros:*** proposed a transmitting adaptive camouflage traffic (TACT) system; mitigating jamming and DoS attacks ***Cons:*** efficiency relies on homogeneous traffic rate, which is not always practical. |
| [149] | unspecified | SM, NAN | Testbed | ***Pros:*** a java based open source smart meter gateway experimental framework; provide end-to-end link; transport layer based security mechanism; and password-based authentication ***Cons:*** implements only a limited subset security functionalities, lack of security analysis. |
| [150] | wireless | SM, NAN | Simulation | ***Pros***: a secure communication in the substation; IEC 61850 specifications; security is provided by TLS; and provide confidentiality, tamper detection, and message-level authentication. |

SAE: simultaneous authentication of equals; EMSA: efficient mesh security associatation; – : unspecified

tacks target the availability of system. Such attacks can disrupt the network or cause delay in packet delivery, jamming/block messages (e.g., high priority control commands), or sometimes misdirect the whole system from top to down and vice versa. Table X summarizes how existing approaches can detect and mitigate DoS attacks.

***Lessons Learned***: The lessons learned from DoS countermeasures is that DoS threats should be addressed at the intrinsic level, as follows. (i) Schemes, such as [145], detects the misbehaviour of the neighbouring nodes where each node is regarded as a watchdog for the two-hop nodes. This watchdog node counts incoming and outgoing packets from the neighbouring nodes, which therefore multiplexes data in the network. Consequently, each watchdog may have storage issues. Moreover, the authors utilized the pre-defined time-based threshold value, which may have different timing classes, e.g., millisecond, seconds, minutes, and so on. Therefore, we believe that to select a particular time class is challenging, since it is usually based on the SG metering applications, as shown in Table IV.

(ii) In order to mitigate the jamming based DoS attack, Lu et al proposed the TACT that measures the delivery of probing packets to adjust the camouflage packets in the network [148]. The TACT also has issues of heterogeneous traffic rates that cannot be considered as the robust solution. This is still an idea to solve the jamming issues. There is a need to do more in-depth analysis considering the heterogeneous traffic rates in real SG metering networks.

(iii) Other approaches include TLS based solutions to mitigate the DoS attacks. For instance, in [149], the jOSEF is proposed as an end-to-end TLS security suite between the smart meter gateway and the external market participant, with proof-of-simulations. Similarly, a TLS-based approach has been studied for the IEC 61850 based substation in [150]. However, Wang et al. demonstrated that if an adversary can inject false data to the plain TCP stream then it can lead to DoS attack on a TLS stream [107]. In addition, a vulnerability reported in TLS-based handshake also leads to DoS attack, as shown in [132]. As the SG metering networks are complex engineering marvels, and are distributed in nature, there is an immense need to investigate the potential impacts and countermeasures of DoS attacks in each part of the networks.

## IX. THEFT OF SERVICES COUNTERMEASURES IN SG METERING NETWORK

**Mitigation to smart meter cloning**: Recall the threat taxonomy – by cloning a smart meter, an attacker can change the original meter or radio channel identity (ID) with the duplicate copy in order to make the frauds on the services provided by the smart grid.

To mitigate such smart meter cloning, Mustapa et al. [152] proposed a hardware based authentication that utilized the challenge-response mechanism. The research suggested that a smart meter is integrated with the unique ring oscillator physically unclonable function (ROPUF) on the integrated circuit (IC), which is known as immutable. More precisely, the small randomness can take place at ICs manufacturing process, and therefore PUF can use the small randomness to produce a number of binary IDs. These IDs are typically unique for every Silicon chip, and cannot be easily modeled.

Each ROPUF needs to be registered at the utility company (UC) before the deployment. During the registration, for each smart meter, the UC records all the hamming code parity bits pairs along with its challenges from each ROPUF IC. Here the hamming code parity bits pairs are utilized to generate the authentication keys and to verify the ROPUF responses at the UC. The scheme can provide different levels of authentication, i.e., L1 - L5, utilizing various lengths of parity bits, i.e., 64, 128, 256, 512, 1024 bits, respectively. To set up a secure communication, the UC sends a challenge request to the SM,

which then replies with a positive response to the UC. If the response is negative then the smart meter will be given two more chances to produce a positive response. If the smart meter still fails, the UC broadcasts a BLOCK message to all the devices in the entire network to block communication from that particular smart meter. The scheme achieves confidentiality and authentication, and secure against the impersonation attack. Moreover, the authors have simulated their scheme, i.e., (i) the authentication time, and (ii) the storage required for (hamming code parity bits pairs and challenge) for 50 years of lifespan. In addition, a machine leaning based algorithm (e.g., support vector machine) can detect if there exists any meter that is modeled by an attacker.

However, the scheme may have storage issues – if there are millions of smart meters in a city/town then the UC needs huge storage (especially for L3 - L5).

To avoid illegal cloning and tampering, Zhou proposed another interesting research, i.e., secure SM sealing based on radio frequency (RF) tag in [113]. In the scheme, each SM is assumed to be sealed with the RFID tag to prevent illegal frauds in the meter (e.g., manipulating readings). To deter possible adversaries, the author designed a new authentication protocol where a SM seal/tag sends random number $(S_{RN})$ to the reader. Upon receiving the random number, the reader generates an encrypted token $(ET)$, which includes a secure key $(S_{Key})$, and sends $ET$ and $S_{RN}$ to the SM tag. The SM now verifies $S_{RN}$, and decrypts $ET$ in order to obtain the key $(S_{Key})$. The scheme also provides message integrity and confidentiality to the wireless messages.

Indeed, such SM sealing can protect the cloning. However, the author did not provide the security and performance analysis on the smart meter sealing. Moreover, the RF sealing may be an expensive solution, and may require back-end database management, which is not discussed in the paper.

**Mitigation to smart meter compromise**: An attacker can compromise the smart meter to make energy theft. More precisely, the energy companies are approximately losing millions of dollars annually due to energy theft [114].

Based on the mathematical analysis, Han-Xiao proposed a non-technical loss fraud detection (NFD) [114]. The NFD utilized Lagrange polynomial interpolation model to detect the behaviour of multiple compromised meters and multiple adversaries. The NFD needs an additional meter (called observer meter) to be deployed to record the energy supplied and reported to/by the smart meters (e.g., $n$ meters) during time $Ti$. The mathematical model can work when all the smart meters have the same accuracy and/or consumption behaviour, which is not always practical. For instance, in a real-time scenario where each meter may have different accuracy at different timings. Moreover, the scheme proposed in [114] requires additional observer meters, which may add significant deployment and maintenance costs to the utility companies. Similarly, Yip et al. proposed another mathematical model to detect defective smart meters and energy theft in [153]. However, this scheme can detect the tampered smart meters but cannot conceal end-user's privacy.

Based on the cryptographic approach, Ho et al. [154] proposed two security schemes against the smart meter compromise attack in smart grid. In their mitigations, the authors proposed to use of signcryption algorithm that achieves weak confidentiality and strong confidentiality in the protocol I and protocol II, respectively. With the help of trusted authority, all the entities (smart meter, data collector unit (DCU), and server) compute their public and private keys, and signing and verification keys. Then each smart meter is registered (securely) with the server. In protocol I, for each data transmission, a smart meter computes hashing and a signcryption message on the meter data, and then sends it to the server via the DCU. Upon receiving the message, the server validates the message by comparing its hashing and verifying the correctness of signcryption. If the server receives numbers of messages then it delegates messages to the DCU. After receiving messages, the DCU verifies the messages, indicates the invalid signature and reports the invalid signatures (if any) to the server. Note that the invalid signatures belong to the compromised smart meters. Finally, the server discards the meter data corresponding to all invalid signatures. In protocol II, the authors mainly focused on the demand response use-case and provided an additional confidentiality service by means of Pallier encryption.

Ho et al. provided a detailed security analysis on the message authentication, confidentiality, and robustness to smart meter compromise attack. However, the scheme did not support data aggregation in protocol I and protocol II, as pointed out in [155]. Moreover, the protocol II may incurred significant communication overhead.

**Mitigation to location migration**: As shown in the threat taxonomy, an attacker may change the smart meter location with a potential to fake measured energy consumptions to lower the bills [157].

Parvez et al. [156] proposed a location-aware key management system in the AMI. The authors introduced an interesting idea, i.e., a location aware encryption scheme where a smart meter utilized a secret key that is associated with its own location coordinates, as shown in Fig. 10. Notably, a TTP manages a codebook that has a pool of encryption keys (with indexes) and each key is associated with the location points (X,Y) of the geo-location. For each data transmission, the smart meter first randomly picks a key index, encrypts it with the node ID and then sends the encrypted text to the TTP. Upon receiving the message, the TTP verifies the node and then sends the randomly chosen key index to the control center to decrypt the data. If an attacker or consumer changes the location of a smart meter then the data cannot be encrypted/decrypted.

The scheme can mitigate the location migration problems, but each meter needs to maintain a table to record the locations of its neighbouring smart meters, which may raise privacy issues. Moreover, it required the TTP always to be online, which may not be practical, e.g., due to lack of the Internet connectivity in remote areas.

In another research, Viswanatham et al. [115] proposed a region-based group key management (KM) scheme where the smart meter location migration is handled in a secure way. The KM scheme is a self-enforceable scheme, since the keys can be computed from the hierarchical levels. The

TABLE XI
THEFT OF SERVICE MITIGATION APPROACHES IN SMART GRID METERING NETWORKS

| Threat | Applications | Wireless/ Wired | Involved entities | Test-bed/ Simulation | Sec. & Pri. Goals | Descriptions | Ref. |
|---|---|---|---|---|---|---|---|
| SMC | Data management | Wireless | Utility, SM | Simulation | 2,3,4,5 | ***Pros:*** hardware based authentication; L1 - L5 authentication levels; provides message confidentiality, integrity, and authentication between smart meter and utility company; safeguard to cloning, impersonating and spoofing attacks; SVM detects whether unauthorized meter exists. ***Cons:*** the scheme may have storage issues. | [152] |
| SMC | Data management | RFID | SM-tag, reader | – | 3,4,5 | ***Pros:*** RFID based smart meter sealing; provides integrity and confidentiality protection capabilities, avoids unauthorized read, write, tampering and recognition. ***Cons:*** lack of security and performance analysis, RF sealing may be an expensive solution. | [113] |
| MC | Data management | unspecified | Utility, SM | Simulation | – | ***Pros:*** proposed a mathematical model to detect the energy frauds, The scheme required an additional observer meter; Observer meter detects the frauds. ***Cons:*** additional cost for the observer meter, the scheme cannot preserve the privacy. | [114] |
| MC | Data & load management | Wireless | meter, data collector, head-end | Simulation | 2,3,4 | ***Pros:*** two schemes against smart meter compromise; Signcryption achieves weak confidentiality in protocol I; In protocol II mainly focused on demand-response program, provides strong confidentiality. ***Cons:*** did not support data aggregation in protocol I and protocol II, as pointed out in [155], protocol II incurs communication overhead. | [154] |
| SLM | Data management | Wireless mesh network | Meter, utility | Simulation | 3 | ***Pros:*** location-aware key management system; TTP manages a code-book; provides message confidentiality. ***Cons:*** TTP always to be online; privacy issues. | [156] |
| SLM | Data management | Wireless | Meter, DSS, TU, MPS | Simulation | 3,4 | ***Pros:*** proposed a region-based group key management; self-enforceable scheme; . ***Cons:*** lack of security analysis; renewing key may be very expensive. | [115] |

SMC: smart meter cloning; MC : Meter compromise; SLM: smart meter location migration; DSS: distribution sub-station; TU : transmission unit; MPS : main power supply; – : no proof of concepts/simulations;
**Security and Privacy goals** – 1 : Availability; 2 : Integrity; 3 : Confidentiality; 4 : Authentication; 5 : Non-repudiation; 6: Authorization; 7 : Accountability; 8 : Anonymity; 9 : Unlinkability; 10 : Undetectability; 11 : Unobservability; 12 : Pseudonymity

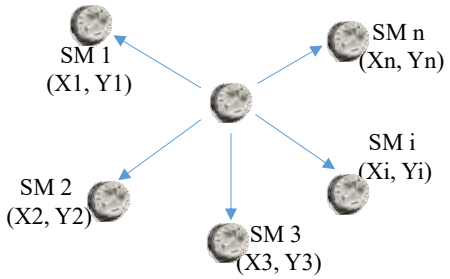


Fig. 10. Location of the smart meters (SMs) [156].

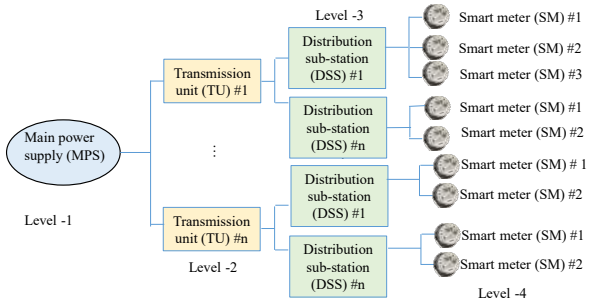


Fig. 11. Hierarchical network of smart grid [115].

authors assumed that a smart grid network can be divided into hierarchical network, e.g., main power supply (MPS), transmission unit (TU), distribution sub-station (DSS) and smart meter (SM). The MPS is main head-end level, the TU and DSS are intermediate levels, and the SM is end-node, as shown in Fig. 11. In a hierarchical network, the keys are distributed by the key distribution server (KDS), as follows. At level one – a group key (GK) is shared among all the entities under the MPS. At level two – another group key $(K_{TU_i})$ is shared between all the lower entities of the TU. In addition, the KDS also distributes an unique key $(K_S)$ to each smart meter. Now, each DSS and smart meter computes their shared key $(K_{KR})$, as $K_{KR} = f(K_S, ID)$. Here, ID is an identity of the smart meter, and $f$ is predefined random function, i.e., embedded in all entities. The authors then generated the DSS group key $(G_{DSS})$, as $(G_{DSS}) = H(K_{KR}||T)$. Here $T$ is the current time of the DSS, and $H$ is a hash function. Likewise, the TU group key $(G_{TU})$ is generated, as follows: $G_{TU} = H(G_{DSS}||r)$, where $r$ is a random number. Finally, the MPS group key $(G_{MPS})$ is derived as $(G_{MPS}) = H(G_{TU}||r)$.

In order to manage the smart meter location migration, the key renewing costs is expensive. For instance, assumed that a smart meter (M) wants to move from TU #1 to TU #2, then the group-keys need to be renewed at every level, i.e., DSS, TU and MSP levels. Therefore, the group key management becomes challenging, if the meters change locations frequently.

***Summary***: Table XI summarizes the mitigations to smart meter cloning [152], [113]; meter compromise [114], [154]; and meter location migration [156], [115], including their communication mode, involved entities, test-bed/simulation, security and privacy goals, and description with pros and cons. Each scheme is proposed to be a safeguard to theft of services in smart grid.

***Lessons Learned***: In SG metering network, smart meters feed data to a plethora of applications which provide different services, e.g., billing, monitoring, outage management, etc. These meters can be used as source of theft that presents a tough challenge for energy companies due to the fact that SMs can be cloned, compromised, and their location can be migrated. However, the disadvantage of the aforementioned proposed approaches can be significant on the involved entities. Hence, there is a need for further investigations to improve the security of such threats to services. For instance, *mitigation to smart meter cloning*: (i) In [152], as the authors suggested a hardware authentication mechanism in AMI. Nevertheless, one of the lessons is to design a tamper resistant IC that is resilient from all types of potential attacks (such as side channel attack) is challenging. Moreover, as the detection of modelled meter is based on the support vector machine (SVM), it requires a large volume of training data. Therefore, such detection scheme is leveraged without the real-time constraints, e.g., the cost of quality of training data. In [113], the RFID based smart meter sealing system requires back-end database to manage the tag, keys, etc. If this part is compromised then it may leak out SM tags data, encryption keys and other paramount information, such as IDs. Therefore, it is essential to strengthen the robust security of the back-end servers. In addition, the utility companies have to pay extra cost to install the sealing on the SM system. Therefore, who will bear such sealing costs can become the concern in the energy market.

*Mitigation to smart meter compromise*: The schemes [114] and [153] are based on the mathematical models that can detect the default meters and energy theft. These schemes are either depending on analysis of customer behaviour that needs a vast quantity of historical data or requiring many extra devices that are costly, e.g., observer meter. Since the proposed solutions are mathematical concepts, it is not clear which scheme can provide the best practical solution against such energy theft and/or compromised/default smart meters. Therefore, there is a critical requirement to make decision on the best solutions with their negative impact's analysis.

*Mitigation to smart meter location migration*: The proposed schemes for smart meter location migration are a necessary attempts to address location migration threats. As Parvez et al [156] proposed a location-aware key management system, it needs to manage a database that records the location of the neighbouring smart meters. Such database still raises the location privacy issues for neighbouring smart metes. Similarly, another research (i.e., [115]) proposed region-based group key management for smart meter migration/moving. However, renewing keys for (frequent) entering and leaving of smart meters cannot be practical for the entities, i.e., DSS, TU and MPS.

## X. Privacy/Confidentiality threats Countermeasures in SG Metering Network

**Mitigation to eavesdropping/interception**: Recall the threat taxonomy, an (unauthorized) eavesdropping on the wireless communication channels allows an attacker to drop, alter, replay the consumption usages to the utility companies. In addition, an attacker can draw the daily routine of an individual via interception and can lead the privacy threats. To mitigate such threats, several novel encryption and authentication approaches have been proposed, as follows.

**Encryption schemes**: It aims to achieve confidentiality/privacy and protect sensitive data among the smart grid components. Cryptographic algorithms make use of either *symmetric* and/or *asymmetric* or *homomorphic* or *altogether* to generate the ciphertext. Table XII summarises how encryption schemes are applied in various smart grid metering applications, involving entities, implementation mode, security and privacy goals, and descriptions (i.e., pros and cons). We reviewed the current state-of-the-art encryption schemes, especially considering symmetric encryption [158], [159]; asymmetric encryption [120], [160]–[162]; and homomorphic encryption [163]–[166].

*Symmetric cryptosystem (SC)*: In the SC, two entities or more utilized a shared secret key to enable a secure channel. Usually symmetric encryption requires approximately constant computational prices regardless of key sizes. A detailed benchmark on symmetric encryption schemes for the resource-hungry devices can be seen in [167]–[170].

To secure smart grid communication, Saxena-Grijalva [158] proposed a dynamic secrets and secret keys based scheme. The scheme mainly includes two entities, i.e., supervisory node (SN) and control node (CN). A supervisory node corresponds to a control center or a data aggregator node that collects consumption unit of the homes via the smart meters. The proposed scheme leverages on a pre-shared long-term string *(str)*, which is shared between each CN and SN. Whenever the CN wants to communicate to the SN, it generates a secure packet using *str* before the packet dissemination. In addition, it counts the successful delivery of every single packet transmitted over the wireless communication. Upon receiving the packet from the CN, the SN verifies and checks packet integrity, and then sends an acknowledgement *(ack)* to the CN. Once *ack* received successfully at the CN, both the nodes (i.e., CN and SN) can generate their dynamic secrets to establish secure communication.

The dynamic secret scheme reduces the cost of cryptography as only the hasing and XORing are required between the CN and SN. However, the scheme has not given enough attention to the SN. If it is compromised in a coherent way, many attacks can be mounted easily.

Liu et al. [159] suggested a secure mechanism called "dynamic secret-based encryption" (DSE) for securing the smart grid networks. DSE was proposed to establish a secure communication connection among the smart devices (i.e., SMs) and the control center (CC). The SM/sender and CC/receiver agreed on two hash functions to compress a threshold value of the one time frames (OTF) for the data link layer into the dynamic secret ($DS(k)$). The agreed key (i.e., $DS(k)$) is utilized for data encryption and decryption at the source and destination node, respectively. Moreover, the authors used XORing for encryption and decryption operations to reduce the computational cost, and claimed that their scheme can protect against information leaking and forging attacks. However, the link layer has inherent security issues, including distance,

interference, environmental factors, collisions, exhaustion, and unfairness that can lead to critical DoS threats, as shown in the request for comments (RFC) 6272 [171].

*Asymmetric cryptosystem*: *Asymmetric* cryptography applies two different keys, i.e., private key and public key. The public key utilized for encryption and can be published publicly. One of the earlier standards is the Rivest, Shamir and Adleman (RSA) encryption, typically using key of 1024 bits or greater. Another approach is ECC, utilizing algebraic geometry-based elliptic curves. ECC uses smaller key (160-bits) for the same level of security as of the RSA (1024 bits). Nevertheless, asymmetric cryptography requires more computational cost than the symmetric cryptosystem [24]. A comprehensive comparisons between asymmetric and symmetric schemes can be checked in [24], [175], [176].

Blending a number of asymmetric cryptographic techniques (e.g., identity-committable signature, zero-knowledge proof, and partially blind signature), Gong et al. [120] proposed a privacy-preserving incentive-based DR program. In the scheme, a smart meter receives identity-committable signature (ICS) and registration token from the demand-response program (DRP), at registration time. In addition, the smart meter also receives a pseudonym, which provides identity privacy to the smart meter and customer. In order to send consumptions report at time $(t)$, a smart meter collects consumption data, computes an ICS signature and attaches the pseudonym to the message. Then it sends entire message to the DRP. Upon receiving the message, the DRP verifies its validity. If the condition is true then it stores the consumption data, otherwise discards the report. The individual metering data is signed in such a way that data can be authenticated without disclosing the personal identity of the signer. Nevertheless, it requires high computational cost in registration and settlement phase due to exponentiation operations.

Based on public key cryptography (i.e., RSA), a different privacy-enhanced data aggregation scheme against the internal attacker is investigated by Fan et al. [160]. The idea is straight forward – an user $(U_i)$ receives smart meter reading (i.e., $M_i$), encrypts the report, and finally sends the encrypted report to the aggregator node. To accomplish the task, the scheme includes an aggregator node (e.g., substation) and users (e.g., end-user). In addition, the scheme also utilizes an offline TTP in the network model. In the registration phase, the aggregator node and end-users initially compute their own key pair (including public and private keys) and other cryptographic *param* and publishes them. The TTP selects $(n+1)$ blinding factors $\{\pi_0 + \pi_1 + ...\pi_n\}$ randomly such that $\pi_0 + \pi_1 + ...\pi_n \equiv 0 \ (mod \ N)$ and sends securely these blinding factors $\pi_0$ to aggregator node, and $\pi_i$ to $U_i$ (user). These blinding factors are being used in aggregation phase: the user collects power usage from the smart meter and transforms it into a ciphertext, computes a signature and sends the report to the data aggregator. The data aggregator verifies the signature and the report in the batches. Fan et al. claimed that the scheme proposed in [160] is secure from external and internal attacks and achieved data integrity. However, the scheme incurs significantly high communication overheads as many thousand of consumers have to send the consumption report every time (e.g., 15 min. or lesser) throughout a day. As a consequent, the high overhead may not be a practical solution in the real-world applications, and may induce a substantial load on the data aggregator node.

For the financial auditing purpose, a range-based query scheme called PaRQ is proposed for smart grid applications in [161]. In this scheme, a residential user first performs asymmetric encryption on his/her consumption usage and then forwards the cipher text (i.e., consumption data) to the cloud server. Later, whenever financial audits are required, an authorized legal entity (e.g. audit requester) usually sends query (including secure tokens) to the cloud repository where the data is stored, and retrieves consumption usage of the residential user. Specifically, the authors utilized a hidden vector encryption (HVE) scheme and constructed a query for encrypting the required attribute and session key. In PaRQ, the authors used symmetric encryption (i.e., AES) for encrypting the query, and achieved data confidentiality and query privacy. Nevertheless, one main demerit in the HVE is that the size of encrypted text and decryption key size are larger than the length of the chosen vector. Another demerit in the HVE scheme is that it may have issues with the one-to-many encryptions scenarios.

Utilizing the PKI, Seo et al. described an automated demand response mechanism that concentrates on the residential model in [162]. The model utilized the standard OpenADR 2.0 protocol for advanced metering infrastructure. All devices ensured security service using public key infrastructure (PKI) certificates and digital certificates issued by a trusted certificate authority. To offer a secure Internet connection, information exchanges are accomplished with transport layer security (TLS) version 1.0 encryption. Similar to other schemes, this scheme also requires high computational cost in registration and settlement phase due to the exponentiation operations.

In [177], Ni et al. proposed EIGamal encryption based scheme for smart meters. The scheme not only aggregates the consumption data from SMs but also defends fault tolerance of malfunctioning SMs. In addition, the authors leverage zero-knowledge based scheme to filter abnormal measurements caused by energy theft without revealing the consumer details. In addition, the authors claimed that their proposed scheme can resist differential attacks. However, EIGamal encryption based schemes are usually compute extensive. In another research, Won et al. [178] proposed a privacy-assured aggregation scheme for DR program in the smart metering. Particularly, the authors designed a future ciphertext using the shared secrets among SMs. The scheme utilized peer-to-peer network to locate the neighbouring SMs for sharing the secrets. However, the scheme may have practical issues, for instance if there is a communication failure then SMs may not be able to communicate with the aggregator. In addition, the scheme may not resist to an impersonation attack. More literature on asymmetric cryptosystems can be found in [179]–[182].

*Homomorphic cryptosystem*: The symmetric and asymmetric cryptosystems are considered to be deterministic, which invariably transforms the unique ciphertext for a given plaintext and key. This may give room to an attacker/eavesdropper to learn the partial information (i.e., information leakage) by

TABLE XII
MITIGATION TO EAVESDROPPING/INTERCEPTION THREATS – ENCRYPTION SCHEMES IN SMART GRID METERING NETWORKS.

| Sch-emes | Applications | Wireless/ Wired | Involved entities | Test-bed/ Simulation | Sec. & Pri. Goals | Descriptions | Ref. |
|---|---|---|---|---|---|---|---|
| SC | Asset/data management | Wireless | SM, substation, Utility | Simulation | 2,3 | ***Pros:*** securing last mile smart grid using dynamic secrets; focus on control center and substation; uses lightweight operations, e.g., XORing and Hashing; secure from MITM, replay and impersonation attacks; and provide confidentiality. ***Cons:*** malicious SN may lead many attacks. | [158] |
| SC | Data & load management | ZigBee | SM, HAN | Testbed | 3 | ***Pros:*** link layer based dynamic secret key is generated; a light-weight encryption (i.e., XORing and Hashing); protection against eavesdropping; and could be integrated with many applications. ***Cons:*** link layer has inherent security issues including collisions, exhaustion and unfairness that causes critical DoS threats. [172] | [159] |
| AC | Load management i.e., DD | unspecified | SM, DRP Custermer device | – | 1,2,3, 8, 12 | ***Pros:*** privacy-preserving protocol; incentive-based demand response; provides privacy, availability, integrity, authenticity, confidentiality, defending cheating customers; and anonymity and unlinkability. ***Cons:*** requires high computational cost in registration and settlement phase due to exponentiation operations. | [120] |
| AC | Data management | Wireless mesh network | SM, NAN | Simulation | 2,3,4 | ***Pros:*** a tree-based secure power-usage data aggregation; uses the blinding factor against insiders; and achieved secure data integrity and batch verification. ***Cons:*** computational costs are high that involves signature aggregation and batch verification for SM and NAN (aggregator). | [160] |
| AC & SC | Data management | ZigBee | SM, HAN, Utility, Cloud Server | Simulation | 3,4,7 | ***Pros:*** to encrypt metering data, hidden vector encryption (HVE) based range query is constructed; data confidentiality and data (query) privacy are evaluated. ***Cons:*** encryption requires high computational cost due to exponentiation operations [173]; and HVE may have one-to-many communication issues. | [161] |
| AC | Load management | Wired | SM DRS | Testbed | 3 | ***Pros:*** introduced an automated residential DR model; used OpenADR 2.0 protocol; Simulation and demonstration tests are conducted; utilized PKI certificates and digital certificates ***Cons:*** requires high computational cost in registration and settlement phase due to exponentiation operations; lack of security analysis. | [162] |
| HE | Data management i.e., billing | Wireless | SM, Utility | – | 3 | ***Pros:*** privacy-preserving data aggregation; smart billing; fraud detection; cryptographic commitment utilized homomorphic encryption; privacy-preservation; and ensured data integrity and authenticity. ***Cons:*** may incur significantly high computational on resource-hungry smart meters [174]; and lack of proof-of-concepts and simulations. | [165] |
| HE | Data management | Wireless mesh network | SM, HAN, Utility | Simulation | 3 | ***Pros:*** a new problem is investigated called packet reassembly; used TCP for secure data aggregation in AMI; and addressed a new presentation layer; utilized a (secure) header including the packet size. ***Cons:*** lack of threat model and security analysis. | [163] |
| HE | Data management | unspecified | SM, NAN | – | 2,3,8 | ***Pros:*** presented a monitoring purpose system; preserves individuals privacy; homomorphically aggregated consumptions of $n$ members of neighbourhood; and HMAC bsaed data integrity or a digital signature. ***Cons:*** lack of performance analysis, and computation overhead on the NAN is larger. | [164] |

SC : symmetric encryption; AC : asymmetric encryption; HE : homomorphic encryption; DRP : demand response provider; DRS: demand response server; TCP : transmission control protocol; HMAC : hashed messages authentication code; – : no proof of concepts/simulations;
**Security and Privacy goals** – 1 : Availability; 2 : Integrity; 3 : Confidentiality; 4 : Authentication; 5 : Non-repudiation; 6: Authorization; 7 : Accountability; 8 : Anonymity; 9 : Unlinkability; 10 : Undetectability; 11 : Unobservability; 12 : Pseudonymity

performing the statical analysis on the transmitted ciphertext [183]. To deal with such deterministic cryptosystems, the *homomorphic* crytosystem is utilized heavily in the literature. Homomorphic cryptosystem is an encryption that performs computation on encrypted messages, without knowing the secret key.

Borges et al. [165] suggested a privacy enhancing scheme for smart metering. The protocol considered mainly two use-cases: data aggregation, and secure and verifiable billing. To achieve the user privacy, the smart meter uses homomorphic encryption and computes a cryptographic-based homomorphic commitment on the consumption usage. Thus, the consumption usages, sent by the smart meter are kept secured through homomorphic commitment or encryption and achieves privacy. Borges et al.'s scheme may incur significantly high computational on resource-hungry smart meters [174]. Moreover, the scheme lacks proof-of-concepts and simulations, so it is hard to analyze its usefulness. To collect the fine-grained power consumptions data, [163] investigated the feasibility and performance of full homomorphic encryption (FHE) aggregation in AMI networks utilizing the reliable data transport control protocol (TCP). The scheme proposed in [163] lacks threat model and security analysis.

Busom et al. proposed a smart metering data monitoring scheme in [164]. The scheme utilized homomorphic encryption and achieved privacy. The authors considered that a smart grid that consists of a neighbourhood $k$, contains smart meters $SM_i, i \in 1, ..., k$ and power supply station $PSt$. In the scheme, each $SM_i$ periodically (e.g., every 30 min) sends electricity measurements $m_i$ to $PSt$. $SM_i$ generates

a random noise value $z_i \in Z_q$ and computes a ciphertext as $c_i = Enc_y(m_i + z_i) = (c_i, d_i)$, where $Enc$ is encryption and $y$ is public key of $SM_i$. Eventually, it transmits the result to $PSt$. The $PSt$ receives all values and then adds them to calculate the total energy consumption. Busom et al. did not provide the performance analysis, which may raise practicality issues. Moreover, the smart meter has to perform hard computations, and therefore, the computation overhead on the NAN gateway is larger when there are many thousands of meters. Moreover, more schemes on homomorphic encryption can be found in [166], [184]–[187].

**Authentication and access control schemes**: Authentication mechanism is paramount that provides sufficient protection against eavesdropping, and eliminates unauthorized entities [188]–[190]. Recently, a number of authentication and access control schemes have been extensively studied in smart grid applications [82], [143], [191]–[203]. Table XIII summarises different approaches on how different entities in smart grid ensures the authentication and access control.

Mohammadali et al. [143] proposed a novel identity-based key establishment protocol (NIKE) that provides data confidentiality. The authors employed ECC to achieve lower computational overhead compared to existing protocols, particularly at the home gateway (i.e., meter side). In this scheme, a meter (M) generates random nonce $a$ and computes $T_M$ and sends $ID_M, T_M, R_M$ to AMI Head-End (AHE), in the first step. Here, $ID_M$, $R_M$ is identity of meter and secure parameter of M, respectively. In the second step, AHE, generates random nonce $b$, computes $T_x$, $T_{AHE}$, $k_{AHE \to M}$ and $M_1$, and sends $T_{AHE}, ID_{AHE}, M_1$ to a meter. In third step, the meter computes $k_{M \to AHE}, M_1'$ and checks $M_1 = M_1'$. It then computes $M_2$ and $K$, and sends $M_2$ to the AHE. In the final step, AHE computes and verifies $M_1 = M_1'$. After performing above three steps, a session key (K) can be derived. The NIKE provides protection from MITM, impersonation and desynchronization attacks. Furthermore, the security of NIKE is verified using AVISPA tool.

Kumar et al. proposed a lightweight authentication and key agreement for smart metering network in [191]. The scheme is based on hybrid cryptography, i.e., ECC and symmetric key. Before sending the consumption usage data to the NAN gateway, a SM first verifies the NAN and then establishes a secure connection. Likewise NIKE, the scheme is verified using AVISPA tool. In addition, the authors implemented their scheme on the IEEE 802.15.4-based SM test-bed. The scheme may provide protection against many attacks (e.g., MITM, replay, and so on), but it did not consider many privacy features, such as unforgeability, undetectability, etc.

To report power consumptions, Chim et al. [192] proposed privacy-preserving scheme. The proposed scheme also performed gateway-assisted authentication while reporting the power usage information. In the scheme, a smart meter sends consumption information from home area gateway/meter to the utility side gateway (i.e., control center) through the building area gateway/meter. Here, the building area network controls performing authentication and data aggregation. The authors exploited a hash-based message authentication code (HMAC) technique to perform the unilateral authentication, and homomorphic encryption technique to achieve privacy. Moreover, the true identity of home meter and the electricity usage plans sent by meter are kept secret even from the utility (i.e., control center) prior the electricity is utilized [192].

To provide security properties, a mitigation authentication protocol is proposed by [193]. The scheme provides mutual authentication and key agreement, and preserves identity privacy. To attain a delicate trade-off (i.e., performance and security), the proposed scheme utilized ECC primitive and achieved privacy. The authors verified the security functionality of their protocol using Gong-Needham-Yahalom (GNY) logic.

Following the identity-based cryptosystems, in [195], [196], the authors proposed secure anonymous key distribution signature schemes. The authors claimed that their schemes can provide mutual authentication and achieves anonymity at a low computation cost while providing security against e.g., impersonation and replay attacks [195], [196].

To moderately mitigate outsider and insider attacks, in [197], Saxena et al. proposed an authentication and authorization scheme. Whenever a registered user wants to access the smart grid device (e.g., smart meter), the scheme allows to perform user's authorization and authentication. Precisely, to access the device, the users are granted permission dynamically via the attribute-based access control. If the device is being requested for an access then the identity of the user is verified together with the device. Moreover, the scheme has been formally analyzed, and is claimed that it can defend many attacks, e.g., MITM, replay, impersonation, and repudiation attacks [197].

In [198], Ruj-Nayak proposed a decentralized security framework for smart grid. The framework supports two secure features: (i) data aggregation, and (ii) an adequate access control in smart grid. In a general scenario, the massive amounts of consumer information are forwarded to the substations where the information are accessed by several remote terminal units (RTUs). Therefore, to achieve the access control, the scheme employs attribute-based encryption (ABE) which allows restricted access on the consumption information that are stored in repositories (i.e., may be in a cloud). The scheme utilized a key distribution center (KDC) to generate and distribute the attributes and cryptographic keys to the RTU and the consumers.

Considering the utility data/information centers/systems, Baek et al. [199] designed a "Smart-Frame" framework for smart grids. The framework effectively utilized the cloud computing technology. The authors divided the framework into hierarchical layers as follows. (i) *Top cloud* is used to securely manage the management services or distribution services. (ii) *Regional cloud* is used to store the user services securely. (iii) *End-user layer* contains individual smart devices (e.g., a smart meter at home). The Smart-Frame incorporated a security solution which utilized an identity-based encryption (IBE) and signature (X.509) and identity-based proxy re-encryption.

In the similar line of work, Mai-Khalil designed and implemented of a secure billing model for SMs in [82]. The authors encrypted SM data using a homomorphic asymmetric cryptosystem and then, stored it on the cloud. Using the homomorphic technique, Mai-Khalil proposed a method to

TABLE XIII
MITIGATION TO EAVESDROPPING THREATS – AUTHENTICATION AND ACCESS CONTROL SCHEMES IN SMART GRID METERING NETWORKS

| Application | Wireless/ Wired | Involved entities | Test-bed/ Simulation | Sec. & Pri. goals | Descriptions | Ref. |
|---|---|---|---|---|---|---|
| Data management | ZigBee | SM, concentrator AME | Simulation | 1-4 | ***Pros:*** novel identity-based key establishment between SM and AME; very low overhead; formally verified using AVISPA tool; and secure against replay, impersonation, MITM, and desynchronization attacks. ***Cons:*** computational complexity is higher particularly at SM. | [143] |
| Data management | ZigBee | SM, NAN | Testbed | 1-4,9 | ***Pros:*** lightweight key establishment between SM and NAN; very low overhead; formally verified using AVISPA tool; and secure against replay, impersonation, and MITM attacks. ***Cons:*** limited privacy features. | [191] |
| Data management | Wireless | HAN,BAN, NAN, Utility | Simulation | 2,4,5,8 | ***Pros:*** provide privacy to consumption unit; verification of consumption unit via authentication; uses cryptographic commitment; homomorphic encryption; bloom filter for data filtering; and secure against DoS. ***Cons:*** unilateral authentication; significant overhead; and security against attack is not analyzed. | [192] |
| Data management | – | SM, NAN | Simulation | 4,9 | ***Pros:*** authentication with identity protection; privacy protection at SM; and less storage overhead and communication cost. ***Cons:*** no threat model; and no simulations/proof-of-concepts | [193] |
| Data management | – | HAN, NAN | Simulation | 2,3,4 | ***Pros:*** proposed a lightweight authentication; exploited bitwise exclusive-OR operation; and achieved confidentiality, integrity and authentication, and replay attack-resistance. ***Cons:*** may require high communication cost at resource-limited SM. | [194] |
| Data management | Wireless | HAN/SM, Service provider | Simulation | 2,4,8 | ***Pros:*** secure anonymous key distribution between SMs and service providers; uses identity-based signature and encryption schemes to achieve anonymity; security under random-oracle model. ***Cons:*** device secrets can be easily leaked, and cannot provide credentials' privacy [196]. | [195] |
| Data management | Wireless | HAN/SM, Service provider | Simulation | 2,4,8 | ***Pros:*** secure authenticated key agreement; provable security; secure against the well-known attacks (impersonation, reply, MITM, etc.); and provides session key security. ***Cons:*** requires high computational and communicational cost. | [196] |
| Data & assest management | Wireless | User, SM, Subsation, Utility | Simulation | 2-4,6, 8 | ***Pros:*** two factor authentication; access control; defeats various outsider attacks and insider attacks, e.g., MITM, replay, impersonation, integrity violation, known key and repudiation attacks. ***Cons:*** overall high communication overhead; and high computation overhead for resource-hungry SM. | [197] |
| Data & assest management | – | HAN, BAN, NAN | – | 3,4,6 | ***Pros:*** proposed privacy-preserving aggregation; achieved access control; employed homomorphic encryption; and attribute based encryption. ***Cons:*** may incur high communication and computation on SM. | [198] |
| Data management | Both | SM, Utility, data storage | Testbed | 2-4 | ***Pros:*** introduced "Smart-Frame"; provides flexibility, scalability and security features; used identity-based encryption; and implemented a prototype. ***Cons:*** may incur high communication and computation due to homomorphic encryption and PKI. | [199] |
| Data management | Wireless | SM, Utility, Cloud | Simulation | 3,8 | ***Pros:*** a cloud-based data storage and processing model; preserved user privacy and confidentiality of data exchanged; used homomorphic asymmetric cryptosystem; and many use-cases: (i) securely compute energy consumption of customer and (ii) proposed billing algorithm. ***Cons:*** may incur high computation overhead due to the high number of homomorphic operations. | [82] |
| Load management | Wireless | DR client, Server, Utility, Cloud | – | 1-4,6,8 | ***Pros:*** discussed cloud computing for DR program; proposed mapping security objectives (identity management, access control, information protection, critical asset protection). ***Cons:*** lack of proof-of-concepts and simulations. | [200] |

**Security and Privacy goals** – 1 : Availability; 2 : Integrity; 3 : Confidentiality; 4 : Authentication; 5 : Non-repudiation; 6: Authorization; 7 : Accountability; 8 : Anonymity; 9 : Unlinkability; 10 : Undetectability; 11 : Unobservability; 12 : Pseudonymity

generate the energy bills for the customers based on their total electricity consumption. More importantly, many real-time experiments have been conducted including the complexities of homomorphic operations, and computational timing values in different billing periods. In another research, Mohan-Mashima worked on cloud computing to secure automated demand-response program [200]. Authors mainly focused on OpenADR 2.0-related networks. In addition, the authors also pointed out key security properties and discussed key challenges that should be undertaken when transforming data from traditional DR networks to the cloud-based networks. More studies on cloud-based authentication schemes for smart meters can be found in [204], [205].

**Other schemes**: Following the different approaches, recently, differential privacy-based schemes have been proposed in smart metering networks. In [206], Zhang et al. proposed two differential privacy mechanisms for the smart meters. The two schemes are known as "battery-based differential privacy-preserving (BDP)" technique and "cost-friendly differential privacy-preserving (CDP) " technique. In BDP, the authors

suggested to install a rechargeable battery in a home. Typically, a smart meter sends the total energy consumption from electrical appliances and the battery. Therefore, the real fine-grained energy consumption is hidden. The authors then extended BDP idea and proposed CDP that utilized the dynamic and static pricing policies. Though, the both schemes can achieved differential privacy using the battery, a battery may have limited capacity.

**Summary**: As the smart meters send sensitive information (i.e., consumption usage data) via the wireless communication technologies, cryptography-based schemes are paramount techniques to achieve privacy for information flow between the homes and utility companies. We reviewed (i) encryption schemes considering symmetric encryption [158] [159], asymmetric encryption [120], [160]–[162], and homomorphic encryption [163]–[166], and (ii) authentication and access control schemes [82], [143], [192]–[200].

**Lessons Learned:** The privacy issues of consumers are emanated from the consumption usage data as the data travelled and stored in the form of plaintext in the SG metering network. In the era of smart metering, in which consumption usage data is invaluable to service providers, utility companies and many more, existing proposed approaches may have a wide attack surface. Nevertheless, as the smart meters are typically resource constraints devices, we find following the trace of SMI where the future researchers need to focus on overhead in the terms of computational and communicational costs. Indeed, strong cryptography requires extensive computation and resource. For example, majority of proposed schemes in Table XII utilized either homomorphic encryption or public key infrastructure (PKI), which requires high resources. In [183], Esposito-Ciampi argued that homomorphic encryption and PKI systems are often too expensive. Therefore, we believe that choosing the right cryptography-based mechanisms are challenging that must provide utmost confidentiality, while minimizing resource consumptions (i.e., especially for the SMs), as follows.

- *Energy*: As the SMI networks are not limited to the smart electricity meters but also involved the smart gas meters. For example, in Britain (and many other countries), energy companies are rolling out smart gas meter as the part of SMI network. Since the smart gas meters are battery-powered, energy-efficiency could be a concern if such heavy homomorphic encryption and PKI systems are implemented on the battery-powered devices.
- *Memory storage*: Indeed, memory requirements depend upon the applications. Since the security and privacy methods are overhead on the applications, optimal storage (i.e., program and data memory) for security and privacy algorithms is a big concern, especially for the resource-limited smart meters, sensors, and so on.
- *Time complexity*: How much the running time is needed to execute the security and privacy mechanisms is another concern. For example, to detect defective lines or apparatus protective relaying requires $\leq 4ms$; and subseconds requires in wide-area monitoring for transmission and distributions, nevertheless the time complexity is one of main concerns in the terms of security in smart grid.

**Mitigation to forwarding point compromise**: As shown in the threat taxonomy, confidential information can be disclosed if a forwarding entity/node is semi honest in smart grid. Such node can neglect routing packets that are supposed to forward, transmit incorrect values, and manipulate protocol messages to compromise the privacy of consumers.

To mitigate such issues, Dimitriou-Awad [207] proposed a secure aggregation scheme that is resilient to semi honest entities. The authors assumed that each meter $(SM_i)$ has a set of neighbouring trustworthy SMs, denoted by $TS_i = \{SM_{i_1}, SM_{i_2}, ..\}$ and each smart meter $(SM_i)$ shares a random key/number with the SMs in the set $TS_i$. The shared key can be a symmetric or pairwise key. The main idea of the protocol is that each smart meter $(SM_j \in TS_j)$, $(SM_i)$ generates a random number $(K_{i,j})$, and computes $(K_i) = \sum_{SM_j \in TS_i} K_{i,j}$. Now $SM_i$ sends $K_{i,j}$ to the $SM_j$. At the same time, $SM_i$ also obtains all the shared $K_{j,i}$ that destined to it from $SM_j \in TS_i$, and calculates the blinded energy measurement $(B_i = EM_i + K_i \sum_{SM_i \in TS_j} K_{j,i})$. Finally, $SM_i$ sends $B_i$ to the aggregator node. After receiving of all blinded energy measurements, the aggregator node computes $\sum_{i=1}^{n} B_i$ that is equal to $\sum_{i=1}^{n} EM_i$. The authors evaluated that scheme is secure against the semi-honest attackers. Hence, an attacker cannot drop the protocol messages, and cannot manipulate the protocol messages to compromise the privacy of legitimate smart meters/home owners.

In the Dimitriou-Awad's scheme, as the number of SMs are increasing in the trusted set $TS_i$, the average delay and the number of messages exchanged are increasing significantly. Moreover, the authors did not consider the negative impacts of their scheme. For example, if a smart meter leaves the set (i.e., $TS_i$), revoking the keys of moving smart meter becomes an issue.

In another research, to protect the privacy leakage of monitoring data in multi-hop environment, a novel broadcast authentication protocol was proposed for WSN based smart grid monitoring in [208]. In order to mitigate the attacks, the control center (e.g., sender) constructs a cipher puzzle and signs each packet with the secret key and broadcasts the packets. Upon receiving the broadcast, all legitimate sensor nodes solve the cipher puzzle, authenticate the received data packets by verifying the signature, and check the hashed values of packets via utilizing the public key of the control center. The authors claimed that the packet arriving at the sensor nodes (i.e., receiver) can not be manipulated. However, the propagation delay of the proposed scheme increases linearly. For instance, assumed that the sender broadcasts 20 packets then the propagation delay is almost 13 seconds. In the same vein, Camara et al. [209] proposed Infinite Timed Efficient Stream Loss-tolerant Authentication *(inf-TESLA)*. The protocol provides a multicast delayed authentication to stream synchrophasor data for controlling the phasor measurement unit (PMU) that is deployed in the wide field area of electric power network. The authors employed a dual offset key chain method for minimizing the authentication delay and computational cost. The *inf-TESLA* is safeguard to man-in-the-middle attack.

However, the *inf-TESLA* may vulnerable to memory-buffer

TABLE XIV
MITIGATION TO FORWARDING POINT COMPROMISE THREATS IN SMART GRID METERING NETWORKS

| Application | Wireless/ Wired | Involved entities | Test-bed/ Simulation | Sec. & Pri. goals | Descriptions | Ref. |
|---|---|---|---|---|---|---|
| Data management | IEEE 802 Wireless | SM, aggregator | Simulation | 3,4,10 | ***Pros:*** a secure aggregation scheme; resilient to semi honest entities; utilized a symmetric or pairwise key; secure against malicious forwarding point, safeguard to manipulation of packets. ***Cons:*** main demerit – the average delay and the number of messages exchanged are increasing significantly. | [207] |
| Assest management | 802.15.4 ZigBee | CC, SM, sensor nodes | Simulation | 2,3,4 | ***Pros:*** a novel broadcast authentication protocol for wide area monitoring; constructs a cipher puzzle to mitigate attacks; and resistance to DoS Attacks and receiver compromise tolerance. ***Cons:*** propagation delay of the proposed scheme is high. | [208] |
| Assest management | Wireless | SM, NAN | Simulation | 2,4 | ***Pros:*** a multicast delayed authentication protocol; wide area control; utilized dual offset key chains technique; minimized authentication delay; and secure from MITM attack. ***Cons:*** the inf-TESLA suffers from memory-based DoS attack, high communication cost. | [209] |

SM : smart meter; NAN : neighbourhood area network; CC : control center; MITM: man-in-the-middle;
**Security and Privacy goals** – 1 : Availability; 2 : Integrity; 3 : Confidentiality; 4 : Authentication; 5 : Non-repudiation; 6: Authorization; 7 : Accountability; 8 : Anonymity; 9 : Unlinkability; 10 : Undetectability; 11 : Unobservability; 12 : Pseudonymity

overflow attack, if many packets are flooded to the network. Moreover, the communication cost in *inf-TESLA* is significantly high, as compared to the traditional protocol.

**Summary**: Table XIV summarises the proposed approaches that preserve privacy as well as mitigate the forwarding point compromise threats. In addition, we presented the advantages and disadvantages of the proposed schemes [207] [208] [209].

**Lessons Learned**: One of the main lessons is that there is no single architecture/solution which is especially designed to mitigate the forwarding point compromise threat, up to now, in the SG metering network. However, the approaches that address this issue somehow, e.g., [207] and [208], suffered from high average delay and propagation delay, respectively, as shown in Table XIV. Such high delays can raise availability issues in the time-critical applications. In [207], the authors discussed that a (malicious) forwarding point can be detected via utilising the trusted set, but it is very likely a smart meter may leave the trusted set then revoking keys may be another prime concern. Moreover, Camara et al.'s [209] scheme suffers from high communication cost and may be vulnerable to memory-based DoS attacks.

Following the above-mentioned solutions, we believe that there is a need of a dedicated solution/architecture that mitigates the forwarding point compromises in SG metering network, so that these issues should be addressed and handled appropriately in order to realize the real SG metering networks.

**Mitigation to backhaul network interception**: As the sensitive information travels through the backhaul network, it can be leaked if adequate security is not implemented, as discussed in Section III. However, few of the recent approaches mitigate such information leakage that can ensure data security and privacy protection in smart grid domain [121]–[123].

Mahmoud et al. [121] suggested privacy-aware scheme over hybrid advanced metering infrastructure/long term evolution (LTE)in smart grid. The basic idea of the scheme is that the utility company collects the power bids from the consumers in a secure and privacy-preserving manner. To achieve privacy, the authors suggested to use homomorphic encryption so that the utility company cannot correlate the consumers' bids. The use case is as follows – the utility wants to buy energy from the consumers. The utility first generates a packet (that includes, a signature and purchase price) and sends it to the consumers via the aggregator node that utilizes the backhaul (i.e., LTE) network. Second, the aggregator receives the packet and checks the authenticity and integrity of the packet. If results are true, the aggregator forwards the packets to the consumers. Upon receiving the packet, the smart meter verifies the authenticity and integrity, and sends a reply-packet (i.e., a signature, amount of power unit, and price) back to the aggregator node. Now, the aggregator collects the reply-packets from all the consumers, and aggregates all these packets in a secure way (using a signature and homomorphic encryption). Then it sends the bid-packets to the utility. Finally, the utility verifies the authenticity and integrity of the bid-packets. Note that the individual's bid cannot be correlated at the utility company. The authors claimed that the scheme is secure to many attacks, e.g., impersonation, replay, MITM, and it achieves privacy.

The authors asserted their scheme is secure and privacy-aware, but it incurs high communication costs due to large packet sizes, which may not be practical for computation-constrained smart meters. Moreover, in [122], the authors demonstrated Mahmoud et al.'s scheme can reveal the bids privacy at the utility. Further to Mahmoud et al.'s scheme, in [122], Zhang et al. proposed an enhancement to mitigate the privacy risks at the utility.

In another research, Kim et al. [123] proposed a new REMP (i.e., resilient end-to-end secure message protection) mechanism for large-scale cyber physical system (CPS) to eliminate the need of traditional costly solutions, such as IPsec/TLS. The REMP is a group-based architecture which utilizes the publish-subscribe communication model. In a group communication, the authors suggested to make use of the trusted third party and/or authentication server that to distribute five types of secret keys and security tokens to the publisher (P), subscriber (S), and packet broker (PB).

To mitigate intermediate malicious entities, each P generates

TABLE XV
MITIGATION TO BACKHAUL NETWORK INTERCEPTION IN SMART GRID METERING NETWORKS

| Application | Wireless/ Wired | Involved entities | Test-bed/ Simulation | Sec. & Pri. goals | Descriptions | Ref. |
|---|---|---|---|---|---|---|
| Data management | IEEE 802 Wireless | SM, aggregator, utility | Simulation | 2-4,8 | ***Pros:*** a secure and privacy-aware power bidding scheme, utilizes LTE network, ensures integrity and authenticity; safeguard to impersonation, replay, man-in-the-middle attack. ***Cons:*** incurs high communication costs, lack of threat model, can reveal bids privacy [122]. | [121] |
| Data management | IEEE 802 Wireless | SM, aggregator, utility | Simulation | 2-4,8 | ***Pros:*** an efficient and privacy-aware power bidding, utilizes LTE network, ensures integrity and authenticity; safeguard to impersonation, replay, man-in-the-middle attack. ***Cons:*** high communication overhead. | [122] |
| Assest management | 802.15.4 | SM, Sensor, field devices | Simulation | 2-4,8 | ***Pros:*** An E2E packet protection, E2E authenticators per packet, high scalability and extensibility. ***Cons:*** lack of practical assumptions. | [123] |

**Security and Privacy goals** – 1 : Availability; 2 : Integrity; 3 : Confidentiality; 4 : Authentication; 5 : Non-repudiation; 6: Authorization; 7 : Accountability; 8 : Anonymity; 9 : Unlinkability; 10 : Undetectability; 11 : Unobservability; 12 : Pseudonymity

a unique session key (using a random number) and uses a symmetric encryption algorithm (i.e., advanced encryption standard, AES) for securing each E2E packet sent. Upon receiving packet from P, the PB verifies whether the source of the packet is a legitimate publisher who has access to the group, and drops if any unauthenticated packet arrives. Then PB forwards packet to the subscriber. When a subscriber receives an encrypted packet, it verifies the source of the packet and decrypts the packet using the shared key. The REMP provides, E2E privacy, E2E integrity, packet source authentication and confidentiality, forward and backward secrecy, and protects against many attacks, e.g., replay, impersonation, long-term key compromised. However, the authors have neither made assumptions about the PB whether it is a trusted entity or nor discuss the negative impacts if the PB is compromised.

**Summary**: Table XV summarises the proposed approaches that are claimed to preserve privacy in end-to-end manner. In addition, we discussed pros and cons of the proposed schemes [121], [122], [123].

**Lessons Learned**: The backhual networks [210], [211] are enablers for the NANs and WANs in SG metering network, as they are operated by the network operators. As shown in [212], a backhual network (e.g., LTE/4G) can have own inherent privacy issues due to the lack of privacy requirements in the standard security protocol. We believe that such weakness may lead to many privacy threats. Therefore, the negative impact of backhual networks should be further investigated as consumptions usage data is invaluable to network operators, and utility companies. Moreover, while reviewing the existing schemes (refer to Table XV), we pointed out few observations. For instance, the scheme proposed in [121] incurred high communicational cost and the threat model is limited to replay attack. Likewise, [122], in general, is also costly in terms of communication costs. We believe that Kim et al. [123] scheme, which is a publish/subscribe based architecture, is more practical, as it imposes less communication costs, and provides scalability and extensibility.

**Mitigation to misuse of data**: Trusted platform module (TPM) based solutions (e.g., [213]–[216]) can be considered as another approach to mitigate the misuse of data threats in smart grid networks.

Paverd et al. introduced a novel and independent entity called "trustworthy remote entity (TRE)" [124], [125] [127] . Nowadays, it has been assumed that the utility company does not need the individual's consumption usages but it mainly requires the total power usages from the homes. The TRE is, therefore, a system (i.e., hardware, software, or both) that demonstrates similar functional features as of the trusted third party (TTP) but renders secure assertions of its trustworthiness. The TRE aggregates energy consumptions from several homes/smart meters and sends the aggregated (consumptions) report to the distribution network operators (DNO) in a privacy-preserving mode. The TRE is assumed to set up a trust relationships between the consumer and the DNO. For instance, an end-user believes that the TRE preserves its privacy, whereas the DNO believes that the TRE first authenticates an end-user and then it provides the aggregated report correctly. The scheme incorporates mainly following: (i) meter-to-utility monitoring information, (ii) billing information, and (iii) bi-directional demand response information. Through formal analysis, the TRE not only achieved authentication, integrity, and confidentiality, but also attained undetectability and unlinkability. In addition, utilizing the TPM and embed Transport Layer Security (TLS) cryptography library, performance evaluations have been demonstrated on different platforms, e.g., Intel TPM, Linux-TPM, VM-vTPM, etc. For more details the reader may refer to [125].

In the same vein, Ankele et al. [217] pointed out that secure multi-party computation (MPC) algorithms are inefficient if there are high numbers of participants, e.g., $(n)$ users, in several use-cases. This is due to the fact of the traditional settings, wherein MPC considered only *input values* as private. Nevertheless, Ankele et al. pointed out the privacy of the users on the ground of computational *output values* is essentially needed. The authors, therefore, discussed many scenarios linked to the MPC paradigm where the number of participants are high (e.g., large scale applications: network monitoring, billing, demand control, and so on). In addition, the authors suggested the utilisation of TRE and proposed privacy-preserving algorithm that can preserve the privacy while providing confidentiality.

Gunes et al. [218] proposed a open cyber architecture

TABLE XVI
MITIGATION TO MISUSE OF DATA –TRUSTED COMPUTING-BASED SCHEMES IN SG METERING NETWORKS

| Application | Involved entities | Testbed/ Simulation | Sec. & Pri. goals | Descriptions | Ref. |
|---|---|---|---|---|---|
| Data management | SM, TRE, DSM | Simulation, testbed | 2-4,8-11 | ***Pros:*** privacy-enhancing communication architecture; incentive-based demand response application; a novel entity called trustworthy remote entity; and provides authentication, integrity, confidentiality, undetectability, and unlinkability. | [124], [127], [125] |
| Data management | SM, TRE Utility, etc. | – | 2,3,8 | ***Pros:*** secure multi-party computation; propose TRE-based privacy-preserving algorithms. ***Cons:*** lack of proof-of-concepts or simulations. | [217] |
| Data management | HAN, WAN/ utility | Simulation | 2-4,8 | ***Pros:*** an open cyber architecture; a blind processing framework; uses TPM hardware; minimize human intervention; and secure to MITM, session injection, and side channel attack. ***Cons:*** the system boot time is considerably slow (i.e., $\approx$ 82 seconds). | [218] |
| Data management | SM, Concentrator | Simulation | 2,4,8 | ***Pros***: Proposed privacy protection scheme; used trusted smart meters; exploited remote anonymous attestation; used attribute certificates for hiding platform attributes; prevented private information; and ensured detection of trusted software updates, if any. | [219] |
| Data management | SM/HAN, utility/ central systems | Testbed | 2-4 | ***Pros:*** uses of protected module architectures; implements high assurance smart meter; and security analyzed; and guarantee integrity and confidentiality. ***Cons:*** does not protect against DoS attack when a buggy application, e.g., overwrites crucial OS data structure. | [220] |

DSM: demand side manager; SP: service provider; OS: operating system; SGIT: interactive terminal of smart grid; TAS: trusted access server; –: unspecified.
**Security and Privacy goals** – 1 : Availability; 2 : Integrity; 3 : Confidentiality; 4 : Authentication; 5 : Non-repudiation; 6: Authorization; 7 : Accountability; 8 : Anonymity; 9 : Unlinkability; 10 : Undetectability; 11 : Unobservability; 12 : Pseudonymity

(OCA) and enhanced information sharing among the utility operators and transmission levels. The entire smart grid network is divided into three main networks: (i) HAN; (ii) MAN; and (iii) WAN. In all three networks, multi-owners devices are interacting with each other in the top-to-bottom approach. To address privacy concerns in the multi-owner systems, the authors suggested a blind processing framework that provides secure data sharing to the dedicated user or process. For the blind processing, a TPM hardware is being utilized so that human operators/network administrators can not access the plain-text of sensitive information. To achieve this, a smart meter first attests identity of the remote entity then establishes a secure channel using its keys to encrypt/decrypt messages. Within the TPM, sensitive data is shielded based on different states of the system and then utilized in the blind processing. In addition, their framework can provide security against MITM attack, session injection and hijacking attacks, and safe from side channel attacks [218]. The proposed OCA may have issues. For instance, the blind executions need robust and trustworthy software to process the smart meter information and to check integrity of other processes. This paper did not provide investigation on the negative impact of the blind processes if a buggy software is running on the platform that may raise concern of the OCA's effectiveness. Moreover, detecting bugs in the blind execution may be challenging, since it requires more sophisticated techniques (e.g., machine learning) and resources. Another major issue with the OCA is that the system boot time is substantially slow ( i.e., $\approx$ 82 seconds) that may lead to several system-level denial of service attacks [221].

Zhao et al. [219] proposed the idea of a trusted smart meter (TSM). In the scheme, attribute certificates are being utilized for hiding the platform configuration information of a smart meter. On the contrary, to hide the user sensitive information, cryptography-based ring signatures are adopted. Based on RSA ring signature, the TSM can provide a list of properties: correctness, anonymity, and unforgeability. In addition, using the digital certificates, a smart meter attributes can be protected. The authors claimed that their scheme provides security against the private information leakage attack while achieving the efficiency. Moreover, the scheme can detect whether the software update is trusted or not. The proposed scheme evaluated the execution time values for several ring sizes, on the Intel Xeon E5-2407 v2 CPU (2.40 GHz) and 4 GB RAM. However, the main drawback of the ring-based scheme is that whenever a trusted smart meter wants to assert its real identity to the data concentrator, it must include neighbouring trusted smart meters by their public key certificates and then compute a ring signature. Moreover, a ring signature scheme can preserve privacy of the smart meters at the data concentrator whilst a faulty meter and/or compromised meter can not be simply detected at the data concentrator, since identity of a (compromised) smart meter is hidden in the ring.

Mühlberg et al. [220] proposed a protected module architecture (PMA) designed for smart metering. The PMA mainly considered three use cases: billing, load switching and consumer feedback between the smart meter, and utility. The authors claimed that their scheme can achieve confidentiality and integrity of internal states in the PMA and authentic execution of (event-based) distributed applications can run on the shared infrastructure with a low trusted computing base (TCB). The designed architecture is evaluated using low-powered TI-MSP430 micro-controller based smart meter. The evaluation parameters are lines of code and binary size in the terms of bytes. However, the scheme has less confidence in authentic execution security guarantees, as the number of supporting software packages (including, embedded operating

systems, module loaders, event management components, etc.) are specified as untrusted.

**Summary**: Table XVI summarises existing trusted computing techniques (with their pros and cons) on SG metering networks. In the trusted computing world, indeed, an adversary is not able to obtain the sensitive information by eavesdropping over wireless channels since the transmitted information are kept privacy-cognizant from the source where they are being generated. The existing trusted computing based solutions are a good first attempts but not all solutions can be deployed directly to such complex SG metering networks.

**Lessons Learned**: Due to the heterogeneity of SMs, data concentrators, control centers, the appropriate embedded security and privacy mechanisms (i.e., trusted computing) are essential in SG metering network. We believe that the TRE based schemes, e.g., [124], [125], [127], [217], are more promising for the SG metering networks. The architecture discussed in [218] attempts to proposed OCA that utilizes blind processing techniques to provide data privacy to multi-owners in the smart grid domains. However, one of the main lessons of this scheme is how to design and develop the robust and trustworthy application/software to execute the blind processes for the entire domains. Moreover, analysing the negative impact of blind processing can be significant since a malicious system may inject false information to the entire network. Such false information particularly raises concern of trade-off between effectiveness and security of the open cyber architecture in the smart grid network. In [219], Zhao et al. proposed the idea of trusted smart meter that provides privacy protection utilizing the digital ring signatures. The verification of a number of signatures usually poses long delays, which may lead to DoS attack to the data concentrator.

Majority of TPM based schemes ( e.g., [218]–[220], may suffer from scalability issues. For instance, in a simple smart metering infrastructure (SMI), all the smart meters maybe run the same application on the homogeneous (hardware) platform, making this fairly easy for the research purposes. However, in the real-world situations, the SMI network generally consists of different types of smart meters (i.e., heterogeneous) or different data concentrator nodes running several (different) applications. In more extreme cases, the SMI network may be comprised of many smart meters from different vendors running various distinct applications, e.g., demand-response, control commands, billing, etc. Therefore, there needs to be more in-depth analysis on how to store and manage the information necessary to attest a million of devices in a secure and scalable manner.

However, more studies need to be done in different directions. For instance, on-fly-software updates are complicated to handle and so are the key management.

## XI. Research issues and future directions

In this section, we summarize a list of open research issues, and discuss them in terms of research problem, existing preliminary solutions, and the future research work.

### A. Reproducibility issue

**Research problem:** The biggest concern related to the system level countermeasures, theft to privacy countermeasures, and privacy countermeasures is that they suffer from reproducibility of research results in this SG domain. The majority of existing literatures (as shown in Tables VIII, IX, X, XI, XII, XIII, XIV, XV, XVI) evaluate their approaches by simulation instead of real-world devices. For example, most of the proposed schemes use wireless mode (i.e., either ZigBee or mesh network) but none of them evaluates their security properties with real smart meters. Therefore, there is a less confidence in assessing the risk of the attacks and efficacy of the countermeasures by their work. This is due to the lack of access to real smart meter devices, i.e., the access of smart meter is either non-existent or limited to the older meters.

**Preliminary solution:** A few researchers have implemented and evaluated their schemes using the off-the-shelf devices. For instance, Liu et al. [159] evaluated secret-based encryption scheme using CC2430-F128 based smart meters. Other works [189], [191] [220], [143], and [208] evaluated the security prices using TI MSP430 and MPR2400 based off-the-shelf devices, respectively. Nevertheless, they are just the minority. Lack of real device may result from custom proprietorship machinery, undocumented devices, strict limitations on the systems, and so on [222].

**Future research directions:** The direct access to the devices appears to be limited at present. Therefore, a comprehensive study on how the simulation study is different from the real-device study can either (1) build the confidence of applying existing mainstream evaluation approaches, or (2) minimize the threats to experimental validity.

### B. Lightweight cipher suites issues

**Research problem:** Many computation and communication devices (e.g., smart meter, sensors, etc.) in SMI have resource constraints in nature, e.g., ZigBee devices. These devices demand for the lightweight cipher suites (standardized protocols) that can be employed to provide adequate (symmetric/asymmetric) encryption, authentication, and other paramount security properties [31].

**Preliminary solution:** For resource-hungry devices (i.e., smart meters, sensors, etc.), it is widely accepted that the public and private key (i.e., asymmetric key cryptography) based mechanisms are considerably expensive with respect to computational complexities (timing and energy cost). In contrast, the symmetric cryptography based primitives are easier to apply and fairly superior. However, one main issue with symmetric key cryptography for millions of SG devices is its key distribution and management. On the contrary, homomorphic cryptosystem can transform a given plain-text into multiple ciphertexts and each of them will be randomly selected for communication. Indeed, the homomorphic operation provides security against information leakage attack (or requires robust cryptanalysis). On the other hand, homomorphic encryption generates larger messages to be exchanged among the entities [183]. Consequently, the larger the messages are, the slower the performance is, as shown in mitigations to forwarding

point compromise threats [207], [208]. Moreover, Table XVII summarizes the merits and demerits of the cryptographic schemes, which are analyzed in Section-V.

TABLE XVII
MERIT AND DEMERIT OF CRYPTOSYSTEMS [183]

| Cryptosystem | Merit | Demerit |
|---|---|---|
| Symmetric | Fast encryption and decryption | Bother of agreement on the used key |
| Asymmetric | Simple key management | Bad encryption and decryption performance for resource hungry devices |
| Homomorphic | Robust and compute arithmetic operations on encrypted data | Expansion issue, higher overhead and other performance issues |

Clearly, each cryptosystem suffers from its specific demerits, which requires a new set of lightweight symmetric, asymmetric, or even other possible cryptosystems for securing SG applications.

**Future research directions:** Given the merits and demerits listed in Table XVII, a more lightweight cipher technique or protocol with regard to limited resources is in great need.

### *C. Over the air upgrades [223] – Advanced Key Management*

**Research problem:** SMI requires an enhanced feature of key upgrading in timely manner, which upgrades the required keys running in end-users smart meter throughout its normal lifespan. However, such enhanced features come with potential risks (e.g., location migration), if adequate security measures (e.g., key management techniques) are not employed from the very beginning of the system design.

**Preliminary solution:** Recently, a number of schemes have been proposed to mitigate location migration threat [156], [115], and to mitigate privacy concerns [190], [195], [196]. These schemes particularly focus on key distribution and management in the SG network. However, many of these schemes are either vulnerable to security attacks or incurred high computational costs at the computation-constraint smart meters and sensors.

**Future research directions:** Designing a security system that stands the test of time for the over next 15 years is a non-trivial task. For above case, how to design a sophisticated key management framework could be a promising research topic – that can provide strong foundation to the security and privacy goals (refer to Section IV) and seamlessly extend security services (i.e., over the air upgrades) across multiple platforms, and networks in the SG networks.

### *D. Secure and efficient routing protocol*

**Research problem:** In SG metering communications, different entities (e.g., smart meter, data concentrator, servers, demand response management system, etc.) will exchange messages back and forth via single-hop or multi-hop routing protocols. These protocols will find out the optimal path in terms of quality of services [110]. As the SMI network suffers from limited communication bandwidth [59], it is much easier to fall prey to DDoS attack and result in network congestion. Moreover, it can be noted that none of the routing scheme is designed with a focus of routing privacy, except Nicanfar et al.'s scheme [86].

**Preliminary solution:** Nicanfar et al. [86] proposed a new secure routing algorithm to route the packets from source to destination. The routing algorithm utilized network coding technology. Indeed, such (network) coding-based protocols can maximise the network throughput. On the other hand, they bring plethora of issues, such as significant increase in buffer capacity, maximised packet delay, and high computational costs on resource-hungry devices [224]. Rahman et al. [225] proposed a formal analysis method for dependable SCADA systems. The main focus is to formally verify secure routing for the SCADA devices (i.e., grid side), while neglecting the end-users devices (smart meters).

**Future research directions:** Advanced secure and efficient (end-to-end) routing protocols need to be developed and integrated to assure end-to-end latency, high reliable data delivery and network throughput. We believe that while designing the secure routing protocols, the future research should also consider the possible aspects of privacy (refer to Section IV, privacy goals) in smart metering routing protocols.

### *E. Novel security mechanisms against DoS attacks*

**Research problem:** As cognitive radio (CR) technology is being widely deployed into SG networks, it experiences many new security and reliability issues [100]–[105]. A recent research demonstrates that a delicate design of jamming and spoofing attacks, can reduce the super users spectrum availability and transmission performance [103].

**Preliminary solution:** In [151], the authors proposed a secure and reliable cognitive radio (CR) solution in SG. This scheme uses a CR sensor that communicates over CR network to transmit consumption usages to the field or neighbourhood area network. This research utilized a physical unclonable function (PUF) to generate the secret keys and to add the noise to the keys. However, the noise needs a correct error detection technique that usually demands high computational resources. Therefore, we believe that more analysis is still needed.

**Future research directions:** To mitigate DoS threat, cross-layer attack detection techniques and security mechanisms are new research topics, since CR networks are widely deployed into the SG networks. To realize a viable security in smart grid meter network, the secure mechanisms should be integrated in the cross-layer design, i.e., from top layer to bottom layer and other aspect of the whole system [104]. Quantum cryptography based key distribution (QKD) and management techniques can be another area of research in SG. For instance, quantum secure communications and applications in power grid have been an interest around the globe [226]. In a recent research [227], the authors proposed and simulated a QKD based security solution for IoT-based smart grid. We believe that there are many important applications of QKD that should be explored in the SG metering networks.

### F. Advanced trusted systems based privacy-preserving mechanisms

**Research problem:** The communications in current SG metering network raise many privacy concerns if the consumption data is misused. The utilities commonly aggregate meter reading data on 15 or 30 minute intervals. The data may be used for many purposes, e.g., billing, load management, etc. However, the consumption data can also be misused to infer what types of appliances are being in a home. Having access to such data, the consumer electronics company may start to promote their appliances, which may be intrusive to the consumers. Therefore, *privacy leakage* turns out to be an inevitable problem in SMI system.

**Preliminary solution:** In one of the leading progress efforts, Paverd et al. [124] [127] presented a privacy-enhancing communication architecture using trusted remote entity (TRE). The TRE can ensure that consumption usages are not disclosed and misused at the utility side. The authors utilized trusted computing to mitigate the cyber security and privacy threats in the next generation energy networks. Considering SG as case study, similar work is also presented in [215] [217]. However, such techniques (TRE) could suffer from single point of attack as pointed out in [181].

**Future research directions:** Advanced trusted computing based privacy-preserving mechanisms needs to be explored where the consumers can control their information and maintain privacy.

### G. Security and privacy assessment tools

**Research problem:** As the scale of smart metering system increases, it is imperative to systematically evaluate the robustness and weakness of each security and privacy solution before the real-time implementation. Thus, it brings the demand for customizing the conventional security assessment simulators.

**Preliminary solution:** Most of the traditional security assessment tools (e.g., AVISPA [228], ProVerif [229], etc.) focus on the generic network adversary model (e.g., Dolev-Yao attack model [230]). In addition, TrustFound [231] applies model checking to verify the security of TPM-based systems and protocols. Early studies have utilized game theory and/or logic based techniques. However, the gap between theoretical analysis and practical tool implementation has not been fulfilled yet in the SG applications. Recently, Fawaz et al. [232] introduced a real cost model work-flow. The model first understands system logs and cyber alerts. If any log or alert appears, it is translated into response costs. In addition, in the context of an attack impact – the authors researched what is the impact on a system if security state changes. Another work [233] applies formal and systematic analysis of different types of security assessment techniques to provide an integrative tool for security assessment on large-scale real-world SG metering networks/systems. Nevertheless, there is a lack of technique to customize these works on SG scenarios.

**Future research directions:** To fill the gap between theoretical analysis and practical deployment, the future research should either enhance existing assessment tools (AVISPA, ProVerif, etc.) or explore new implementations.

## XII. Conclusion

The traditional power-grids world-wide of today will transform to the next-generation smart grids in the coming future. These grids are able to exploit the advantage of two-way communication and deliver sustainable and reliable power to the end-users. However, the success of SG metering network depends on its security properties. Another crucial feature of SG metering network is the consumers' privacy, i.e., how to aggregate consumers' data without disclosing their personal and sensitive information. A strategic communication framework integrated with robust security and privacy features should be designed in the very beginning of the smart grid technology deployment. Therefore, security and privacy in power grid are considered as an emergent research theme, which is worth analysing.

This survey discusses a comprehensive survey on security and privacy research in SG metering network. We discuss the real cyber attacks incidents in the power industry and related applications. In addition, we investigate detailed threat taxonomy including system-level, theft of service, and privacy/confidentiality threats that has led to the security and privacy requirement in SG metering networks. Moreover, we present and compare the advantages and disadvantages of state-of-the-art existing most up-to date solutions, then finalize this paper by pointing out the future research problems.

## Acknowledgment

This work is supported by the UK EPSRC (Security and Privacy in Smart Grid Systems: Countermeasure and Formal Verifications) under Grant EP/NO20170/1; and the National Research Foundation, Singapore (No. NRF2015NCR-NCR003-003).

## References

[1] N. Saxena and B. J. Choi, "State of the art authentication, access control, and secure integration in smart grid," *Energies*, vol. 8, no. 10, pp. 11 883–11 915, 2015.

[2] D. Alahakoon and X. Yu, "Smart electricity meter data intelligence for future energy systems: A survey," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 1, pp. 425–436, 2016.

[3] M. Ehsani, Y. Gao, S. Longo, and K. Ebrahimi, *Modern electric, hybrid electric, and fuel cell vehicles*. CRC press, 2018.

[4] M. H. Rehmani, M. Reisslein, A. Rachedi, M. Erol-Kantarci, and M. Radenkovic, "Integrating renewable energy resources into the smart grid: Recent developments in information and communication technologies," *IEEE Transactions on Industrial Informatics*, vol. PP, no. 99, pp. 1–1, 2018.

[5] J. Wu, S. Rangan, and H. Zhang, *Green communications: theoretical fundamentals, algorithms, and applications*. CRC press, 2016.

[6] K. Hamedani, L. Liu, R. Atat, J. Wu, and Y. Yi, "Reservoir computing meets smart grids: attack detection using delayed feedback networks," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 2, pp. 734–743, 2018.

[7] "Smart Grid Market," https://www.marketsandmarkets.com/Market-Reports/smart-grid-market-208777577.html.

[8] J. Bryson and P. D. Gallagher, "Nist special publication 1108r2: Nist framework and roadmap for smart grid interoperability standards, release 2.0," National Institute of Standards and Technology (NIST), Tech. Rep., 2012.

[9] ——, "CEN-CENELEC-ETSI Smart Grid Coordination Group Smart Grid Reference Architecture," CEN-CENELEC-ETSI Smart Grid Coordination Group, Tech. Rep., 2012.

[10] J. C. L. Chan and D. S. Wong, "Cyber attacks and the smart grid," *IEEE SmartGrid news letter*, no. 10, 2015.

[11] J. Wu, S. Guo, J. Li, and D. Zeng, "Big data meet green challenges: big data toward green applications," *IEEE Systems Journal*, vol. 10, no. 3, pp. 888–900, 2016.

[12] ——, "Big data meet green challenges: Greening big data," *IEEE Systems Journal*, vol. 10, no. 3, pp. 873–887, 2016.

[13] N. Uribe-Pérez, L. Hernández, D. de la Vega, and I. Angulo, "State of the art and trends review of smart metering in electricity grids," *Applied Sciences*, vol. 6, no. 3, p. 68, 2016.

[14] "Directive 2012/27/eu of the european parliament and of the council of 25 october 2012 on energy efficiency, amending directives 2009/125/ec and 2010/30/eu and repealing directives 2004/8/ec and 2006/32/ec text with eea relevance." [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32012L0027

[15] J. Wu, S. Guo, H. Huang, W. Liu, and Y. Xiang, "Information and communications technologies for sustainable development goals: State-of-the-art, needs and perspectives," *IEEE Communications Surveys & Tutorials*, 2018.

[16] H. Khurana, M. Hadley, N. Lu, and D. A. Frincke, "Smart-grid security issues," *IEEE Security & Privacy*, vol. 1, no. 8, pp. 81–85, 2010.

[17] Y. Wang, Q. Chen, T. Hong, and C. Kang, "Review of smart meter data analytics: Applications, methodologies, and challenges," *IEEE Transactions on Smart Grid*, pp. 1–1, 2018.

[18] "Advanced persistent threat activity targeting energy and other critical infrastructure sectors." [Online]. Available: https://www.us-cert.gov/ncas/alerts/TA17-293A

[19] "Cyberattack suspected in Ukraine power outage," http://www.pcworld.com/article/3152010/security/cyberattack-suspected-in-ukraine-power-outage.html.

[20] "Ukraine's Power Grid Gets Hacked Again, a Worrying Sign for Infrastructure Attacks," https://www.technologyreview.com/s/603262/ukraines-power-grid-gets-hacked-again-a-worrying-sign-for\\-infrastructure-attacks/.

[21] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in smart grid and smart home security: Issues, challenges and countermeasures," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 1933–1954, 2014.

[22] K. Weaver, "A perspective on how smart meters invade individual privacy," 2014.

[23] S. Finster and I. Baumgart, "Privacy-aware smart metering: A survey," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 2, pp. 1088–1101, 2015.

[24] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," *Computer Networks*, vol. 57, no. 5, pp. 1344–1371, 2013.

[25] S. Tan, D. De, W.-Z. Song, J. Yang, and S. K. Das, "Survey of security advances in smart grid: A data driven approach," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 397–422, 2017.

[26] H. He and J. Yan, "Cyber-physical attacks and defences in the smart grid: a survey," *IET Cyber-Physical Systems: Theory & Applications*, vol. 1, no. 1, pp. 13–27, 2016.

[27] M. R. Asghar, G. Dán, D. Miorandi, and I. Chlamtac, "Smart meter data privacy: A survey," *IEEE Communications Surveys & Tutorials*, 2017.

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

[29] Y. Kabalci, "A survey on smart metering and smart grid communication," *Renewable and Sustainable Energy Reviews*, vol. 57, no. Supplement C, pp. 302 – 318, 2016.

[30] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, "A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services," *IEEE Communications Surveys Tutorials*, pp. 1–1, 2018.

[31] X. Fan and G. Gong, "Security challenges in smart-grid metering and control systems," *Technology Innovation Management Review*, vol. 3, no. 7, p. 42, 2013.

[32] K. Sharma and L. M. Saini, "Performance analysis of smart metering for smart grid: An overview," *Renewable and Sustainable Energy Reviews*, vol. 49, pp. 720–735, 2015.

[33] P. Kumar, A. Braeken, A. Gurtov, J. Iinatti, and P. H. Ha, "Anonymous secure framework in connected smart home environments," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 4, pp. 968–979, 2017.

[34] "Smart Metering Equipment Technical Specifications," https://www.gov.uk/government/consultations/smart-metering-equipment-technical-specifications-second-version.

[35] F. Gómez-Cuba, R. Asorey-Cacheda, and F. J. González-Castaño, "Wimax for smart grid last-mile communications: Tos traffic mapping and performance assessment," in *Innovative Smart Grid Technologies (ISGT Europe), 2012 3rd IEEE PES International Conference and Exhibition on*. IEEE, 2012, pp. 1–8.

[36] F. Aalamifar and L. Lampe, "Optimized wimax profile configuration for smart grid communications," *IEEE Transactions on Smart Grid*, vol. 8, no. 6, pp. 2723–2732, Nov 2017.

[37] S. Zahurul, N. Mariun, I. Grozescu, H. Tsuyoshi, Y. Mitani, M. Othman, H. Hizam, and I. Abidin, "Future strategic plan analysis for integrating distributed renewable generation to smart grid through wireless sensor network: Malaysia prospect," *Renewable and Sustainable Energy Reviews*, vol. 53, pp. 978–992, 2016.

[38] R. Mao and V. Julka, "Wimax for advanced metering infrastructure," in *Green and Ubiquitous Technology (GUT), 2012 International Conference on*. IEEE, 2012, pp. 15–19.

[39] F. Han, S. Zhao, L. Zhang, and J. Wu, "Survey of strategies for switching off base stations in heterogeneous networks for greener 5g systems," *IEEE Access*, vol. 4, pp. 4959–4973, 2016.

[40] N. S. Nafi, K. Ahmed, M. A. Gregory, and M. Datta, "A survey of smart grid architectures, applications, benefits and standardization," *Journal of Network and Computer Applications*, vol. 76, pp. 23–36, 2016.

[41] T. N. Le, W.-L. Chin, and H.-H. Chen, "Standardization and security for smart grid communications based on cognitive radio technologies—a comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 423–445, 2017.

[42] "Smart Grid Standardization Analysis, version 2; Smart Grids and Energy Markets (SGEM)," https://portal.cleen.fi/.

[43] R. Atat, L. Liu, H. Chen, J. Wu, H. Li, and Y. Yi, "Enabling cyber-physical communication in 5g cellular networks: challenges, spatial spectrum sensing, and cyber-security," *IET Cyber-Physical Systems: Theory & Applications*, vol. 2, no. 1, pp. 49–54, 2017.

[44] J. Wu, "Green wireless communications: from concept to reality [industry perspectives]," *IEEE Wireless Communications*, vol. 19, no. 4, 2012.

[45] J. An, K. Yang, J. Wu, N. Ye, S. Guo, and Z. Liao, "Achieving sustainable ultra-dense heterogeneous networks for 5g," *IEEE Communications Magazine*, vol. 55, no. 12, pp. 84–90, 2017.

[46] R. Hidalgo-León, C. Sanchez-Zurita, P. Jácome-Ruiz, J. Wu, and Y. Muñoz-Jadan, "Roles, challenges, and approaches of droop control methods for microgrids," in *2017 IEEE PES Innovative Smart Grid Technologies Conference - Latin America (ISGT Latin America)*, Sept 2017, pp. 1–6.

[47] C. Zhou, R. Feng, L. Wang, W. Huang, and Y. Guo, "Security attack detection algorithm for electric power gis system based on mobile application," *IOP Conference Series: Earth and Environmental Science*, vol. 64, no. 1, p. 012101, 2017. [Online]. Available: http://stacks.iop.org/1755-1315/64/i=1/a=012101

[48] W. Luan, J. Peng, M. Maras, J. Lo, and B. Harapnuk, "Smart meter data analytics for distribution network connectivity verification," *IEEE Transactions on Smart Grid*, vol. 6, no. 4, pp. 1964–1971, 2015.

[49] S. Pathak, "Leveraging gis mapping and smart metering for improved oms and saidi for smart city," in *2016 Saudi Arabia Smart Grid (SASG)*, Dec 2016, pp. 1–5.

[50] P. Balakrishna, K. Rajagopal, and K. Swarup, "Distribution automation analysis based on extended load data from ami systems integration," *International Journal of Electrical Power and Energy Systems*, vol. 86, no. Supplement C, pp. 154 – 162, 2017.

[51] G. Kumar and N. M. Pindoriya, "Outage management system for power distribution network," in *2014 International Conference on Smart Electric Grid (ISEG)*, Sept 2014, pp. 1–8.

[52] P. Siano, "Demand response and smart grids—a survey," *Renewable and Sustainable Energy Reviews*, vol. 30, pp. 461–478, 2014.

[53] M. Pipattanasomporn, M. Kuzlu, and S. Rahman, "An algorithm for intelligent home energy management and demand response analysis," *IEEE Transactions on Smart Grid*, vol. 3, no. 4, pp. 2166–2173, 2012.

[54] "Smart Grid Resource Center," http://smartgrid.epri.com/Repository/Repository.aspx.

[55] "Analysis of the Cyber Attack on the Ukrainian Power Grid," https://ics.sans.org/media/E-ISAC˙SANS˙Ukraine˙DUC˙5.pdf.

[56] C. Wueest, "Targeted attacks against the energy sector."

[57] "Locus energy lgate command injection vulnerability," 2016. [Online]. Available: https://ics-cert.us-cert.gov/advisories/ICSA-16-231-01-0

[58] "Xzeres 442sr wind turbine cross-site scripting vulnerability," 2016. [Online]. Available: https://ics-cert.us-cert.gov/advisories/ICSA-15-342-01

[59] P. Yi, T. Zhu, Q. Zhang, Y. Wu, and L. Pan, "Puppet attack: A denial of service attack in advanced metering infrastructure network," *Journal of Network and Computer Applications*, vol. 59, pp. 325–332, 2016.

[60] G. Alberto and V. Javier, "Lights off! the darkness of the smart meters."

[61] D. Tellbach and Y.-F. Li, "Cyber-attacks on smart meters in household nanogrid: Modeling, simulation and analysis," *Energies*, vol. 11, no. 2, 2018.

[62] "Cyber-Attack Against Ukrainian Critical Infrastructure," https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

[63] "Rle nova-wind turbine hmi unsecure credentials vulnerability," 2016. [Online]. Available: https://ics-cert.us-cert.gov/advisories/ICSA-15-162-01A

[64] "Sinapsi esolar light plaintext passwords vulnerability," 2016. [Online]. Available: https://ics-cert.us-cert.gov/advisories/ICSA-15-160-02

[65] C. Carter, I. Onunkwo, P. Cordeiro, and J. Johnson, "Cyber security assessment of distributed energy resources."

[66] "Smart grid threat landscape and good practice guide."

[67] S. Ali, T. Al Balushi, Z. Nadir, and O. K. Hussain, *Embedded Systems Security for Cyber-Physical Systems*. Cham: Springer International Publishing, 2018, pp. 115–140. [Online]. Available: https://doi.org/10.1007/978-3-319-75880-0_6

[68] D.-d. CHEN, Z.-q. LI, L. Tian, M.-x. TENG, and X. Feng, "Big data based intrusion detection of smart meters," *DEStech Transactions on Computer Science and Engineering*, no. cnsce, 2017.

[69] K. Fu, A. Drobnis, G. Morrisett, E. Mynatt, S. Patel, R. Poovendran, and B. Zorn, "Safety and security for intelligent infrastructure," *arXiv preprint arXiv:1705.02002*, 2017.

[70] S. Tweneboah-Koduah, A. K. Tsetse, J. Azasoo, and B. Endicott-Popovsky, "Evaluation of cybersecurity threats on smart metering system," in *Information Technology - New Generations*, S. Latifi, Ed. Cham: Springer International Publishing, 2018, pp. 199–207.

[71] P. Morgner, S. Mattejat, Z. Benenson, C. Müller, and F. Armknecht, "Insecure to the touch: attacking zigbee 3.0 via touchlink commissioning," in *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. ACM, 2017, pp. 230–240.

[72] J. Yao, P. Venkitasubramaniam, S. Kishore, L. V. Snyder, and R. S. Blum, "Network topology risk assessment of stealthy cyber attacks on advanced metering infrastructure networks," in *2017 51st Annual Conference on Information Sciences and Systems (CISS)*, March 2017, pp. 1–6.

[73] S. Bhattacharjee, A. Thakur, and S. K. Das, "Towards fast and semi-supervised identification of smart meters launching data falsification attacks," in *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*, ser. ASIACCS '18. ACM, 2018, pp. 173–185. [Online]. Available: http://doi.acm.org/10.1145/3196494.3196551

[74] E. Inga, S. Cespedes, R. Hincapie, and C. A. Cardenas, "Scalable route map for advanced metering infrastructure based on optimal routing of wireless heterogeneous networks," *IEEE Wireless Communications*, vol. 24, no. 2, pp. 26–33, April 2017.

[75] "Realising the potential of demand-side response to 2025." [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/657144/DSR_Summary_Report.pdf

[76] {http://www.silverspringnet.com/wp-content/uploads/silverspringwhitepaper-smartgridsecurity-mythsreality-080814.pdf}, title=Smart Grid security myths vs. reality,.

[77] "What's at Risk as We Get Smarter?" http://smartgrid.ieee.org/newsletters/april-2012/what-s-at-risk-as-we-get-smarter.

[78] "NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0," http://dx.doi.org/10.6028/NIST.SP.1108r3.

[79] A. Bari, J. Jiang, W. Saad, and A. Jaekel, "Challenges in the smart grid applications: an overview," *International Journal of Distributed Sensor Networks*, vol. 2014, 2014.

[80] "Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements," http://dx.doi.org/10.6028/NIST.IR.7628r1.

[81] "Functional reference architecture for communications in smart metering systems," CEN/CLC/ETSI, Tech. Rep., 2011, ftp://ftp.cen.eu/cen/Sectors/List/Measurement/Smartmeters/CENCLCETSI_TR50572.pdf, accessed at 11 October 2016.

[82] V. Mai and I. Khalil, "Design and implementation of a secure cloud-based billing model for smart meters as an internet of things using homomorphic cryptography," *Future Generation Computer Systems*, vol. 72, pp. 327–338, 2017.

[83] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 4, pp. 998–1010, 2012.

[84] J. Liu, Y. Xiao, and J. Gao, "Achieving accountability in smart grid," *IEEE Systems Journal*, vol. 8, no. 2, pp. 493–508, 2014.

[85] J. Hajny, P. Dzurenda, and L. Malina, *Privacy-Enhanced Data Collection Scheme for Smart-Metering*, 2016, pp. 413–429.

[86] H. Nicanfar, P. TalebiFard, A. Alasaad, and V. C. Leung, "Enhanced network coding to maintain privacy in smart grid communication," *IEEE Transactions on Emerging Topics in Computing*, vol. 1, no. 2, pp. 286–296, 2013.

[87] V. Tudor, M. Almgren, and M. Papatriantafilou, "Analysis of the impact of data granularity on privacy for the smart grid," in *Proceedings of the 12th ACM workshop on Workshop on privacy in the electronic society*. ACM, 2013, pp. 61–70.

[88] S. Goel, "Anonymity vs. security: The right balance for the smart grid."

[89] A. Pfitzmann and M. Hansen, "A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management," 2010.

[90] A. Paverd, M. Andrew, and B. Ian, "Modelling and automatically analysing privacy properties for honest-but-curious adversaries," University of Oxford, Tech. Rep., 2014, https://www.cs.ox.ac.uk/people/andrew.paverd/casper/casper-privacy-report.pdf, accessed at 11 October 2016.

[91] S. Kaplantzis and Y. A. Şekercioğlu, "Security and smart metering," in *European Wireless, 2012. EW. 18th European Wireless Conference*. VDE, 2012, pp. 1–8.

[92] N. Saxena and S. Grijalva, "Efficient signature scheme for delivering authentic control commands in the smart grid," *IEEE Transactions on Smart Grid*, 2017.

[93] O. Ur-Rehman, N. Zivic, and C. Ruland, "Security issues in smart metering systems," in *Smart Energy Grid Engineering (SEGE), 2015 IEEE International Conference on*. IEEE, 2015, pp. 1–7.

[94] "Electricity Grid in U.S. Penetrated By Spies," http://www.wsj.com/articles/SB123914805204099085.

[95] S. Asri and B. Pranggono, "Impact of distributed denial-of-service attack on advanced metering infrastructure," *Wireless Personal Communications*, vol. 83, no. 3, pp. 2211–2223, 2015.

[96] B. Vaidya, D. Makrakis, and H. Mouftah, "Secure communication mechanism for ubiquitous smart grid infrastructure," *The Journal of Supercomputing*, pp. 1–21, 2013.

[97] D. Mashima, P. Gunathilaka, and B. Chen, "Artificial command delaying for secure substation remote control: Design and implementation," *IEEE Transactions on Smart Grid*, vol. PP, no. 99, pp. 1–1, 2017.

[98] R. Khan, P. Maynard, K. McLaughlin, D. Laverty, and S. Sezer, "Threat analysis of blackenergy malware for synchrophasor based real-time control and monitoring in smart grid." in *ICS-CSR*, 2016.

[99] N. Saputro and K. Akkaya, "PARP-S: A secure piggybacking-based ARP for IEEE 802.11 s-based Smart Grid AMI networks," *Computer Communications*, vol. 58, pp. 16–28, 2015.

[100] Z. A. Baig and A.-R. Amoudi, "An analysis of smart grid attacks and countermeasures," *Journal of Communications*, vol. 8, no. 8, pp. 473–479, 2013.

[101] 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*, vol. 8, no. 2, pp. 509–520, 2014.

[102] Z. Yang, P. Cheng, and J. Chen, "Learning-based jamming attack against low-duty-cycle networks," *IEEE Transactions on Dependable and Secure Computing*, vol. PP, no. 99, pp. 1–1, 2015.

[103] K. Gai, M. Qiu, Z. Ming, H. Zhao, and L. Qiu, "Spoofing-jamming attack strategy using optimal power distributions in wireless smart grid networks," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2431–2439, 2017.

[104] A. A. Khan, M. H. Rehmani, and M. Reisslein, "Requirements, design challenges, and review of routing and mac protocols for cr-based smart grid systems," *IEEE Communications Magazine*, vol. 55, no. 5, pp. 206–215, 2017.

[105] J. Ma, Y. Liu, L. Song, and Z. Han, "Multiact dynamic game strategy for jamming attack in electricity market," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2273–2282, 2015.

[106] J. Lin, W. Yu, X. Yang, G. Xu, and W. Zhao, "On false data injection attacks against distributed energy routing in smart grid," in *Cyber-Physical Systems (ICCPS), 2012 IEEE/ACM Third International Conference on*, April 2012, pp. 183–192.

[107] Y. Wang, T. T. Gamage, and C. H. Hauser, "Security implications of transport layer protocols in power grid synchrophasor data communication," *IEEE Transactions on Smart Grid*, vol. 7, no. 2, pp. 807–816, March 2016.

[108] K. Shuaib, Z. Trabelsi, M. Abed-Hafez, A. Gaouda, and M. Alahmad, "Resiliency of smart power meters to common security attacks," *Procedia Computer Science*, vol. 52, pp. 145 – 152, 2015.

[109] A. A. Khan, M. H. Rehmani, and M. Reisslein, "Cognitive radio for smart grids: Survey of architectures, spectrum sensing mechanisms, and networking protocols," *IEEE Communications Surveys Tutorials*, vol. 18, no. 1, pp. 860–898, Firstquarter 2016.

[110] A. I. Sabbah, A. El-Mougy, and M. Ibnkahla, "A survey of networking challenges and routing protocols in smart grids," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 1, pp. 210–221, 2014.

[111] W. Meng, R. Ma, and H.-H. Chen, "Smart grid neighborhood area networks: a survey," *IEEE Network*, vol. 28, no. 1, pp. 24–32, 2014.

[112] S. McLaughlin, D. Podkuiko, and P. McDaniel, "Energy theft in the advanced metering infrastructure," in *International Workshop on Critical Information Infrastructures Security*. Springer, 2009, pp. 176–187.

[113] Z. Zhou, "Design and implementation about secure smart electricity meter sealing based on rf tag," *International Journal of Security and Its Applications*, vol. 9, no. 6, pp. 79–88, 2015.

[114] W. Han and Y. Xiao, "Nfd: Non-technical loss fraud detection in smart grid," *Computers & Security*, vol. 65, pp. 187–201, 2017.

[115] V. M. Viswanatham, A. Chari, and V. Saritha, "Region-based group and hierarchical key management for secure smart grid communications," *International Journal of Smart Grid and Green Communications*, vol. 1, no. 1, pp. 50–61, 2016.

[116] "Security in the smart grid," http://www02.abb.com/db/db0003/db002698.nsf/0/832c29e54746dd0fc12576400024ef16/$file/paper_Security+in+the+Smart+Grid+%28Sept+09%29_docnum.pdf.

[117] E. McCary and Y. Xiao, "Smart grid attacks and countermeasures," *EAI Endorsed Transactions on Industrial Networks and Intelligent Systems*, vol. 15, no. 2, 2 2015.

[118] "Battling threats in smart grid supply chain," http://pdfserv.maximintegrated.com/en/an/AN5926.pdf.

[119] S. Werner and J. Lundén, "Smart load tracking and reporting for real-time metering in electric power grids," *IEEE Transactions on Smart Grid*, vol. 7, no. 3, pp. 1723–1731, May 2016.

[120] Y. Gong, Y. Cai, Y. Guo, and Y. Fang, "A privacy-preserving scheme for incentive-based demand response in the smart grid," *IEEE Transactions on Smart Grid*, vol. 7, no. 3, pp. 1304–1313, May 2016.

[121] M. Mahmoud, N. Saputro, P. Akula *et al.*, "Privacy-preserving power injection over a hybrid ami/lte smart grid network," *IEEE Internet of Things Journal*, 2017.

[122] Y. Zhang, J. Zhao, and D. Zheng, "Efficient and privacy-aware power injection over ami and smart grid slice in future 5g networks," *Mobile Information Systems*, vol. 2017, 2017.

[123] Y. Kim, V. Kolesnikov, and M. Thottan, "Resilient end-to-end message protection for cyber-physical system communications," *IEEE Transactions on Smart Grid*, vol. PP, no. 99, pp. 1–1, 2016.

[124] A. Paverd, A. Martin, and I. Brown, "Privacy-enhanced bi-directional communication in the smart grid using trusted computing," in *Smart Grid Communications (SmartGridComm), 2014 IEEE International Conference on*. IEEE, 2014, pp. 872–877.

[125] A. J. Paverd, "Enhancing communication privacy using trustworthy remote entities," Ph.D. dissertation, University of Oxford, 2015.

[126] P. Ponnaganti, J. R. Pillai, and B. Bak-Jensen, "Opportunities and challenges of demand response in active distribution networks," *Wiley Interdisciplinary Reviews: Energy and Environment*, 2017.

[127] A. Paverd, A. Martin, and I. Brown, "Security and privacy in smart grid demand response systems," in *Smart Grid Security: Second International Workshop, SmartGridSec 2014, Munich, Germany, February 26, 2014, Revised Selected Papers*, J. Cuellar, Ed. Cham: Springer International Publishing, 2014, pp. 1–15.

[128] R. d. T. Caropreso, R. A. S. Fernandes, D. P. M. Osorio, and I. N. da Silva, "An open source framework for smart meters: Data communication and security traffic analysis," *IEEE Transactions on Industrial Electronics*, pp. 1–1, 2018.

[129] M. M. Hasan and H. T. Mouftah, "Cloud-centric collaborative security service placement for advanced metering infrastructures," *IEEE Transactions on Smart Grid*, pp. 1–1, 2018.

[130] L. Duan, D. Liu, Y. Zhang, S. Chen, R. P. Liu, B. Cheng, and J. Chen, "Secure data-centric access control for smart grid services based on publish/subscribe systems," *ACM Transactions on Internet Technology (TOIT)*, vol. 16, no. 4, p. 23, 2016.

[131] E. Smith, S. Corzine, D. Racey, P. Dunne, C. Hassett, and J. Weiss, "Going beyond cybersecurity compliance: What power and utility companies really need to consider," *IEEE Power and Energy Magazine*, vol. 14, no. 5, pp. 48–56, Sept 2016.

[132] "Vulnerabilities in openssl." [Online]. Available: https://www.openssl.org/news/vulnerabilities.html

[133] M. Wan, W. Shang, P. Zeng, and J. Zhao, "SRDA: A Secure Routing and Data Aggregation Approach for Wireless Smart Meter," *Journal of Communications*, vol. 11, no. 1, 2016.

[134] J. Wei and D. Kundur, "Goalie: Goal-seeking obstacle and collision evasion for resilient multicast routing in smart grid," *IEEE Transactions on Smart Grid*, vol. 7, no. 2, pp. 567–579, 2016.

[135] D. Sahin, V. C. Gungor, T. Kocak, and G. Tuna, "Quality-of-service differentiation in single-path and multi-path routing for wireless sensor network-based smart grid applications," *Ad Hoc Networks*, vol. 22, pp. 43–60, 2014.

[136] S.-G. Yoon, S. Jang, Y.-H. Kim, and S. Bahk, "Opportunistic routing for smart grid with power line communication access networks," *IEEE Transactions on Smart Grid*, vol. 5, no. 1, pp. 303–311, 2014.

[137] Q.-D. Ho, Y. Gao, G. Rajalingham, and T. Le-Ngoc, "Performance and applicability of candidate routing protocols for smart grid's wireless mesh neighbor area networks," in *2014 IEEE International Conference on Communications (ICC)*. IEEE, 2014, pp. 3682–3687.

[138] S. Misra, P. V. Krishna, V. Saritha, H. Agarwal, and A. Ahuja, "Learning automata-based multi-constrained fault-tolerance approach for effective energy management in smart grid communication network," *Journal of Network and Computer Applications*, vol. 44, pp. 212–219, 2014.

[139] M. Yigit, V. C. Gungor, E. Fadel, L. Nassef, N. Akkari, and I. F. Akyildiz, "Channel-aware routing and priority-aware multi-channel scheduling for wsn-based smart grid applications," *Journal of Network and Computer Applications*, vol. 71, pp. 50–58, 2016.

[140] C. Taylor and T. Johnson, "Strong authentication countermeasures using dynamic keying for sinkhole and distance spoofing attacks in smart grid networks," in *2015 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 2015, pp. 1835–1840.

[141] E. Hammad, J. Zhao, A. Farraj, and D. Kundur, "Mitigating link insecurities in smart grids via qos multi-constraint routing," in *Communications Workshops (ICC), 2016 IEEE International Conference on*. IEEE, 2016, pp. 380–386.

[142] F. Masoumiyan, Y. Mishra, Y.-C. Tian, and G. Ledwich, "Communication requirements of wide area control in smart grid," in *Proceedings of the 42nd IEEE Industrial Electronics Conference*. IEEE, 2016.

[143] A. Mohammadali, M. S. Haghighi, M. H. Tadayon, and A. M. Nodooshan, "A novel identity-based key establishment method for advanced metering infrastructure in smart grid," *IEEE Transactions on Smart Grid*, 2016.

[144] S. Mishra, T. N. Dinh, M. T. Thai, J. Seo, and I. Shin, "Optimal packet scan against malicious attacks in smart grids," *Theoretical Computer Science*, vol. 609, Part 3, pp. 606 – 619, 2016, computing and Combinatorics Conference.

[145] G. Lee, Y.-S. Kim, and J. Kang, *An Adaptive DoS Attack Mitigation Measure for Field Networks in Smart Grids*. Cham: Springer International Publishing, 2017, pp. 419–428.

[146] B. Hu and H. Gharavi, "Smart grid mesh network security using dynamic key distribution with merkle tree 4-way handshaking," *IEEE Transactions on Smart Grid*, vol. 5, no. 2, pp. 550–558, 2014.

[147] G. S. Toor and M. Ma, "Security enhancement for dynamic key refreshment in neighborhood area network of smart grid," *Security and Communication Networks*, vol. 9, no. 16, pp. 3353–3364, 2016.

[148] Z. Lu, W. Wang, and C. Wang, "Camouflage traffic: Minimizing message delay for smart grid applications under jamming," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 1, pp. 31–44, Jan 2015.

[149] M. Hoefling, F. Heimgaertner, D. Fuchs, and M. Menth, *jOSEF: A Java-Based Open-Source Smart Meter Gateway Experimentation Framework*. Cham: Springer International Publishing, 2015, pp. 165–176.

[150] O. Khaled, A. Marín, F. Almenares, P. Arias, and D. Díaz, "Analysis of secure tcp/ip profile in 61850 based substation automation system for smart grids," *International Journal of Distributed Sensor Networks*, vol. 12, no. 4, p. 5793183, 2016.

[151] U. S. Premarathne, I. Khalil, and M. Atiquzzaman, "Secure and reliable surveillance over cognitive radio sensor networks in smart grid," *Pervasive and Mobile Computing*, vol. 22, pp. 3–15, 2015.

[152] M. Mustapa, M. Niamat, A. P. D. Nath, and M. Alam, "Hardware-oriented authentication for advanced metering infrastructure," *IEEE Transactions on Smart Grid*, 2017.

[153] S.-C. Yip, K. Wong, W.-P. Hew, M.-T. Gan, R. C.-W. Phan, and S.-W. Tan, "Detection of energy theft and defective smart meters in smart

grids using linear regression," *International Journal of Electrical Power & Energy Systems*, vol. 91, pp. 230–240, 2017.

[154] H. J. Jo, I. S. Kim, and D. H. Lee, "Efficient and privacy-preserving metering protocols for smart grid systems," *IEEE Transactions on Smart Grid*, vol. 7, no. 3, pp. 1732–1742, 2016.

[155] J. Ni, K. Zhang, X. Lin, and X. Shen, "Balancing security and efficiency for smart metering against misbehaving collectors," *IEEE Transactions on Smart Grid*, 2017.

[156] I. Parvez, F. Abdul, and A. I. Sarwat, "A location based key management system for advanced metering infrastructure of smart grid," in *Green Technologies Conference (GreenTech), 2016 IEEE*. IEEE, 2016, pp. 62–67.

[157] M. Raciti and S. Nadjm-Tehrani, "Embedded cyber-physical anomaly detection in smart meters," in *International Workshop on Critical Information Infrastructures Security*. Springer, 2012, pp. 34–45.

[158] N. Saxena and S. Grijalva, "Dynamic secrets and secret keys based scheme for securing last mile smart grid wireless communication," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 3, pp. 1482–1491, 2017.

[159] T. Liu, Y. Liu, Y. Mao, Y. Sun, X. Guan, W. Gong, and S. Xiao, "A dynamic secret-based encryption scheme for smart grid wireless communication," *IEEE Transactions on Smart Grid*, vol. 5, no. 3, pp. 1175–1182, 2014.

[160] C.-I. Fan, S.-Y. Huang, and Y.-L. Lai, "Privacy-enhanced data aggregation scheme against internal attackers in smart grid," *IEEE Transactions on Industrial informatics*, vol. 10, no. 1, pp. 666–675, 2014.

[161] M. Wen, R. Lu, K. Zhang, J. Lei, X. Liang, and X. Shen, "Parq: A privacy-preserving range query scheme over encrypted metering data for smart grid," *IEEE Transactions on Emerging Topics in Computing*, vol. 1, no. 1, pp. 178–191, 2013.

[162] J. Seo, J. Jin, J. Y. Kim, and J.-J. Lee, "Automated residential demand response based on advanced metering infrastructure network," *International Journal of Distributed Sensor Networks*, vol. 12, no. 2, p. 4234806, 2016.

[163] S. Tonyali, K. Akkaya, N. Saputro, and A. S. Uluagac, "A reliable data aggregation mechanism with homomorphic encryption in smart grid ami networks," in *2016 13th IEEE Annual Consumer Communications Networking Conference (CCNC)*, Jan 2016, pp. 550–555.

[164] N. Busom, R. Petrlic, F. Sebé, C. Sorge, and M. Valls, "Efficient smart metering based on homomorphic encryption," *Computer Communications*, vol. 82, pp. 95–101, 2016.

[165] F. Borges, D. Demirel, L. Böck, J. Buchmann, and M. Mühlhäuser, "A privacy-enhancing protocol that provides in-network data aggregation and verifiable smart meter billing," in *2014 IEEE Symposium on Computers and Communications (ISCC)*. IEEE, 2014, pp. 1–6.

[166] A. Barletta, C. Callegari, S. Giordano, M. Pagano, and G. Procissi, "Privacy preserving smart grid communications by verifiable secret key sharing," in *2015 International Conference on Computing and Network Communications (CoCoNet)*. IEEE, 2015, pp. 199–204.

[167] M. Cazorla, K. Marquet, and M. Minier, "Survey and benchmark of lightweight block ciphers for wireless sensor networks," in *Security and Cryptography (SECRYPT), 2013 International Conference on*. IEEE, 2013, pp. 1–6.

[168] J. Lee, K. Kapitanova, and S. H. Son, "The price of security in wireless sensor networks," *Computer Networks*, vol. 54, no. 17, pp. 2967–2978, 2010.

[169] A. Trad, A. A. Bahattab, and S. B. Othman, "Performance trade-offs of encryption algorithms for wireless sensor networks," in *Computer Applications and Information Systems (WCCAIS), 2014 World Congress on*. IEEE, 2014, pp. 1–6.

[170] J. H. Kong, L.-M. Ang, and K. P. Seng, "A comprehensive survey of modern symmetric cryptographic solutions for resource constrained environments," *Journal of Network and Computer Applications*, vol. 49, pp. 15 – 50, 2015.

[171] D. Meyer and F. Baker, "Internet protocols for the smart grid," 2011. [Online]. Available: https://tools.ietf.org/html/rfc6272

[172] N. E. Petroulakis, E. Z. Tragos, A. G. Fragkiadakis, and G. Spanoudakis, "A lightweight framework for secure life-logging in smart environments," *Information Security Technical Report*, vol. 17, no. 3, pp. 58–70, 2013.

[173] Y. Lu, "Privacy-preserving logarithmic-time search on encrypted data in cloud." in *NDSS*. The Internet Society, 2012.

[174] J. B. Hur, D. Y. Koo, and Y. J. Shin, "Privacy-preserving smart metering with authentication in a smart grid," *Applied Sciences*, vol. 5, no. 4, p. 1503, 2015.

[175] K.-A. Shim, "A survey of public-key cryptographic primitives in wireless sensor networks," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 577–601, 2016.

[176] S. B. Sasi, D. Dixon, J. Wilson, and P. No, "A general comparison of symmetric and asymmetric cryptosystems for wsns and an overview of location based encryption technique for improving security," *IOSR Journal of Engineering*, vol. 4, no. 3, p. 1, 2014.

[177] J. Ni, K. Zhang, K. Alharbi, X. Lin, N. Zhang, and X. S. Shen, "Differentially private smart metering with fault tolerance and range-based filtering," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2483–2493, 2017.

[178] J. Won, C. Y. Ma, D. K. Yau, and N. S. Rao, "Privacy-assured aggregation protocol for smart metering: A proactive fault-tolerant approach," *IEEE/ACM Transactions on Networking (TON)*, vol. 24, no. 3, pp. 1661–1674, 2016.

[179] A. Abdallah and X. Shen, "Lightweight security and privacy preserving scheme for smart grid customer-side networks," *IEEE Transactions on Smart Grid*, vol. 8, no. 3, pp. 1064–1074, 2017.

[180] M. S. Rahman, A. Basu, and S. Kiyomoto, "Privacy-friendly secure bidding scheme for demand response in smart grid," in *Smart Cities Conference (ISC2), 2015 IEEE First International*. IEEE, 2015, pp. 1–6.

[181] M. S. Rahman, A. Basu, S. Kiyomoto, and M. A. Bhuiyan, "Privacy-friendly secure bidding for smart grid demand-response," *Information Sciences*, vol. 379, pp. 229–240, 2017.

[182] M. A. Mustafa, N. Zhang, G. Kalogridis, and Z. Fan, "Musp: Multi-service, user self-controllable and privacy-preserving system for smart metering," in *Communications (ICC), 2015 IEEE International Conference on*. IEEE, 2015, pp. 788–794.

[183] C. Esposito and M. Ciampi, "On security in publish/subscribe services: a survey," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 2, pp. 966–997.

[184] C. Rottondi, G. Verticale, and A. Capone, "A security framework for smart metering with multiple data consumers," in *Computer Communications Workshops (INFOCOM WKSHPS), 2012 IEEE Conference on*. IEEE, 2012, pp. 103–108.

[185] X. He, M.-O. Pun, and C. C. J. Kuo, "Secure and efficient cryptosystem for smart grid using homomorphic encryption," in *2012 IEEE PES Innovative Smart Grid Technologies (ISGT)*, Jan 2012, pp. 1–8.

[186] X. Liang, X. Li, R. Lu, X. Lin, and X. Shen, "Udp: Usage-based dynamic pricing with privacy preservation for smart grid," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 141–150, March 2013.

[187] H. Li, X. Lin, H. Yang, X. Liang, R. Lu, and X. Shen, "EPPDR: An efficient privacy-preserving demand response scheme with adaptive key evolution in smart grid," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 8, pp. 2053–2064, Aug 2014.

[188] M. M. Fouda, Z. M. Fadlullah, N. Kato, R. Lu, and X. S. Shen, "A lightweight message authentication scheme for smart grid communications," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 675–685, 2011.

[189] P. Kumar, A. Gurtov, and P. H. Ha, "An efficient authentication model in smart grid networks," in *2016 15th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN)*. IEEE, 2016, pp. 1–2.

[190] K. Mahmood, S. A. Chaudhry, H. Naqvi, T. Shon, and H. F. Ahmad, "A lightweight message authentication scheme for smart grid communications in power sector," *Computers & Electrical Engineering*, 2016.

[191] P. Kumar, A. Gurtov, M. Sain, A. Martin, and P. H. Ha, "Lightweight authentication and key agreement for smart metering in smart energy networks," *IEEE Transactions on Smart Grid*, pp. 1–1, 2018.

[192] T. W. Chim, S. M. Yiu, V. O. K. Li, L. C. K. Hui, and J. Zhong, "PRGA: Privacy-Preserving Recording amp; Gateway-Assisted Authentication of Power Usage Information for Smart Grid," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 1, pp. 85–97, Jan 2015.

[193] L. Zhang, S. Tang, and H. Luo, "Elliptic curve cryptography-based authentication with identity protection for smart grids," *PloS one*, vol. 11, no. 3, p. e0151253, 2016.

[194] Y. Liu, C. Cheng, T. Gu, T. Jiang, and X. Li, "A lightweight authenticated communication scheme for smart grid," *IEEE Sensors Journal*, vol. 16, no. 3, pp. 836–842, 2016.

[195] J. L. Tsai and N. W. Lo, "Secure anonymous key distribution scheme for smart grid," *IEEE Transactions on Smart Grid*, vol. 7, no. 2, pp. 906–914, March 2016.

[196] V. Odelu, A. K. Das, M. Wazid, and M. Conti, "Provably secure authenticated key agreement scheme for smart grid," *IEEE Transactions on Smart Grid*, vol. PP, no. 99, pp. 1–1, 2016.

[197] N. Saxena, B. J. Choi, and R. Lu, "Authentication and authorization scheme for various user roles and devices in smart grid," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 5, pp. 907–921, 2016.

[198] S. Ruj and A. Nayak, "A decentralized security framework for data aggregation and access control in smart grids," *IEEE transactions on smart grid*, vol. 4, no. 1, pp. 196–205, 2013.

[199] J. Baek, Q. H. Vu, J. K. Liu, X. Huang, and Y. Xiang, "A secure cloud computing based framework for big data information management of smart grid," *IEEE transactions on cloud computing*, vol. 3, no. 2, pp. 233–244, 2015.

[200] A. Mohan and D. Mashima, "Towards secure demand-response systems on the cloud," in *2014 IEEE International Conference on Distributed Computing in Sensor Systems*. IEEE, 2014, pp. 361–366.

[201] Y. Xie, H. Wen, J. Wu, Y. Jiang, J. Meng, X. Guo, A. Xu, and Z. Guan, "Three-layers secure access control for cloud-based smart grids," in *Vehicular Technology Conference (VTC Fall), 2015 IEEE 82nd*. IEEE, 2015, pp. 1–5.

[202] A. Braeken, P. Kumar, and A. Martin, "Efficient and provably secure key agreement for modern smart metering communications," *Energies*, vol. 11, no. 10, p. 2662, 2018.

[203] Braeken, An and Kumar, Pardeep and Martin, Andrew, "Efficient and privacy-preserving data aggregation and dynamic billing in smart grid metering networks," *Energies*, vol. 11, no. 8, p. 2085, 2018.

[204] M. T. Alam, "A review on cloud-based privacy preserving schemes for smart meters," *INFOCOMP Journal of Computer Science*, vol. 15, no. 1, pp. 19–33, 2016.

[205] L. Xiaobing, C. Wei, Z. Feng, X. Bin, and S. Zhiqiang, "Design of a security smart meter software testing cloud service system," in *2016 IEEE Information Technology, Networking, Electronic and Automation Control Conference*, May 2016, pp. 874–878.

[206] Z. Zhang, Z. Qin, L. Zhu, J. Weng, and K. Ren, "Cost-friendly differential privacy for smart meters: Exploiting the dual roles of the noise," *IEEE Transactions on Smart Grid*, vol. 8, no. 2, pp. 619–626, 2017.

[207] "Secure and scalable aggregation in the smart grid resilient against malicious entities," *Ad Hoc Networks*, vol. 50, no. Supplement C, pp. 58 – 67, 2016.

[208] D. He, S. Chan, and M. Guizani, "Cyber security analysis and protection of wireless sensor networks for smart grid monitoring," *IEEE Wireless Communications*, vol. PP, no. 99, pp. 2–7, 2017.

[209] S. Câmara, D. Anand, V. Pillitteri, and L. Carmo, *Multicast Delayed Authentication for Streaming Synchrophasor Data in the Smart Grid*. Cham: Springer International Publishing, 2016, pp. 32–46.

[210] P. J. Ollukaren, R. Swaminathan, S. L. King, K. W. McBee, J. C. Gutierrez, and M. Rodriguez-Perez, "Systems and methods for managing advanced metering infrastructure," May 8 2018, uS Patent 9,967,235.

[211] N. Cam-Winget, J. Hui, and D. Popa, "Applicability statement for the routing protocol for low-power and lossy networks (rpl) in advanced metering infrastructure (ami) networks," Tech. Rep., 2017.

[212] A. Shaik, R. Borgaonkar, J.-P. Seifert, N. Asokan, and V. Niemi, "Practical attacks against privacy and availability in 4g/lte," in *23nd Annual Network and Distributed System Security Symposium, NDSS 2016, San Diego, California, USA, February 21-24, 2016*, 2016. [Online]. Available: http://www.internetsociety.org/events/ndss-symposium-2016

[213] J. Wang, J. Liu, S. Yang, and M. Zhang, "Integrated trusted protection technologies for industrial control systems," in *2016 18th International Conference on Advanced Communication Technology (ICACT)*, Jan 2016, pp. 70–75.

[214] A. Mazloomzadeh, O. A. Mohammed, and S. Zonouzsaman, "Empirical development of a trusted sensing base for power system infrastructures," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2454–2463, Sept 2015.

[215] K. A. Küçük, A. Paverd, A. Martin, N. Asokan, A. Simpson, and R. Ankele, "Exploring the use of intel sgx for secure many-party applications," in *Proceedings of the 1st Workshop on System Software for Trusted Execution*, ser. SysTEX '16, New York, NY, USA, 2016, pp. 5:1–5:6.

[216] K. Wu, F. Chen, and Y. Li, "Research of remote attestation model and protocol ofinteractive terminals of smart grid," *International Journal of Grid and Distributed Computing*, vol. 7, no. 3, pp. 221–232, 2014.

[217] R. Ankele, K. A. Küçük, A. Martin, A. Simpson, and A. Paverd, "Applying the trustworthy remote entity to privacy-preserving multiparty computation: Requirements and criteria for large-scale applications."

[218] M. H. Gunes, M. Yuksel, and H. Ceker, "A blind processing framework to facilitate openness in smart grid communications," *Computer Networks*, vol. 86, pp. 14 – 26, 2015.

[219] J. Zhao, J. Liu, Z. Qin, and K. Ren, "Privacy protection scheme based on remote anonymous attestation for trusted smart meters," *IEEE Transactions on Smart Grid*, vol. PP, no. 99, pp. 1–1, 2016.

[220] J. T. Mühlberg, S. Cleemput, M. A. Mustafa, J. Van Bulck, B. Preneel, and F. Piessens, "An implementation of a high assurance smart meter using protected module architectures," in *IFIP International Conference on Information Security Theory and Practice*. Springer, 2016, pp. 53–69.

[221] F. Abdi, C.-Y. Chen, M. Hasan, S. Liu, S. Mohan, and M. Caccamo, "Restart-Based Security Mechanisms for Safety-Critical Embedded Systems," https://arxiv.org/pdf/1705.01520.pdf, 2017.

[222] L. Langer, F. Skopik, P. Smith, and M. Kammerstetter, "From old to new: Assessing cybersecurity risks for an evolving smart grid," *computers & security*, vol. 62, pp. 165–176, 2016.

[223] "Smart meter security survey." [Online]. Available: http://www.globalsmartgridfederation.org/wp-content/uploads/2016/08/smart_meter_security_survey.pdf

[224] S. E. Tan, S. C. K. Lye, Z. W. Siew, A. Kiring, and K. T. K. Teo, "Performance measurement of evolutionary routing protocol in network coding," in *2012 International Conference on Advanced Computer Science Applications and Technologies (ACSAT)*, Nov 2012, pp. 284–289.

[225] M. A. Rahman, A. Jakaria, and E. Al-Shaer, "Formal analysis for dependable supervisory control and data acquisition in smart grids," in *Dependable Systems and Networks (DSN), 2016 46th Annual IEEE/IFIP International Conference on*. IEEE, 2016, pp. 263–274.

[226] J. Y. NI Zhen-hua, LI Ya-lin, "Brief introduction of quantum secure communications and the application survey in state grid," *Electric Power Information and Communication Technology*, vol. 15, no. 10, p. 43, 2017. [Online]. Available: http://www.dlxxtx.com/EN/abstract/article_1526.shtml

[227] M. Kaur and S. Kalra, "Security in iot-based smart grid through quantum key distribution," in *Advances in Computer and Computational Sciences*, S. K. Bhatia, K. K. Mishra, S. Tiwari, and V. K. Singh, Eds. Singapore: Springer Singapore, 2018, pp. 523–530.

[228] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuéllar, P. H. Drielsma, P.-C. Héam, O. Kouchnarenko, J. Mantovani *et al.*, "The avispa tool for the automated validation of internet security protocols and applications," in *International Conference on Computer Aided Verification*. Springer, 2005, pp. 281–285.

[229] B. Blanchet, B. Smyth, and V. Cheval, "Proverif 1.90: Automatic cryptographic protocol verifier, user manual and tutorial," *URL: http://prosecco. gforge. inria. fr/personal/bblanche/proverif/manual. pdf*, 2015.

[230] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on information theory*, vol. 29, no. 2, pp. 198–208, 1983.

[231] G. Bai, J. Hao, J. Wu, Y. Liu, Z. Liang, and A. Martin, "Trustfound: Towards a formal foundation for model checking trusted computing platforms," in *International Symposium on Formal Methods*. Springer, 2014, pp. 110–126.

[232] A. Fawaz, R. Berthier, and W. H. Sanders, "A response cost model for advanced metering infrastructures," *IEEE Transactions on Smart Grid*, vol. 7, no. 2, pp. 543–553, March 2016.

[233] "Smart grid: Intergrative security assessment." [Online]. Available: http://publish.illinois.edu/integrative-security-assessment/

**Pardeep Kumar** (M'13) received the B.E. degree in computer science from Maharishi Dayanand University, Haryana (India), in 2002 and the M.Tech degree in computer science from Chaudhary Devilal University, Harnana (India), in 2006 and the Ph.D. degree in ubiquitous computing from Dongseo University, Busan (South Korea) in 2012. He is currently a Lecturer/Assistant Professor with the Department of Computer Science, Swansea University, Swansea, UK. From 2012 to 2018, he had held postdoc positions at the Department of Computer Science, Oxford University, Oxford UK (08/2016 - 09/2018), and at the Department of Computer Science, The Arctic University of Norway, Tromso, Norway (08/2015- 08/2016), and at Centre for Wireless Communications and the Department of Communications Engineering, University of Oulu, Finland (04/2012 to 08/2015). His research interests include security and privacy in connected smart environments, cyber physical systems and 5G networks.

**Yun Lin** is a Research Fellow in School of Computing, National University of Singapore. He received his Ph.D. degree from Fudan University, China, and B.S. degree from East China Normal University, China. His research interests include software engineering, program analysis, and cyber security.

**Guangdong Bai** received Bachelor and Master degrees in computing science from Peking University, China in 2008 and 2011. In 2015, he received PhD degrees in computing science from National University of Singapore (NUS). He worked as a postdoctoral Research Fellow in NUS and an Assistant Professor in Singapore Institute of Technology (SIT). He has been a faculty member of Griffith University since 2018. His research interests include cyber security, protocol verification, and software engineering.

**Andrew Parverd** obtained his B.Sc. degree in Electrical Engineering from the University of the Witwatersrand, Johannesburg, in 2010, his M.Sc. degree in Engineering from the University of Cape Town in 2012, and his DPhil in Computer Science from the University of Oxford in 2016. From 2015 to 2018 he was a post-doctoral researcher and subsequently a research fellow in the Secure Systems Group at Aalto University, Finland. In 2018 he was a Fulbright Cyber Security Scholar at the University of California, Irvine. Dr Paverd now works as a Researcher at Microsoft Research Cambridge, in collaboration with the Microsoft Security Response Centre. His research interests are broadly in the field of systems security.

**Jin Song Dong** received the bachelor's (hon I) and PhD degrees in computing from the University of Queensland, in 1992 and 1996, respectively. From 1995 to 1998, he was research scientist with CSIRO Australia. Since 1998, he has been in the School of Computing, National University of Singapore (NUS) where he received full professorship in 2016. He is on the editorial board of the ACM Transactions on Software Engineering and Methodology and the Formal of Computing.

**Andrew Martin** is Professor of Systems Security in the Department of Computer Science in the University of Oxford, where he leads the Centre for Doctoral Training in Cyber Security. He has been a faculty member in Oxford for 20 years, leading a research group studying the security of distributed systems and applications of hardware security technologies. His previous work in formal specification and verification earned him his DPhil degree from the University of Oxford, and was further pursued as a post-doctoral fellow at the University of Queensland in Australia.