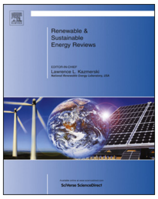
Contents lists available at ScienceDirect

Renewable and Sustainable Energy Reviews

journal homepage: www.elsevier.com/locate/rser



Performance analysis of smart metering for smart grid: An overview

Konark Sharma*, Lalit Mohan Saini

Department of Electrical Engineering, National Institute of Technology, Kurukshetra, Haryana, India

ARTICLE INFO

Article history:
Received 13 November 2014
Received in revised form
16 April 2015
Accepted 27 April 2015
Available online 18 May 2015

Keywords:
Cyber security
Energy measurement
Renewable energy
Smart grid
Smart meter

ABSTRACT

Smart metering systems generally referred to as the next-generation power measurement system, is considered as a revolutionary and evolutionary regime of existing power grids. More importantly, with integration of advanced computing and communication technologies, the smart meter (SM) is expected to greatly enhance efficiency and reliability of future power systems with renewable energy resources, as well as distributed intelligence and demand response. Different electrical energy metering standards are point of concern for power/energy measurements. As measurement standards are formed, systems built around them can become interoperable from a standards point of view but still have incompatible configurations or different maturity levels, or include non-standardized functions. Even in areas that are standardized, there are sometimes implementation decisions that can result in different measurement and security behavior. With this paper we make three contributions: firstly, we identify various 1-channel and 3-channel metrology integrated circuits (ICs), which are mandatory for the standard measurement of distributed and renewable electricity generation. Secondly, we describe harmonics effect on metrology, which impacts on reliability of widespread smart metering infrastructure. Finally, we develop and describe a comprehensive set of security issues for SMs. Specifically, we focus on reviewing and discussing smart metrology meter (SMM) applications (i.e. metrological functions and real-time monitoring functions), security requirements, network vulnerabilities, attack countermeasures, secure communication protocols required in smart grid (SG) architectures. This review will enable the researchers, public policy makers and stakeholders to open the mind to explore possible in an evolving energy domain as well as beyond this area.

Contents

Abbreviations: ADC, Analog to digital converter; ADVISE, Adversary view security evaluation; AES, Advanced encryption standard; AGC, auto gain control; AIM, Artificial intelligent met; AMI, Automatic metering infrastructure; AVISPA, Automated validation of internet security protocols; BAN, Building area network; CPS, Cyber-physical system; DSP, Digital signal processing; DOS, Denial-of-services; DSSS, Direct-sequence-spread-spectrum modulation; ENOB, Equivalent number of bits; FPGA, Field programmable gate array; FTP, File transfer protocol; GPRS, General packet radio service; GSM, Global system for mobile communications; GT, Green technology; HSDC, High speed data capture; HTTP, Hypertext transfer protocol; HV, High voltage; HVQFN, Heat-sink very-thin quad flat-pack no-leads; IC, Integrated circuit; IGBT, Insulated gate bipolar transistor; I^2C, Inter-integrated circuit; IPH, Index of phasor harmonics; IPSEC, Internet protocol security; JTAG, Joint text action group; KB, Kilo bytes; LCD, Liquid crystal display; LED, Light emitting diode; LFCSP, Lead frame chip scale package; LFLO, Logic function logic output; LV, Low voltage; LQFP, Low profile quad flat package; MR, Magneto-resistive; MDMS, Meter data management system; MOA, Massive online analysis; MGS, Modified gradient search; MID, European directive on measuring instruments; MITM, Man-in-the-middle; MOSFET, Metal oxide field effect transistors; MPU, Microprocessor unit; MTTF, mean-time-to-failure; MV, Medium voltage; NAN, Neighbor-hood area network; OMPA, Optimal meter placement algorithm; PLC, Power line communication; PMU, Phase measurement unit; PSTN, Public switched telephone network; PUF, Physically un-clonable function; PV, Photovoltaic; QFN, Quad-flat no-leads; QFP, Quad-flat package; RF, Radio frequency; RFID, Radio frequency identification; RISC, Reduced instruction set computing; RMS, Root mean square; RTC, Real-time clock; SCADA, Supervisory control and data acquisition; SG, Smart grid; SM, Smart meter; SMM, Smart metrology meter; SNR, Signal-to-noise ratio; SOC, System on chip; SOIC, Small outline integrated circuit; SPI, Serial peripheral interface; SSH, Secure shell; SSI, synchronous serial interface; SSL, Secure socket layer; SSOP, Shrink small outline package; SSP, Secure signal processing; SUN, smart utility network; TCP/IP, Transmission control protocol /internet protocol; THD, Total harmonic distortion; THD_F, Total harmonic distortion of fundamental; TLS, Transport layer security; TOD, Time-of-day; TOE, target of evaluation; TOU, Time-of-use; TQFN, Thin quad flat no-lead; TQFP, Thinner quad flat package; TSSOP, Thin-shrink small outline package; TSV, Tunable signing and verification; TTL, Transistor-transistor logic; UART, Universal asynchronous receiver transmitter; USB, Universal serial bus; VFQFPN, Very thin fine pitch quad flat pack no lead package; V2G, Vehicle-to-grid; WAMS, Wide area management system; WAN, Wide area network; WELMEC, European cooperation in legal metrology

* Corresponding author.
E-mail address: konark123@gmail.com (K. Sharma).

http://dx.doi.org/10.1016/j.rser.2015.04.170
1364-0321/© 2015 Elsevier Ltd. All rights reserved.

1. Introduction

The smart meters (SMs) requirements are rapidly evolving in response to competitive market forces and various governmental regulations mandating smart grid (SG) deployments in most areas of the world. Now days it has made the scenario guaranteeing higher bit rates, robust and flexibility. Soon they will roll out utility consumers by the hundreds of millions smart meters by replacing century-old analog electro-mechanical (Ferrari's) energy meters [1]. A snapshot of analog electro-mechanical meter is shown in Fig. 1(a). Ferrari's energy meter were introduced in the late 1880s and operate by counting the revolutions of an aluminum disc which is made to rotate at a speed proportional to the power disc speed may fast or slow, during non linear loads (i.e. fluorescent light, energy storage systems) monitoring results error in readings. They could measure only active energy [2]. During 1990s, advanced electronics solutions such as microprocessor units (MPUs) and fast analog-to-digital converters (ADCs) allowed the manufacturers to start introducing meters that were mostly electronic and the only moving parts were the electro-mechanical counters used to record energy [3,4]. A snapshot of an electronic meter is shown in Fig. 1(b). A third generation power metering circuit could measure not only active power but also various important parameters such as reactive power, apparent power, voltage and current root mean square (RMS) values, power factor and harmonic distortion using configurable digital signal processing (DSP) core [5]. Early 2000s saw further advances in electronics, instrumentation, communication and data handling. They allowed manufacturers to produce meters that were all electronic without rotating parts [6]. These meters could measure following parameters such as.

- Instantaneous parameters: voltage, current, power, power factor, etc.
- Billing parameters: kilowatt-hour (kWh), reactive power (kVArh), maximum demand and load profile etc.

These meters with existing communication technologies such as radio frequency (RF), global system for mobile communications (GSM), general packet radio service (GPRS), public switched telephone network (PSTN) and power line communication (PLC), allowed consumers value-added services[7,8].

As compare to legacy electronic meter, present electronic meter is smart, and can provide a range of intelligent functions such as dynamic pricing, demand response, remotely power connect/disconnect; outage management, network security, and reduction of non-technical losses. It offer higher accuracy and require less power at a considerably lower cost. It is fully envisioned to integrate high-speed two-way communication into millions of power equipments to establish a dynamic and interactive infrastructure with energy management facility capabilities [9]. There are eight basic metrology computation blocks, which are the backbone of latest SM.

- Microcontroller unit (MCU): The integrated MCU core with inbuilt flash memory provides a flexible means of configuration, post-processing, data formatting, and interfacing to any host processor through suitable interface type or any data in/out pins. Records power consumption details can be sent to energy suppliers or prosumers on request.
- Analog-to-digital converter (ADC): It digitizes the voltage and current inputs and provides an instantaneous snapshot of power factor and energy consumption. It can also measure magnitude of phase currents and voltages over the cycle [4]. At present metrology IC with 64 bit ADC are available in market [10].
- Analog-front end (AFE): It is comprised of an input multiplexer, ADC converter and voltage reference It is a link between the real world and the processing world, which collects and calculates single phase and poly-phase voltage, current, power, energy, and power-quality disturbances such as harmonics. This computed results can be retrieved with the help of an external master unit through on-chip host interface [9,11].
- Interface unit: It supports various types of interfaces such as serial peripheral interface (SPI), universal asynchronous receiver transmitter (UART), high speed data capture (HSDC) and Inter-integrated circuit (I^2C), which are useful to connect external devices for special applications. An isolated RS-485 communications interface is also provided with the EM773, for any serial communications needs [12].
- Liquid crystal display (LCD) driver: It helps to display the calculated energy in LCD display for billing purpose. The MSP430F676 consist of integrated LCD driver with contrast control up to 25-MHz system clock for up to 320 Segments in 8 multiplexer modes [13].
- Real-time clock (RTC): The typical metrology IC always inbuilt with RTC for tariff information. This involves dividing the day, month and year into tariff slots (Time of Day). Usually higher rates are applied at peak load periods and lower tariff rates at off-peak load periods. Therefore RTC for metrological application must be very accurate to avoid dispute between consumer and utility applications regarding measurement of fundamental reactive energy even in non-sinusoidal conditions [14].
- Security scheme: It supports highest levels of available security schemes, which helps to protect ones physical tampering events (i.e. mechanical and electrical anti-tampering), consumer data and ensures privacy [15].
- Communication protocol stack (wireless/wire-line): With the help of communication processor, it supports all latest communication technologies (i.e. both RF and PLC solutions), which is useful for gateway concentrators and AMI applications [16].

Considering all necessary requirements SMM solutions can be classified into three categories:

1. Metrology AFE: Fig. 1(c) illustrates block diagram for metrology AFE. AS per latest metrological standards, the metrology IC integrator must be able to translate the class/range specification to the AFE fundamental requirements (i.e. signal-to-noise ratio (SNR), input referred noise voltage or equivalent number of bits (ENOB). At present latest metrology IC have high SNR with ADC built-in auto gain control (AGC) mechanism, which can perform wide range current measurement with accuracy better than class 0.5 [17]. The 71M6515HA with high-speed

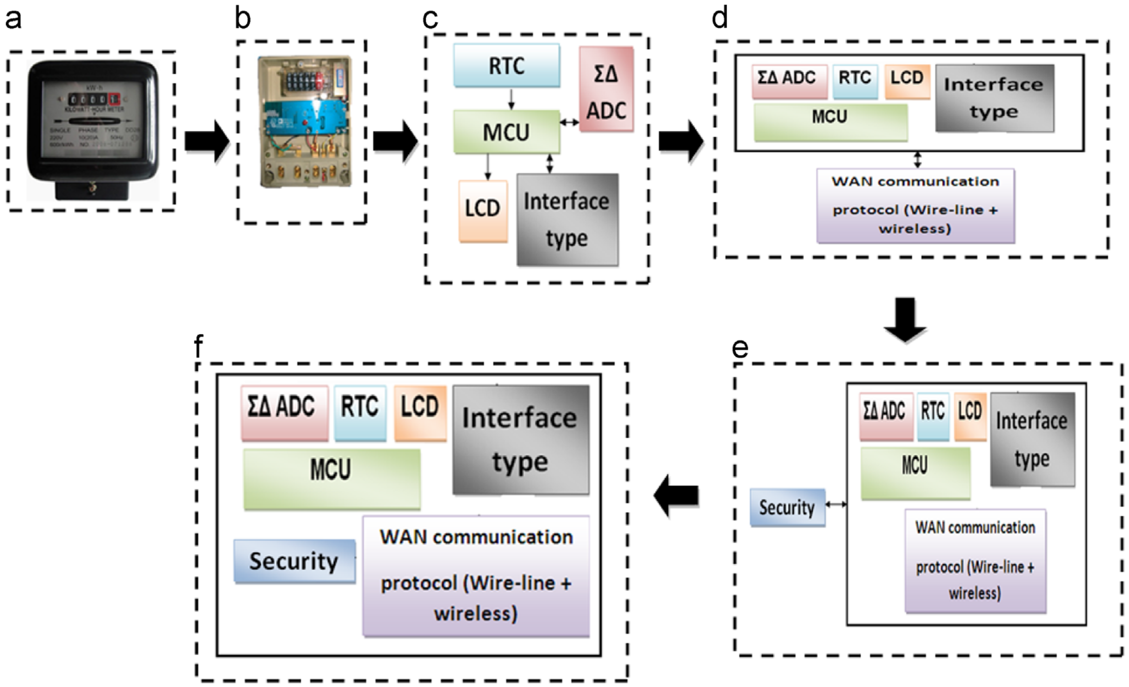

a
b
c
RTC
ΣΔ ADC
MCU
LCD
Interface type
d
ΣΔ ADC
RTC
LCD
Interface type
MCU
WAN communication protocol (Wire-line + wireless)
e
ΣΔ ADC
RTC
LCD
Interface type
MCU
Security
WAN communication protocol (Wire-line + wireless)
f
ΣΔ ADC
RTC
LCD
Interface type
MCU
Security
WAN communication protocol (Wire-line + wireless)

Fig. 1. Historical development of metrology (i.e. analog electro-mechanical meter to smart meter) (a), Analog electro-mechanical meter (b), Electronic meter (c), Metrology AFE (d), Metrology SoC (e) and (f) Metrology SaoC.

synchronous serial interface (SSI) port provides measurements for four-quadrant 3-channel metering [18].

2. Metrology system-on-chip (SoC): It locks an application into a fixed amount of memory and peripherals, which offers highly accurate metrology, multiple layers of security, and processing for advanced communication protocols. Fig. 1(d) illustrates block diagram for metrology SoC.
3. Metrology smart-application-on-chip (SaoC): It consists of a communication interface also. Many USA companies have optioned the ZigBee wireless radio as utility link, while in Europe, a number of manufacturers and utility groups have agreed to use PLC standards. The STCOMET [19] and ASM221 [10], are recently launched programmable and firmware-upgradeable SaoC platform, that integrates a narrow band power line communication (NBPLC) standards such as PRIME, IEC61334-5-1, G3-PLC, METERS AND MORE®, P1901.2, and supports high accuracy metrology applications like EN 50470-1, EN 50470-3, IEC 62053-2x compliant class1/0.5/0.2 measurement with necessary security features in a single chip. The ASM221 can be use for both, 1-channel and 3-channel energy measurement for residential SMs. Fig. 1(e) and (f) illustrates block diagram for metrology SaoC.

However, such a heavy dependence on information networking inevitably surrenders the SM to potential vulnerabilities associated with communications and networking systems. This increases the risk of compromising reliable and secure power system operation. For example, it has been proven that potential network intrusion by adversaries may lead to a variety of severe consequences in SG applications, from consumer information leakage [20] to a cascade of failure of automatic metering infrastructures (AMIs) [21]. As a result, we are motivated to investigate SM security issues, which are of critical importance to the design of information networks and have been considered as one of the highest priorities for the SG infrastructure. Since the research on SM security for SG infrastructure is still in its early stage, our objective is to provide an overview, analyze potential SM security threats, review existing and ongoing SM security solutions, and summarize research challenges regarding SG deployments. Therefore following issues are discussed in the paper:

- Objective and requirement: We first describe the objectives and requirements of SM for SG, with a special focus on identifying fundamental differences between analog electromechanical meter and SM.
- Metrological characterization: We present past, present and ongoing research in the field of 1-channel and 3-channel metrological ICs by considering their standards, power measurement parameters (i.e. watt-hour accuracy (Wh) accuracy, dynamic range, Supply voltage, host interface, harmonics realization facility, ADC, package type) and security features,
- Smart meter security and privacy issues: We analyze SM security and privacy preserving schemes considering from individual SM location to SG infrastructure applications (around the globe), covering different communication technologies in real-time/simulation manner.
- Smart meter attack prevention and defense: To efficiently counteract SM attacks, it is essential to widely deploy attack prevention and defense strategies covering individual SM location to SG infrastructure. Therefore, we tabulate existing and ongoing solutions, including their coverage area, and mode of operation, by considering their SG applications.

Rest of the paper is organized in the following way: Section 2 we introduce various 1- channel and 3-channel metrology ICs specifications covering various features like standards, host interface, supply voltage, harmonic realization facility, security feature and package size description, are important for secure and robust SM design.; Section 3 discusses effect of harmonic factor on performance on SMs and their measurement and minimization schemes; Section 4 we present the objectives and requirements of security outlines attacks on SMs covering physical, cyber-physical system Section 5 illustrates various privacy-preservation/security schemes, covering individual user and clusters of users across the globe; and finally, we conclude Section 6 summarizing the status of smart metering infrastructure and draws outlines for future SG applications.

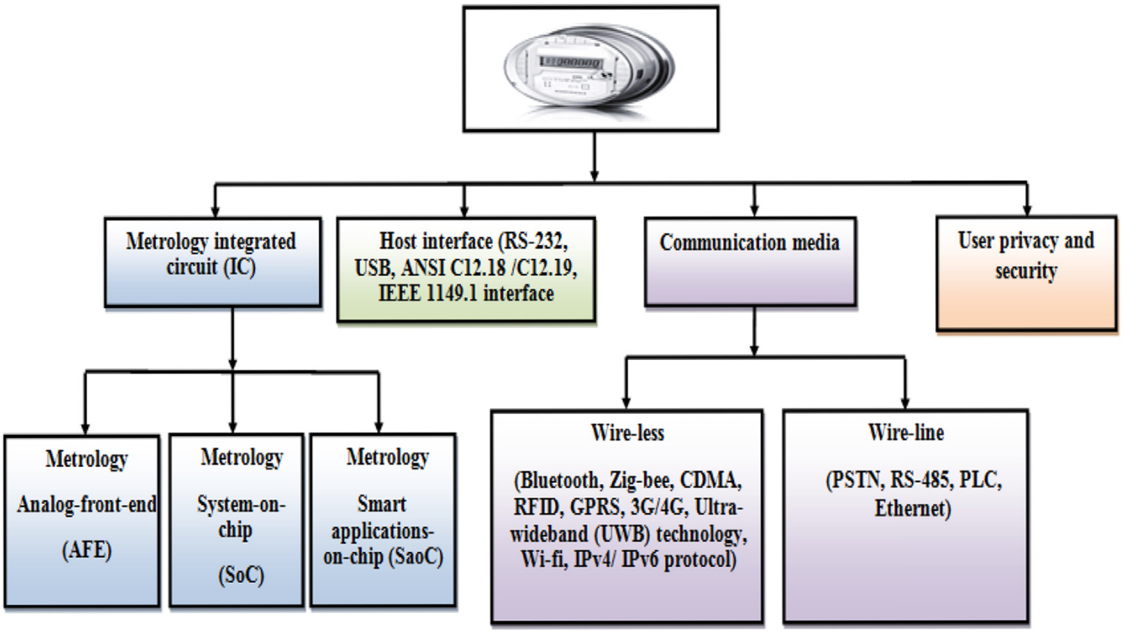

Metrology integrated circuit (IC)
Host interface (RS-232, USB, ANSI C12.18 /C12.19, IEEE 1149.1 interface
Communication media
User privacy and security
Metrology Analog-front-end (AFE)
Metrology System-on-chip (SoC)
Metrology Smart applications-on-chip (SaoC)
Wire-less (Bluetooth, Zig-bee, CDMA, RFID, GPRS, 3G/4G, Ultra-wideband (UWB) technology, Wi-fi, IPv4/ IPv6 protocol)
Wire-line (PSTN, RS-485, PLC, Ethernet)

Fig. 2. Building blocks of smart meter.

2. Smart metrology

SMs are accelerating world market with proven elements such as accurate energy measurement, robust communications features, and integrated security. Fig. 2 shows the SM building blocks and the detail of each block are as follows.

- Metrology integrated circuit (IC): It provides highly accurate, cost-effective solutions for advanced power measurements. It may be equipped with any suitable metrological solutions such as metrology AFE, metrology SoC, metrology SaoC.
- Host interface: There is provision with SM to have an optical port compliant with the ANSI C12.18/ANSI C12.19 specifications. It has been known for a practical approach in meter reading and programming [22]. The MSP430 has a IEEE 1149.1, joint text action group (JTAG) interface that allows for programming [9].
- Communication media: For SMs, there is a varied choice of communication modes available such as ZigBee protocols [23], RF mesh [24] and radio frequency identification (RFID**)** [25]**,** which forms a multi-point to multi-point network without single failure covers home area networks (HANs) and building area networks (BANs) applications. While PLC [6], 4G [26], GSM/GPRS [27] and ultra-wideband (UWB) technologies [28], are promising solution to cover vehicle-to-grid (V2G) and renewable energy applications [29].
- User privacy and security: As SM data travels through several networks, secure point-to-point communication based on strong authentication mechanisms and a robust and scalable key management schemes are crucial for assuring the confidentiality and the integrity of this data. For this SMM solutions with latest security features in order to ensure consumer privacy [30].

SMs with latest metrological solutions with existing communication solutions can monitor identity/location based power consumption of individual or complete household appliances. The following table shows various energy management schemes using SMs (Table 1).

Electrical energy meters specifications as per their class and range are defined by several standardization groups, especially by the International Electrotechnical Commission (IEC), American National Standards Institute (ANSI), European Directive on Measuring instruments (MID) and the European cooperation in legal metrology (WELMEC) standards. They standardize, regulate accuracies and reliability towards active and reactive energy measurement at all levels in the power system hierarchy. The existing metrological standards are already able to describe many functions that are necessary for SG deployments. But there are still some difficulties to simultaneously support weekday/weekend tariffication facility, real-time data control functionalities in active low voltage (LV) and medium voltage (MV) networks, aggregated energy services, power quality assessment, control of production and storage, data security and consumer privacy between standards. For this a much wider range of metrology ICs offering more fabless semiconductor companies to enter the power/energy measurement field. Present metrology ICs are highly integrated, cost effective, secure by design, tamper resistant and work on very low power platform for house-hold, commercial and industrial SG applications. They not only provide power measurement information facility, but also satisfying consumer favorable purposes:

- Flexible billing and weekday/weekend tariffication facility;
- Real-time data support and network communication/control functionalities for supervisory control and data acquisition (SCADA systems) and phase measurement units (PMUs);
- Support demand response and power quality assessment services of consumers;
- Support data security and maintains consumer privacy, etc.

With the increasing deployment of grid-based distributed renewable energy resources in the distribution network [31], and with rapid evolution of photovoltaic (PV) energy through net metering [32], and energy services markets including local neighborhood and smart islands [33] toward dynamic spot markets. Latest SM solutions with near-real-time support are providing consistent functionalities and remarkable energy management opportunities, from simple energy efficient appliance such as light emitting diode (LED) lamp to renewable energy micro grid and enhanced for the new markets evolution [34].

Metrology ICs with watt-hour accuracy classes between 0.1–0.5 with dynamic ranges up to 5000 is available in market [30], which enables accurate, dependable and robust SM. The ADE7953 includes security measures (i.e. unwanted data write protection, communication verification, and checksum facility), which increase communication

Table 1
Energy management services using smart meter.

Technique/scheme	Mode of communication		Advantages	Coverage area	Mode of operation		Country	Key reference
	Wire-less	Wire-line			Hardware	Software		
Power consumption consulting system (PCCS)	–	✓ LAN	Collects AMR data, weather data, load management and consulting	HAN ⇔ WAN	✓	✓	South Korea	[8]
Wireless multimedia sensor networks (WMSNs)	✓ Cognitive radio	–	Supports large-size and time sensitive multimedia messages	HAN ⇔ WAN	–	✓	USA	[66]
Smart multi-power trap (SMPT) smart meter	✓ Zigbee	✓ PLC	Provides identity and location of appliances on basis of temporal power consumption data	HAN	✓	–	South Korea	[108]
SystemC simulator	–	–	Predicts the power dissipation from individual appliance to complete household appliances	HAN	–	✓ SystemC	South Korea	[110]
Intelligent energy management system (IEMS)	✓ Zigbee	–	Controls the power consumption of various appliances individually	HAN ⇔ BAN	✓	–	South Korea	[118]
Embedded secure access module (ESAM)	✓ RF transceiver	–	Secure e-wallet facility for prepayment mode	HAN ⇔ BAN	✓	–	China	[121]
Message authentication code (MAC)	–	✓ LAN	Load monitoring with data aggregator via CAN bus	HAN ⇔ WAN	✓	✓	Italy	[127]
High performance computing (HPC) algorithm	–	–	Customer energy consumption without compromising data quality	HAN ⇔ WAN	–	✓ LibASVM	USA	[129]
Analysis of variance (ANOVA) scheme	–	✓	Detects individual meter data anomaly	HAN ⇔ WAN	–	✓ IEEE-13 bus system	Taiwan	[132]
(i) Meanvar protocol (ii) Compare protocol (iii) Compare3way protocol	–	–	Less computation keys and theft prevention	HAN ⇔ BAN	–	–	United Kingdom	[134]
Energy consumption scheduler (ECS)	✓	✓	Checks and balance residential load curves upto 33%	HAN	–	✓ Matlab/ Simulink	Pakistan	[148]
Event window based load monitoring technique	✓ Zigbee	–	Process based signature and event window technique monitors complicated loads	HAN	✓	✓	Canada	[149]
Explicit-duration-hidden markov-model with differential observations (EDHMM-diff) model	–	–	Modeling of individual load appliances on bases of aggregated power signal with state durations	HAN	–	✓	Canada	[151]
Distributed subgradient algorithm (DSA)	–	–	Models individuals power consumption schedule during absences of AMI messages	HAN ⇔ WAN	–	✓	USA	[160]
Privacy-preserving energy management (PPEM) technique	–	–	A systematic framework between smart meter data privacy and electricity cost	HAN	✓	✓	USA	[164]
Secure multi-party computation (SMC) protocol	–	–	Paillier cryptosytem used	HAN	–	✓	USA	[167]

robustness and avoid inadvertent data modifications [35]. The 78M6613 is industry's first SoC solution for AC/DC power supplies measurement. It deliver accurate, four-quadrant electricity measurement with custom firmware, which provide valuable data measurement for monitoring/measuring efficient solar-panel inversion and industrial motor health monitoring applications [36,37]. The following table show various 1-channel metrology ICs (Table 2).

The EM773 contains, 32-bit MCU, which offers high performance at very low power consumption [12]. As per WELMEC and MID directives, metrology IC with 32 bit reduced instruction set computing (RISC) MCU, 128 – 256 Kilo bytes (KB) flash memory allows metrological and monitoring applications with minimal effort [15,30]. The following table show various 3-channel metrology ICs (Table 3), which are in practice for domestic/industrial SMs design.

3. Effect of harmonics on metrology

The SMM market is facing many challenges (i.e. government regulations, updating energy policies, technology innovations and end consumer expectations) in today's rapidly evolving world. With greater awareness of the increasing gap between consumed real power (watts) and generated apparent power (VA). Furthermore, metrology needs more sophistication with increased semiconductor development in the field of highly non-resistive and non-linear loads (i.e. rectifiers, inverters, industrial power electronics and electric transport) in power distribution networks [38]. Voltage and current harmonics for total harmonic distortion (THD) are very common with multiple distributed energy resources (DER) such as solar and wind energy systems and their harmonic measurement up-to 15th harmonic order is recommended [39]. This can lead to more significant load current distortions. THD are based upon the harmonic magnitude only. Index of phasor harmonics (IPH) is an important parameter, which is useful for harmonic measurement with storages, electric vehicles and DER systems in power distribution networks. It considers magnitude and angle of waveforms [40]. In LV networks, such as residential PV systems [41] and various types of loads generate high harmonics, which influences commercial and industrial metering characteristics [42]. High harmonics overheat power transformers, trips circuit breakers, reactive power compensators and neutral conductors [43]. Therefore it is necessary for power industry to measure and analyze harmonic energy accurately in order to provide harmonic energy measurement products with high accuracy, multi-rate and multi-function for present SG deployments. For this presently metrology ICs with harmonic analysis functions can characterize the state of the load or supply. Harmonic measurement from solid-state MPUs and ADCs [3] to field-programmable-gate-array (FPGA) [44], it has been reported.

Table 2
1-Channel metrology ICs specifications.

Part number	Standard specification	Watt-hour (Wh) accuracy (%)	Dynamic range	Voltage (V_{supply})	Host interface	Harmonics realization facility	Security feature	$\Delta\sum$ ADC (bit)	Package type	Key references
ADE7755	IEC60687, IEC61036	< 0.1	500:1	2.5	LFLO	✓	–	16	24-SSOP	[6]
ADE7753	IEC 60687, IEC61036, IEC61268, IEC62053-2x	< 0.1	1000:1	2.4	SPI	✓	–	16	20-SSOP	[7]
MSP430FE4A	-	< 0.1	2400:1	2.7–3.6	USART, SPI	–	–	16	64-QFP	[9]
ASM221	IEC62053-21, IEC62053-22, IEC62053-23, ANSI C12.1,ANSI C12.20	< 0.1	10000:1	1.8–3.6	SPI, I^{2}C, UART	✓	✓	64	128-LQFP	[10]
MSP430F676	ANSIC12.20, IEC62053	< 0.1	5000:1	1.8–3.6	UART, SPI, I^{2}C	✓	✓	24	80-LQFP, 100-LQFP	[13]
PS2100	IEC62053-22, ANSI C12.20	< 0.1	2000:1	3	UART, SPI, I^{2}C	✓	✓	10	128-LQFP	[17]
ADE7751	IEC60687, IEC61036	< 0.1	500:1	2.5	LFLO	✓	–	16	24-DIP, 24-SSOP	[27]
ADE7757	IEC61036, IEC521	< 0.1	500:1	2.5	LFLO	✓	–	16	16-SOIC	[29]
MAX71617	MID/WELMEC	< 0.1	5000:1	2.7–3.6	I^{2}C, UART, SPI, ISO UART	✓	✓	32	120-LQFP	[30]
ADE7953	EN50470-x, IEC62053-2x	(a) < 0.1 (b) < 0.2	(a) 3000:1 (b) 1000:1	3.3	UART, SPI, I^{2}C	✓	✓	16	28-LFCSP	[35]
78M6613	IEC 62053, ANSI C12.20	< 0.5	2000:1	3.3	UART	✓	✓	22	32-QFN	[36]
CS5464	IEC/ANSI/JIS	< 0.1	1000:1	2.5	SPI	✓		16	28-SSOP	[115]
PL3201	IEC60687, IEC61036, IEC61268, IEC62053-2x	< 0.1	1000:1	5	UART	✓	–	16	100-LQFP	[116]
MCP3905A	IEC62053, IEC 61036, IEC60687	< 0.1	500:1	2.4	LFLO	✓	–	16	24-SSOP	[122]
ADE7761	IEC60687, IEC61036	< 0.1	500:1	2.5	LFLO	✓	–	24	20-SSOP	[123]
STPM32	EN 50470-x, IEC62053-2x, ANSI C12.2x	< 0.1	5000:1	3.3	UART, SPI	✓	–	24	32-QFN	[158]
ATM90E26	IEC62052-11, IEC62053-21, IEC62053-23	< 0.1	5000:1	2.8–3.6	SPI, UART	✓	–	32	28-SSOP	[159]

- Harmonic content of load waveform affects power measurement significantly [3]. Therefore reactive power measurement is essential during harmonics [45].
- Total harmonic distortion of fundamental (THD_F) parameter is a much better option for harmonic content measurement [46].
- IEEE 519-1992 standard based metrological solution not only reduces the measurement differences but also recover harmonic losses for power supply companies [47].
- Separate measurement of fundamental harmonics (H_F) and high harmonics for distribution network, can eliminate supply network harmonics [48].
- Although hall sensors, can measure harmonic levels up-to 25th harmonic order [49]. But magneto-resistive (MR) sensors [50] as compared to hall sensors and current transformers (CTs) [51], are good option for harmonic power measurement.
- As per IEC6100-4-7 standard, modified gradient search (MGS) technique can estimate harmonics/inter-harmonics of power system voltage and currents up-to 40th harmonic order [52].
- Optimal meter placement algorithm (OMPA) can locate harmonic from a single source to 50th harmonic order [53].
- Second harmonic filtering technique limits the harmonic effects of non-linear loads [54].
- Newton-type algorithm and recursive differentiation filter (NTA-DF) technique under different conditions (i.e. dc offset, harmonics, frequency drifts, amplitudes, notches and spikes) can estimate fundamental frequency, which is useful for SMs [55].
- Although IEEE 1459-2000 standard does not describe reactive power definition under non-sinusoidal conditions, and meters can measure active power and non-active power during harmonics [56]. But standard IEEE 1459-2010, quantifies 1-channel and 3-channel different conditions (i.e. under sinusoidal, non-sinusoidal, balanced and un-balanced load) [57].

Government regulations and standards in smart metering infrastructure, along with the AMI network, have dramatically increased the need for products that offer precise harmonic measurements 3-channel metrological applications, while simplifying security designs and reducing costs. Earlier successive measurement scheme based metrological AFEs could measure each harmonic element and THD_F [11]. At present different metrological solutions such as the PL3223 [58] and the ATT7022B [59], can accurately measure total harmonic component analysis of each phase active power, reactive power, voltage, and currents up-to 21st harmonic order and the ATM90E36A can measure up-to 32nd harmonic order [60].

4. Smart meter security issues and privacy-preserving schemes

Today's SMs are endpoints in large/medium scale, machine-to-machine (M2M) networks that extend to both SG infrastructure and to the vast array of future machines and devices that connect to SG applications. With existing two-way communication techniques SMs provide time-related consumption information which is used in time-of-use (TOU) or time-of-day (TOD) pricing between the utilities and consumers. They can measure power at a fine-grained level from seconds to 15 minutes interval. This measured data is transmitted intermittently via different communication technologies and sent to local distribution system operators (DSOs) [61]. In addition to protecting business and consumer data/details on an electricity grid, SMs and their associated infrastructure monitor such as AMI network, control, and even protect the critical power infrastructure. AMI network is an important infrastructure which has much functionality and SM is an entity which can be implemented at each and every home/industrial energy conservation applications. There is an important

Table 3
3-Channel metrology ICs specifications.

Part number	Standard specification	Watt-hour (Wh) accuracy %	Dynamic range	Supply voltage (V_{supply})	Hostinterface	Harmonics realization facility	Security feature	$\Delta\sum$ ADC (bit)	Package type	Key reference
ASM221	IEC62053-21, IEC62053-22, IEC62053-23, ANSI C12.1,ANSI C12.20	<0.5	2000:1	1.8–3.6	SPI, I^{2}C, UART	✓	✓	64	128-LQFP	[10]
MAXQ3180	IEC60687, IEC61036, IEC61268	–	–	3.3	SPI	✓	–	16	28-TSSOP	[11]
EM773	IEC 60134	–	–	1.8–3.6	SPI	✓	✓	32	33-HVQFN	[12]
MAX71637	MID, WELMEC	<0.1	5000:1	2.7–3.6	I^{2}C, UART, SPI, ISO UART	✓	✓	32	120-LQFP	[15]
71M6515H	IEC62053, ANSI C12.20	<0.1	2000:1	3.3	UART	✓	–	20	64-LQFP	[18]
ADE7754	IEC60687, IEC61036	<0.1	1000:1	2.4	SPI	✓	–	16	24-SOIC	[23]
78M6631	IEC62053, ANSI C12.20	<0.5	2000:1	3.3	UART, I^{2}C,SPI	✓	✓	22	56-TQFN	[25]
(i) MAX71334L (ii) MAX71335L	MID, WELMEC	<0.1	2000:1	3–3.6	SPI, Master I^{2}C, UART	✓	✓	32	100-LQFP	[30]
PL3223	IEC60687, IEC61036, IEC61268, IEC62053-2x	<0.1	1000:1	5	SPI	✓	✓	16	44-QFP	[58]
ATT7022B	IEC62053-22, GB/T 17883-1998	<0.1	1000:1	2.4	SPI	✓	–	16	44-QFP	[59]
ATM90E36A	IEC62052-11, IEC62053-22, IEC62053-23, ANSI C12.1,ANSI C12.20	<0.1	6000:1	2.8–3.6	SPI	✓	–	32	48-TQFP	[60]
ADE7758	IEC60687	<0.1	1000:1	2.4	SPI	✓	–	16	24-SOIC	[109]
71M6513	IEC62053, ANSIC12.20	<0.1	2000:1	3.3	UART, I^{2}C	✓	–	20	100-LQFP	[112]
MCP 3909	IEC62053, IEC1036, IEC61036, IEC60687	<0.1	1000:1	2.4	SPI	✓	–	16	24- SSOP	[114]
ADE7878	IEC62053-2x	<0.1	1000:1	2.4	I^{2}C, SPI, HSDC	✓	–	16	40-LFCSP	[119]
SA9904B	IEC61036, IEC61268	<0.1	1000:1	2.4	SPI	–	–	24	20-DIP	[120]
MSP430F6779	ANSI C12.2x, IEC62053	<0.1	2000:1	1.8–3.6	UART, SPI, I^{2}C	✓	✓	24	100-LQFP, 128-LQFP	[156]
ADE7880	IEC62053-2x, EN50470-x	(a) <0.1 (b) <0.2 (c) <0.1	(a) 1000:1 (b) 5000:1 (c) 1000:1	2.4–3.7	HSDC, SPI, I^{2}C	✓	–	24	40-LFCSP	[157]
ADE7752	IEC62053-2x	<0.1	500:1	2.4	LFLO	✓	–	16	24-SOIC	[165]
MSP430F6779	IEC 62053, ANSI C12.20	<0.1	2000:1	1.8–3.6	SPI, I^{2}C, UART	✓	✓	24	100-LQFP, 128-LQFP	[166]

relation between AMI and SG in terms of communicational needs and network topologies due to their functionality, measuring components, coverage area and architecture. SM communication technologies depends upon local environmental conditions, business model and communication interface [24]. Considering existing communication standards of SMs and their coverage from HAN to wide area network (WAN) application/layer, It is found that each application/layer is important in determining suitable technology for SG deployment. From communicational and security prospective an AMI can be considered to include the following components as shown in Fig. 3.

- Home area network (HAN) and building area network (BAN): It comprises a computerized, intelligent network of electronics instruments (i.e. sensors and actuators), designed to reduce energy consumption. SMs pose multiple sensors and data sources, which can indicate energy theft, in practice, the individual methods exhibit many false positives [62,63]. SMs sensors usually have resource constraint; therefore it is desirable to have lightweight security mechanism [64,65]. Performance of multiuser selection scheme for HANs/BANs for SMM applications depends upon total number of devices, traffic intensity and modulation schemes [66,67].
- Smart meter gateway (SMGW): It is the central communication component of SG infrastructure, which connects a WAN with a network of devices of one or more SMs. They maintain communication between the prosumer with his consuming and generating devices, and are secure from physical attacks [68]. SMGW contains security module, which is responsible for basic authentication and aggregation of messages sent by various meters on their way to control center [69,70]. In Europe, the German organization released the protection profile (PP) for secure gateways in smart metering systems [71]. PP defines about the target of evaluation (TOE), an electronic unit with following functionalities.
  (i) Data integrity, authenticity, protection of confidentiality
  (ii) Information flow control

  So there is need of secure mechanism between data concentrators and SMs to protect end-to-end information. For this high data security mechanism for secure crypto algorithms/operating systems are required to AMI networks (i.e. individual meter to gateway meters, and sub-metering devices). The following table shows various SMGW security schemes (Table 4).
- Neighborhood area network (NAN): It may be the combination of number of HANs/BANs, where all types of necessary information like, power consumption data, appliances control, and security alarms are transmitted to accomplish energy management [72–74].
- Wide area network (WAN): It is a computer network which connects an AMI headend in the local utility network and a data concentrator. Data concentrator collects over a network from group of SMs and sends this bulk data to headend. AMI headend manages the information exchanges between external systems, such as meter data management system (MDMS) and AMI network. As with all high speed communication networks, such as Wimax, 3G/GPRS and broadband power line

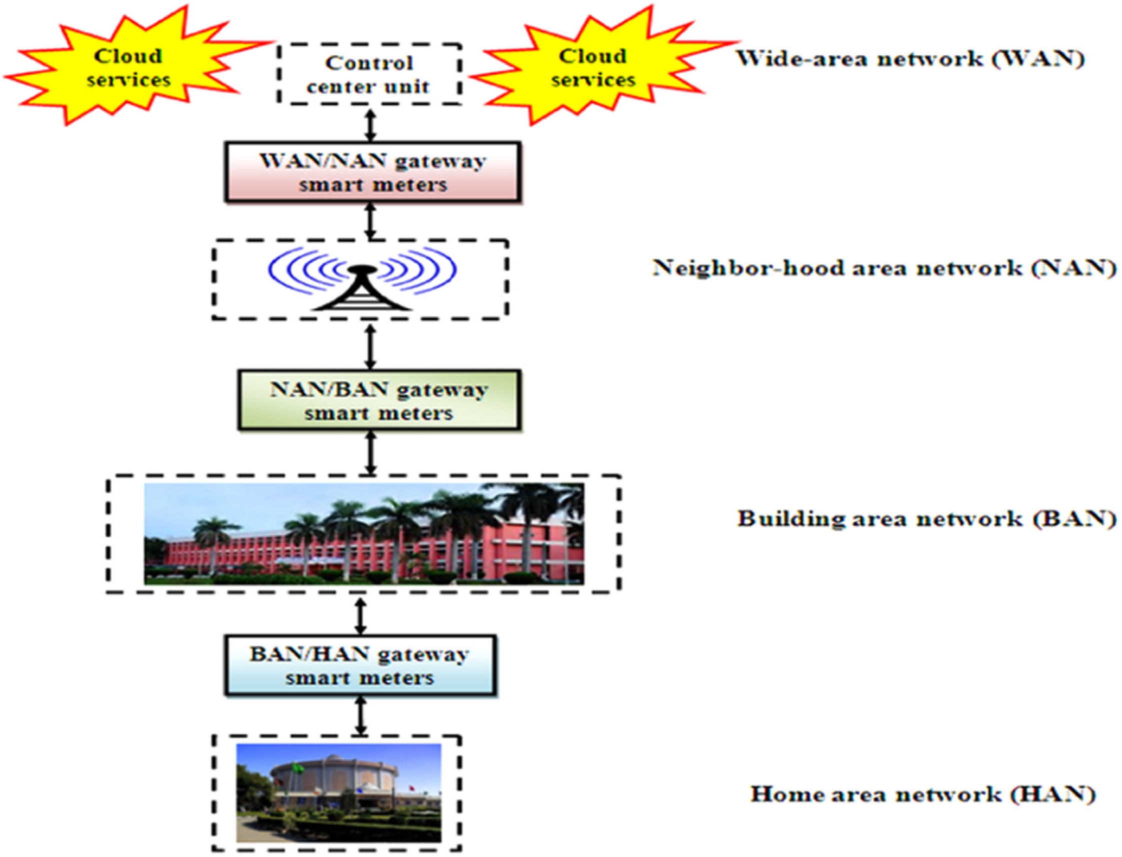

Cloud services
Control center unit
Cloud services
Wide-area network (WAN)
WAN/NAN gateway smart meters
Neighbor-hood area network (NAN)
NAN/BAN gateway smart meters
Building area network (BAN)
BAN/HAN gateway smart meters
Home area network (HAN)

Fig. 3. Hierarchical architecture of advanced metering infrastructure (AMI).

Table 4
Smart meter gateway (SMGW) security schemes.

Technique/scheme	Mode of communication		Advantages	Coverage area	Mode of operation		Country	Keyreference
	Wire-less	Wire-line			Hardware	Software		
Two-layer security scheme	✓	✓	Conducts secure key management between data concentrators and meters	HAN ⇔ WAN	✓	✓	Taiwan	[21]
Datagram transport layer security (DTLS) protocol	✓	–	Protects end-to-end information exchange via lightweight protocol	HAN ⇔ WAN	–	✓	India	[65]
Threat modeling	✓	✓	Supports methodological development for system design and software development	HAN ⇔ WAN	–	✓ STRIDE	Germany	[68]
Authentication and fragmentation layer (AFL) protocol	✓ M-Bus protocol (EN13757-4)	–	Fragmentation of long messages in several fragments	HAN ⇔ WAN	✓	✓	Germany	[69]
Privacy-preserving recording and gateway-assisted authentication	✓	✓	Allow gateway smart meters to help aggregate power usage information	HAN ⇔ WAN	–	✓	Hongkong	[70]
Adaptive binary-tree based inspection algorithm	✓	✓	Individual meter to gateway meter data scanning and inspection	HAN ⇔ NAN	–	✓	USA	[125]
Secure communication protocol (SCP)	✓	✓	Shamir secret sharing (SSS) encryption scheme based on chord protocol	HAN ⇔ WAN	–	✓	Italy	[131]
Java card applet	✓	✓	Provides secure and efficient operating systems (OS) for data storage and cryptosystems	HAN ⇔ WAN	✓	–	India	[136]
(i) Terminal smart meter (TSM) (ii) Gateway smart meter (GSM)	–	✓ PLC	Overall illegal electricity measurement	HAN ⇔ WAN	✓	✓ Matlab/ Simulink	South Korea	[137]
(i) ETE-H protocol (ii) HBH-A protocol (iii) HBH-C protocol	✓	✓	Homomorphic multiplication technique used	HAN ⇔ WAN	–	✓	USA	[154]

communication (BPL) connectivity enables functions and applications that consume a high bandwidth; connectivity makes access to the system functionality easier. This drive toward using internet protocol (IP) will achieve interoperability will create robust SG networks, and SMs will operate at low cost [21,61].

With SMs and growing grid distribution communication, AMI network is becoming more pervasive. Therefore AMI security ranging over a spectrum from resisting attacks aimed at supervisory and control systems; to end user privacy concerns [75,76]. This multi-faceted problem also includes vulnerabilities that arise from deployment of physical attack at SM location, with a potential to manipulate the measured energy consumption, and being massively deployed aiming at de-stabilization [20]. It is no surprise that basic encryption algorithms and passwords protection schemes for SMs can no longer ensure the highest level of AMI networks protection. The command and control nature of AMI data networks poses a difficulty from SM security prospective. Therefore SMs require a complete life-cycle security from cradle to grave and should fulfill four necessary security requirements are shown in Fig. 4, and can be described below:

1. Device authenticity: SM accessing features (i.e. manufacturing tests, software debugging) should only be allowed with an authorized mechanism. Inauthentic SM requesting the service of wire-less/wire-line network should not be allowed [77].
2. Data confidentiality: It is concerned with creating, transferring, processing, and storing consumer data, either dynamically produced data, such as meter readings and power consumption profiles. Now a day's consumer data (i.e. metrology and consumption information) is a highly important asset for utility providers. At AMI headend, the exploitation of consumer profiles has to be confidential from eavesdroppers, and only authorized systems will have right to access the specific consumer data [78].
3. Data authenticity and integrity: During AMI applications, it is necessary to ensure that the consumer data and transactions are genuine. It is also important for authenticity to validate that both parties involved are who they claim to be. Some information security systems incorporate authentication features such as HASH function [79], which provide evidence that the message data is genuine and was sent by authorized person with proper signing key.
4. Consumer privacy and security: Consumer privacy protection is a key requirement of today's SG infrastructure. For this SM should have latest storage components with high security mechanism. It should not be accessed by unauthorized requesters. Only authorized requesters must be able to decrypt the encrypted meter data.

Considering all necessary parameters requirements, it has been observed that SMs security should be flexible enough to handle any security threats that evolve over the years. Following table shows various SM privacy-preservation schemes that are used for SG applications (Table 5).

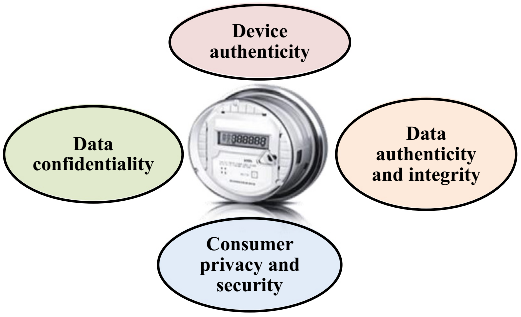

Device authenticity
Data confidentiality
Data authenticity and integrity
Consumer privacy and security

Fig. 4. Smart meter objectives.

5. Smart meter attacks types and their minimization schemes

Traditionally analog electro-mechanical meters and electronic meters were easy for attackers, to steal power and manipulate power consumption details. Electricity theft produces non-technical losses. But SMs based AMIs can detect and minimize electricity theft [80], therefore SM security gets a lot of attention from various governments, utilities, and consumers. SM attacks can be classified in two major categories. Different types of SM attacks are shown in Fig. 5.

1. Physical attacks; 2. Cyber-physical system (CPS) attacks.

1. Physical attacks: SMs are at higher risk of a physical security breach, where illegal user/attacker tries to modify SM records individually or through its interfaces in different ways [81],
   - Replacement of dedicated metrology IC with fake IC: An attacker programs the fake or an intercepted metrology IC to share memory contents with any other attacker as shown in Fig. 6. Secret keys loading during the manufacturing cycle can be easy to manipulate all necessary calculations and consumer details since the fake or an intercepted IC can be program to share such data. To avoid this type of attack there is a need of a high level of engagement between end-users, with the help of advanced encryption standard (AES) based encryption techniques. Physical attack using a smart resistance implementation [82] and zero line CTs [83] can be avoid
   - Steal software to clone a meter: An attacker can rebuild the software that was to be loaded on a smart meter, they could structure the software to share—instead of protect—secret encryption keys. For this latest reliability prediction software are required to design and develop SM characteristics to accurately calculate the reliability indicators such as failure rate, mean-time-to-failure (MTTF) and reliability [85,86].
   - Abusing host interface: Power consumption details generally transmitted to remote places through electrically connected medium like RS 232/RS485 serial communication or through ANSI C12.18/ANSI C12.19 optically isolated medium. Therefore host interface abusing is one of the known hackers' ways to execute unauthorized program code, getting control over secure applications and running code in privileged modes [88]. For this strong authentication protocol, such as secure hashing algorithm (SHA-1) can avoid such type of attacks [89]. Physically unclonable function (PUF) technology with ANSI standard compliant can provide strong hardware based authentication and efficient key management to assure the confidentiality/integrity of messages exchanged between SMs and utilities [84].
2. Cyber-physical system (CPS) attacks: AMI is suitable example of CPS [90], which consists of different types of hardware, communication devices and MDMS, to summarize the collected data into software application platform [85,91]. As SMs networked, MDMS software must have adequate security against any unauthorized change in software configurations, reading of recorded data, change of calibration data, etc [86]. AMI security depends upon authentication mechanism [92], communication technologies [89,93] and routing protocols [74,94]. For efficient and reliable AMI netwoks there is need of systematic framework, which can offer high accuracy between data concentrators and AMI head-ends. Paillier cryptosystems is a homomorphic encryption scheme which secure and efficient way for smart metering systems. The following table encompasses various types of intrusion detection systems (IDSs), performance improvement and privacy preservation schemes that are used in AMIs (Table 6).

Table 5
Privacy-aware smart metering schemes

Technique/scheme	Mode of communication		Advantages	Coverage area	Mode of operation		Country	Key references
	Wireless	Wire-line			Hardware	Software		
Privacy preserving protocol (PPP) scheme	✓	✓	Provides high degree of privacy but does not cover usage consumption profile	HAN ⇔ WAN	–	✓	USA	[20]
Compressed sensing technique	✓ CSMA	–	Pseudo-random spreading codes used	WAN	–	✓	USA	[61]
Privacy-aware yet accountable secure scheme (PASS)	✓	–	Requires less computations and does not affect billing procedure	HAN ⇔ WAN	–	✓	China	[64]
Ring signature scheme	✓	–	Does not affect the performance of wireless sensor network	HAN ⇔ BAN	–	✓	India	[67]
Elderberry protocol	–	✓ PLC	Saves network bandwidth and does not require complex cryptography	HAN ⇔ WAN	–	✓	Germany	[126]
Privacy preserving nodes (PPN) scheme	✓	✓	Shamir secret sharing (SSS) encryption scheme used	HAN ⇔ WAN	–	✓	Italy	[128]
Privacy-preserving-range-query (PARQ)	✓	✓	Stores meter data on cloud servers in encrypted form	HAN ⇔ WAN	–	✓	China	[130]
Unified security and privacy protection (USAPP) scheme	✓	✓	Useful for system control, secure computing and communication security	HAN ⇔ WAN	✓	✓	United Kingdom	[153]
Efficient privacy-preservation protocol for smart metering systems (EPPP4SMS)	✓	✓	Paillier cryptosystem used	HAN ⇔ WAN	–	✓	Germany	[155]
Trustworthy cloud computing (TCC) scheme	✓	✓	Executes infrastructure-as-a-service (IAAS) users to support guest virtual machines	HAN ⇔ WAN	–	✓	India	[161]
Secure multi-party computation (SMC) protocol	–	✓ PLC	100 smart meters data aggregation at once with 100 kbps speed	HAN ⇔ WAN	✓	–	Austria	[168]

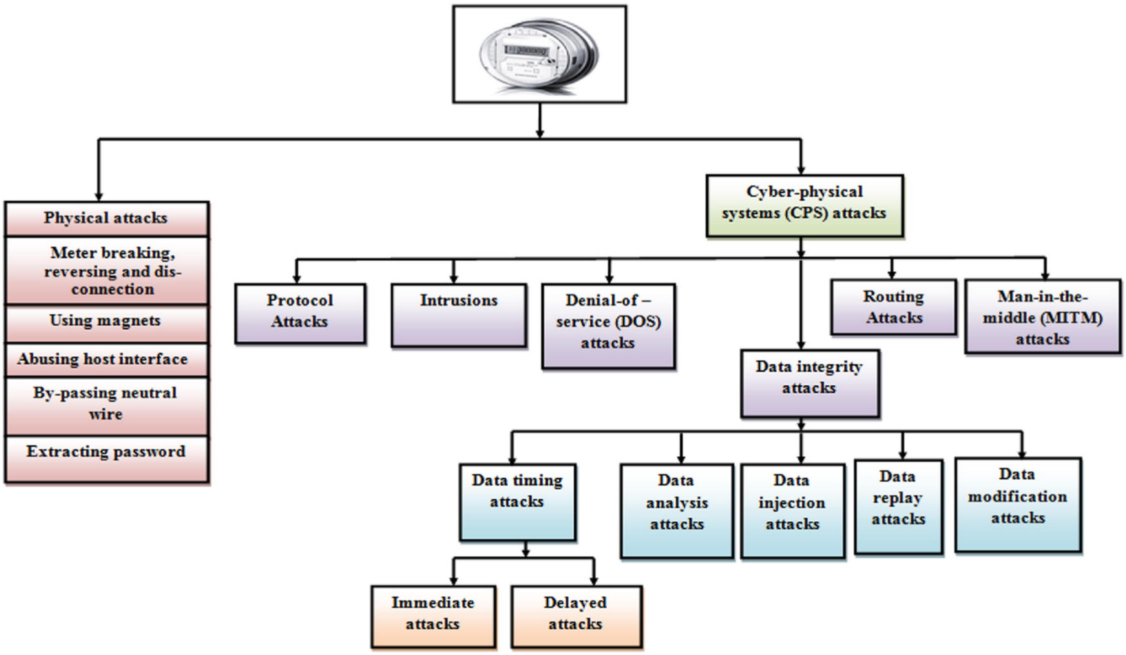


Fig. 5. Different types of attacks on smart meter.

CPS attacks can be sub classified in three categories:

- Denial-of-services (DOS) attacks: It may be an adversary forges the demand request of a smart meter, and keeps requesting a large amount of energy [78]. These attacks are related with temporary or permanently connect/disconnect AMI messages and communication link (wire-line or wire-less) flooding/jamming by spoofing packets [95]. As per IEC 61850, there is need of secure communication system which requires less computation overhead during data verification and attack detection between SMs and consumer equipments. Tunable signing and verification (TSV) protocol is good for wide area measurement system (WAMS) based communication applications [96]. The following table highlights various types of DOS attacks prevention schemes (Table 7).
- Man-in-the-middle (MITM) attacks: It is a type of an eavesdropping attack, where a malicious intruder inserts him/herself as a relay/proxy into a communication session between consumer or systems. After making independent connections with the victims and relays messages, making them believe that they are directly connected with each other. But in fact the entire

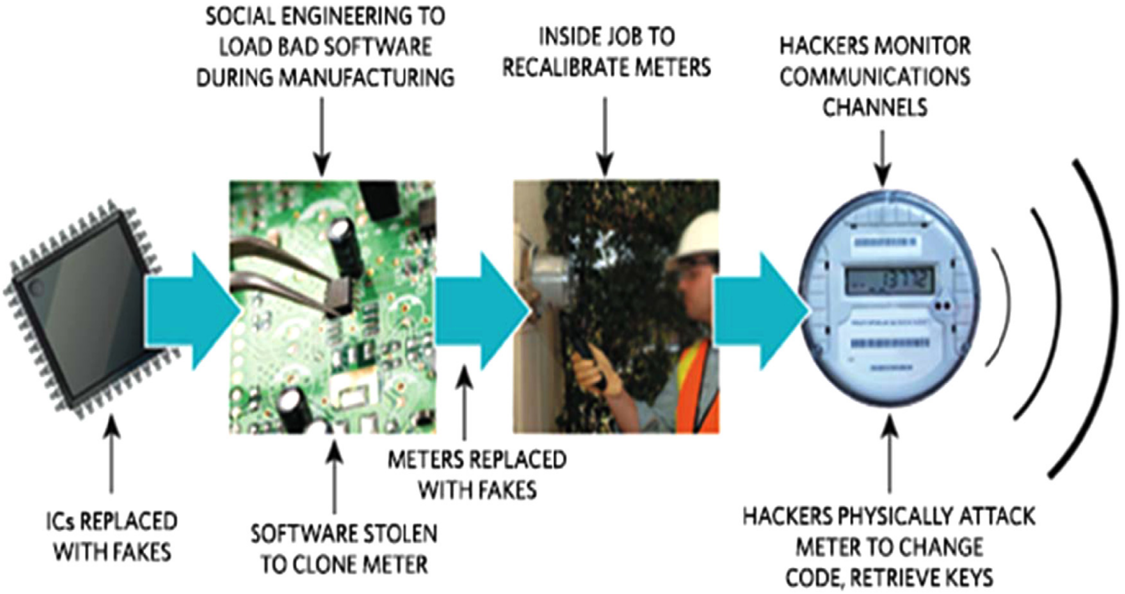

SOCIAL ENGINEERING TO LOAD BAD SOFTWARE DURING MANUFACTURING
INSIDE JOB TO RECALIBRATE METERS
HACKERS MONITOR COMMUNICATIONS CHANNELS
ICs REPLACED WITH FAKES
SOFTWARE STOLEN TO CLONE METER
METERS REPLACED WITH FAKES
HACKERS PHYSICALLY ATTACK METER TO CHANGE CODE, RETRIEVE KEYS

Fig. 6. A simplified model of threats to the life cycle of smart meters [81].

communication is controlled by the attacker. Several data exchange protocols such as transmission control protocol /internet protocol (TCP/IP), hypertext transfer protocol (HTTP) and file transfer protocol (FTP) can be easily hacked during MITM attacks [97,98]. So these protocols must be replaced with high security protocols like internet protocol security (IPSec), secure socket layer (SSL), transport layer security (TLS) and secure shell (SSH) for user data confidentiality, integrity and authentication. Considering all necessary points about MITM attacks, there is need to to implement efficient meter data aggregation system without individual leakage values between HAN devices. For this additive homo-morphic encryption scheme is good option [99]. The following table shows various MITM attacks prevention schemes (Table 8).

- Data integrity attacks: These attacks are related with data timings, data analysis, false-data injection, data replay and data modifications. During AMI applications sparse attacks [100], and churning attacks [101], are difficult to detect since they can be performed by an honest and curious adversary [101]. For this S/key on-time password scheme [102], and preprocessing algorithms [103], can provide secure authentication and mitigate privacy risks between SMs and SG servers With the advent of cloud computing and new technology trends that result in new failure modes for storage, interesting challenges arise in ensuring data integrity such as artificial data injections, data replay, and data modification. The following table shows various false-data attack prevention schemes (Table 9).

6. Conclusion

SM is a new area of research in SG infrastructure that has attracted rapidly growing attention in the government, industry and academia. Different countries and utility companies are working to establish better communication technologies and control over their electricity resources, manage peak demand, operate more efficiently, and accommodate massive amounts of DER systems. In this paper, we presented a comprehensive survey of smart metering for SG infrastructure, starting from discussing the potential benefits and past development stages to giving directions of future SMs infrastructure. SG infrastructure includes high efficiency power electronics components (i.e. metal-oxide-field-effect transistors (MOSFETs), insulated gate bipolar transistors (IGBTs) and diodes) with power ratings from few watts to megawatts to enable highly efficient and reliable power conversion for wind energy harvesting applications, where low power consumption is key requirement. In future PV installation based energy supply could be feasible. Economically an artificial intelligent meter (AIM) based AMI network and energy management schemes will decreases the peak hour usage of appliances, and decreases the consumers' carbon footprint [104]. Therefore AIM in future to accelerate roll-out of SGs. So we need to ensure stable, affordable, low-carbon SMM solutions. Harmonics measurement and their minimization at every level of SG applications increase the power quality area and deliver green technology (GT) to consumers. For this latest metrological solutions are reviewed, which are ideal to achieve higher power densities, voltages and efficiency levels that will be needed in the future. They also promise a state-of-the-art combination of hardware and software security for existing and ongoing SMs, smart sensors and renewable energy and storage systems.

SG communication network features, such as heterogeneous devices [105,106] and network architecture/model and topologies, delay constraints on different time scales between AMI and SCADA systems scalability, and diversified capabilities of embedded devices, make it indeed impractical to uniformly deploy strong security approaches over SG systems [63]. Consequently, there is no single and ultimate solution to security concerns involving electricity networks. Earlier days SM security was only focused on setting standards for privacy and the prevention of data theft. Now the SMs security threats are varied and evolving. Therefore we analyzed SM security vulnerabilities (i.e. hardware and software) through case studies, and discussed various attack prevention schemes. As we have reviewed, SM security is very fruitful and challenging research area and still under development for a new democratic and sustainable SG environment, especially because information security must be taken into account with various measurement systems such as PMUs [54,107] We wish to highlight the importance of SMs for SG by latest privacy-preserving/security schemes that has been globally treated as a technical issue. Although this work is ongoing and big efforts are still needed to accomplish this task, but the analysis is made in terms of suitable metrology ICs selection, energy management schemes and consumer privacy protection schemes, and the hurdles to be overcome for realization of nobel SG operation.

Table 6
Intrusion detection systems (IDS)/performance improvement/privacy preservation schemes in AMI.

Technique/scheme	Mode of communication		Advantages	Coverage area	Mode of operation		Country	Key reference
	Wire-less	Wire-line			Hardware	Software		
Certificate-less public key cryptography (CL-PKC)	✓	✓	Schnorr signature algorithm used	HAN ⇔ WAN	–	✓	USA	[22]
Hidden markov model (HMM) scheme	✓	–	Accurately audits physical and cyber-physical theft events	HAN ⇔ WAN	✓	✓	USA	[62]
Homo-morphic encryption scheme	✓	✓	Paillier cryptosystem used	HAN ⇔ WAN	–	✓	USA	[73]
Peer-to-peer computing protocol	✓	✓	Efficient and reliable to identify fraudulent electricity users constantly	NAN	–	✓ Matlab	USA	[74]
Homo-morphic encryption scheme	✓	✓	Key distribution table setup for secure data aggregation	HAN ⇔ NAN	–	✓	USA	[77]
Homo-morphic hash scheme (matrix based)	✓	✓	Reduces metrology computation	HAN ⇔ WAN	–	✓	South Korea	[79]
Physically un-clonable function (PUF) scheme	✓	–	Zero-knowledge proof of knowledge (ZKPK) protocol used	HAN ⇔ WAN	✓	✓	USA	[84]
Multiple key distribution server (KDS) scheme	✓	✓ LAN	Secure hashing (SHA-1) algorithm used	HAN ⇔ WAN	–	✓	India	[89]
Key management scheme (KMS)	✓	✓	Simple cryptographic algorithm used to avoid storage problems	HAN ⇔ WAN	–	✓	China	[91]
Authentication code (A-code)	–	✓ LAN	Short authenticators and feasible number of security keys	HAN ⇔ WAN	✓	✓	Japan	[92]
Enhanced routing protocol for low power and lossy networks (ERPLLNs)	✓ IEEE 802.15.4 Mesh radio	–	Easy to deploy and cost effective and reliable solution for smart metering networks	HAN ⇔ WAN	✓	–	United Kingdom	[93]
Integrated authentication and confidentiality (IAC) protocol	✓	–	Better end-to-end delay and low packet loss	HAN ⇔ WAN	–	✓	USA	[94]
Multi-interface zigbee building area network (MIZBAN)	✓ Zigbee	–	Improvement in application-layer latency up to 67-75 % to cater high-traffic AMI (HTAMI) networks	BAN	✓	✓ OPNET	Hongkong	[106]
Physical layer-assisted message authentication (PLAA) scheme	✓ SUN	–	Fast and lightweight message authentication between IEEE 802.15.4 g networks	HAN ⇔ NAN	–	✓	China	[124]
Gabidulin-Paramonov-Trejtakov (GPT) scheme	–	–	Location based security with smallest key size cryptosystem	HAN ⇔ WAN	–	✓	United Kingdom	[135]
Split and aggregated-TCP (SA-TCP) scheme	✓	–	Evaluates data traffic dynamics (i.e throughput, packet loss rate and packet delay)	HAN ⇔ WAN	–	✓ Network simulator-2	Canada	[140]
Data-stream based intrusion detection scheme	✓	✓	Offers higher accuracy in data concentrators and AMI head-ends	HAN ⇔ WAN	–	✓ MOA	UAE	[142]
Public key infrastructure (PKI) mechanism	✓	✓	Offers ID based mutual authentication between smart devices	HAN ⇔ WAN	–	✓	South Korea	[143]
Risk assessment framework	–	–	A systematic framework for AMI network improvement	HAN ⇔ WAN	–	✓ ADVISE	USA	[144]
Decentralized, efficient and selective aggregation (DESA) scheme	–	–	Paillier cryptosystems used	HAN ⇔ WAN	–	✓	United Kingdom	[170]

Table 7
Denial-of-service (DOS) attack prevention schemes for smart meter.

Technique/scheme	Mode of communication		Advantages	Coverage area	Mode of operation		Country	Key references
	Wire-less	Wire-line			Hardware	Software		
SecureHAN framework	✓ Zigbee	–	Secure communication system between smart meter and consumer equipment	HAN	✓	–	USA	[95]
Secure smart metering protocol (SSMP)	–	✓ PLC	Does not affect encrypted meter readings	HAN ⇔ WAN	✓	–	South Korea	[117]
Homomorphic encryption scheme	–	✓	Requires less communication and computation overhead during data verification and attack detection	HAN ⇔ WAN	–	✓	South Korea	[133]
Wide-area monitoring, protection and control (WAMPAC) scheme	–	–	Supports IEC 61850 and monitors local/substation devices geographically	HAN ⇔ WAN	–	–	Egypt	[139]

Table 8
Man-in-the-middle (MITM) attacks prevention schemes.

Technique/scheme	Mode of communication		Advantages	Coverage area	Mode of operation		Country	Key reference
	Wire-less	Wire-line			Hardware	Software		
Privacy-preserving aggregation (PPA) protocol	–	–	Efficient meter data aggregation without individual leakage values	HAN ⇔ WAN	–	✓	China	[97]
Device authentication algorithm	✓ Zigbee	–	Easy to implement between HAN devices	HAN	✓	–	USA	[111]
Time-varying encryption system (TVES) scheme	–	✓ LAN	Caesar cipher used	NAN ⇔ WAN	✓	✓ Labview	Taiwan	[113]
Privacy-enhanced data aggregation scheme	✓	✓	Tree-based aggregation scheme provides formal security proofs	HAN ⇔ WAN	–	✓	Taiwan	[141]
(i) Smart grid mutual authentication (SGMA) scheme (ii) Smart grid key management (SGKM) scheme	✓	✓	Enhanced identity-based cryptography (EIBC) used	HAN ⇔ WAN	–	✓ AVISPA	Canada	[152]
Group key scheme	✓	–	Pairing-based cryptosystem used	HAN ⇔ BAN	–	✓ Network simulator-2	USA	[163]

Table 9
False-data attack prevention schemes.

Technique/scheme	Mode of communication		Advantages	Coverage area	Mode of operation		Country	Key reference
	Wire-less	Wire-line			Hardware	Software		
Karush-kuhn-tucker (KKT) scheme	–	–	Identifies the most damaging attack on power system state estimation	HAN ⇔ WAN	–	✓ MATPOWER	USA	[72]
NeSSi^2 tool	✓	✓	Creates required network models and implement new applications	HAN ⇔ WAN	–	✓ NeSSi^2	Germany	[75]
Minimum transmission energy (MTE) routing protocol	✓ Ad-hoc	–	Energy aware protocol that least burdens transmitting nodes	HAN ⇔ WAN	–	✓	Australia	[76]
(i) Change and transmit (CAT) scheme (ii) Artificial spoofing packet (ASP) scheme	✓	–	Addition of artificial spoofing packets to mitigate the attack	HAN ⇔ WAN	–	✓ Qualnet	USA	[78]
Message authentication scheme (MAS)	✓	–	User data strong privacy preservation	HAN ⇔ BAN	✓	–	South Korea	[87]
An efficient aggregation protocol with error detection (APED) protocol	✓	✓	Guarantees security and privacy during malfunctioning smart meters	HAN WAN	–	✓	China	[138]
State summation detection (SSD) scheme	–	–	Compatible with traditional false data detection scheme	HAN ⇔ WAN	–	✓ MATPOWER	China	[145]
Watermarking-based detection scheme	✓ DSSS modulation	–	Identifies strong and stealthy data attacks	HAN ⇔ WAN	–	✓ Matlab	USA	[146]
Hardware/Software based crypto-engines	✓ Zigbee	–	Galois counter mode (GCM) cryptography used	HAN ⇔ BAN	✓	✓	Thailand	[147]
Merkle hash tree technique (MHTT)	✓ Wi-fi	–	Avoids replay attacks and data integrity attacks	HAN WAN	✓	✓	China/ Canada	[150]
Privacy-preservation aggregation scheme (PARK)	–	–	Users automatically can update encryption keys	HAN ⇔ WAN	–	✓	Canada	[162]
In-network data aggregation scheme	–	–	Light-weight security scheme for current smart meters configuration	NAN	–	✓	USA	[169]

Acknowledgement

This work was supported by Department of Electrical Engineering, National Institute of Technology Kurukshetra, India, and also by the Ministry of Human Resource Development (MHRD), Government of India. The authors would like to thank the editor and anonymous reviewers for their helpful and constructive comments that greatly contributed to improving the final version of the paper.

References

[1] Smart meter. Available from: ⟨http://en.wikipedia.org/wiki/Smart_meter⟩.
[2] Chou Chih-Ju, Liu Chun-Chang. Analysis of the performance of induction watthour meters in the presence of harmonics (a new model approach). Electric Power Syst Res 1995;32(1):71–9.
[3] Purkayastha I, Savoie PJ. Effect of harmonics on power measurement. IEEE Trans Ind Appl 1990;26(5):944–6.
[4] Op't Eynde F. A power metering ASIC with a sigma-delta-based multiplying ADC. In: Proceedings of the 1994 IEEE international conference on solid-state circuits. Digest of Technical Papers. 41st ISSCC; 16 – 18 Feb. 1994. p. 186 – 7.
[5] Riedmuller K, Forsyth R, Gierlinger A, Grimm G, Ofner E, Sattler S, et al. A mixed–signal ASIC with embedded DSP core for power metering application. In: Proceedings of the 24th European conference on solid-state circuits. ESSCIRC '98; 22 – 24 Sept. 1998. p. 460 – 3.
[6] Cavdar IH. A solution to remote detection of illegal electricity usage via power line communications. IEEE Trans Power Deliv 2004;19:1663–7.
[7] Yute C, Jeng HK. A reliable energy information system for promoting voluntary energy conservation benefits. IEEE Trans Power Deliv 2006;21(1):102–7.
[8] Sun-Ic Kim, Jong-Min Ko, Moon-Jong Jang, In Hyeob Yu, Il Kwon Yang, Won Chul Yang, et al.. Development of value-added service systems based on AMR data in power industry. In: Proceedings of the international joint conference, SICE-ICASE; 18 – 21 Oct. 2006. p. 1562 – 5.

[9] Majchrak M, Heinrich J, Fuchs P, Hostyn V. Single phase electricity meter based on mixed-signal processor MSP430FE427 with PLC modem. In: Proceedings of the 17th international conference, Radioelektronika; 24 – 25 April 2007. p. 1 – 4.

[10] ASM221: ASMGRID2^{TM} system-on-chip for smart meter PLC communication, single and polyphase metrology, communication and application processing. Available from: 〈http://www.accent-soc.com/products/ASM221_abridged_datasheet.pdf〉.

[11] Weiqing Tao, Yuqiu Xiang, Lin Li, Beijing Cui. Two methods realization of harmonic measurement based on MAXQ3180 for grid. In: Proceedings of the 2nd international conference on industrial and information systems (IIS), vol. 2; 10 – 11 July 2010. p. 176 – 9.

[12] Porcarelli Danilo, Balsamo Domenico, Brunelli Davide, Paci Giacomo. Perpetual and low-cost power meter for monitoring residential and industrial appliances. In: Proceedings of the design, automation & test in Europe conference & exhibition (DATE), 18 – 22 March 2013. p. 1155 – 60.

[13] MSP430F6736 mixed signal microcontroller. Available from: 〈http://www.ti.com/product/msp430f6736〉.

[14] Bernieri A, Ferrigno L, Laracca M, Luongo C. A discussion about the effect of the MID directive on the calibration of electrical energy meters. In: Proceedings of the 43rd international universities power engineering conference, UPEC 2008; 1 – 4 Sept. 2008. p. 1 – 5.

[15] Application note 5631 ensuring the complete life-cycle security of smart meter. Available from: 〈http://www.maximintegrated.com/en/app-notes/index.mvp/id/5631〉.

[16] Smart grid and energy solutions guide. Available from: 〈http://www.ti.com/general/docs/lit/getliterature.tsp?baseLiteratureNumber=slym071〉.

[17] PS2100 single phase power meter soc. Available from: 〈http://uk.alibaba.com/product/123927057-PS2100-Single-Phase-Power-Meter-SOC.html〉.

[18] Luo Zhi-kun, Wan Quan, Xu Xian-yong, Gao Yun-peng. Design of harmonic energy meter based on TDK+DSP+MCU. In: Proceedings of the 2012 international conference on measurement, information and control (MIC), vol. 2; 18 – 20 May 2012. p. 874 – 8.

[19] Smart meter and powerline communication system-on-chip. Available from: 〈http://www.st.com/stwebui/static/active/en/resource/technical/document/data_brief/DM00097094.pdf〉.

[20] Jawurek M, Johns M, Kerschbaum F. Plug-in privacy for smart metering billing. Privacy enhancing technologies. Berlin Heidelberg: Springer; 2011. p. 192–210.

[21] Ping-Hai Hsu, Wenshiang Tang, Chiakai Tsai, Bo-Chao Cheng. Two-layer security scheme for AMI system in Taiwan. In: Proceedings of the 2011 ninth IEEE international symposium on parallel and distributed processing with applications workshops (ISPAW); 26 – 28 May 2011. p. 105 – 10.

[22] Seung-Hyun Seo, Xiaoyu Ding, Bertino E. Encryption key management for secure communication in smart advanced metering infrastructures. In: Proceedings of the IEEE international conference on smart grid communications (SmartGridComm); 21 – 24 Oct. 2013. p. 498 – 503.

[23] Maity T, Das PS. A novel three phase energy meter model with wireless data reading and online billing solution. In: Proceedings of the 2011 IEEE symposium on computers & informatics (ISCI); 20 – 23 March 2011. p. 74 – 7.

[24] Erlinghagen Sabine, Lichtensteiger Bill, Markard Jochen. Smart meter communication standards in Europe – a comparison. Renew Sustain Energy Rev 2015;43:1249–62.

[25] Rahmatia, S, Samudra, Iswandi B. Design monitoring system kWh meter 3 phase using RFID system: PT. Multifabrindo Gemilang. In: Proceedings of the 2013 International Conference on ICT for Smart Society (ICISS); 13 – 14 June 2013. p. 1 – 4.

[26] Yaacoub Elias, Abu-Dayya Adnan. Automatic meter reading in the smart grid using contention based random access over the free cellular spectrum. Comput Netw 2014;59:171–83.

[27] Mohammad N, Barua A, Arafat MA. A smart prepaid energy metering system to control electricity theft. In: Proceedings of the 2013 international conference on power, energy and control (ICPEC); 6 – 8 Feb. 2013. p. 562 – 5.

[28] Khan TA, Khan AB, Babar M, Taj TA, Ijaz I. Smart meter incorporating UWB technology. In: Proceedings of the 2014 IEEE electrical and electronic engineering conference (ElConRusNW), NW Russia Young Researchers; 3 – 5 Feb. 2014. p. 75 – 8.

[29] Ghodki Manish Kumar. Microcontroller and solar power based electrical energy management system for renewable energy applications. Int J Electr Power Energy Syst 2013;44(1):852–60.

[30] Press release maxim intregated's complete smart-meter system-on-a-chip combines metrology, security, and communication. Available from: 〈http://www.maximintegrated.com/en/company/newsroom/pr_products/show.mvp/npk/1680〉.

[31] Ciuciu IG, Meersman R, Dillon T. Social network of smart-metered homes and SMEs for grid-based renewable energy exchange. In: Proceedings of the 6th IEEE international conference on digital ecosystems technologies (DEST). 18 – 20 June 2012. p. 1 – 6.

[32] Christoforidis GC, Chrysochos A, Papagiannis G, Hatzipanayi M, Georghiou GE. Promoting PV energy through net metering optimization: the PV-NET project. In: Proceedings of the 2013 international conference on renewable energy research and applications (ICRERA); 20 – 23 Oct. 2013. p. 1117 – 22.

[33] Yang Fan, Rimali V, Tang M, Nayar C. Design and implementation of stand-alone smart grid employing renewable energy resources on Pulau Ubin Island of Singapore. In: Proceedings of the 2012 Asia-Pacific symposium on electromagnetic compatibility (APEMC); 21 – 24 May 2012. p. 441 – 4.

[34] De Smedt G, Adonis M. Smart meter for renewable energy microgrid island. In: Proceedings of the twenty-second domestic use of energy (DUE); 1 – 2 April 2014. p. 1 – 5.

[35] Ngamchuen S, Pirak C. Smart anti-tampering algorithm design for single phase smart meter applied to AMI systems. In: Proceedings of the 10th international conference on electrical engineering/electronics, computer, telecommunications and information technology (ECTI-CON); 15 – 17 May 2013. p. 1 – 6.

[36] 78M6613 single-phase ac power measurement IC. Available from: 〈http://datasheets.maximintegrated.com/en/ds/78M6613.pdf〉.

[37] Application note 5536 energy measurement and security for the smart grid – too long overlooked. Available from: 〈http://www.maximintegrated.com/en/app-notes/index.mvp/id/5536〉.

[38] Suslov KV, Stepanov VS, Solonina NN. Smart grid: effect of high harmonics on electricity consumers in distribution networks. In: Proceedings of the international symposium on electromagnetic compatibility (EMC EUROPE); 2 – 6 Sept. 2013. p. 841 – 5.

[39] Lee PK, Lai LL. A practical approach of smart metering in remote monitoring of renewable energy applications. In: Proceedings of the IEEE power & energy society general meeting (PES '09); 26 – 30 July 2009. p. 1 – 4.

[40] Arghandeh Reza, Onen Ahmet, Jung Jaesung, Broadwater Robert P. Harmonic interactions of multiple distributed energy resources in power distribution networks. Electric Power Syst Res 2013;105:124–33.

[41] Benhabib MC, Myrzik JMA, Duarte JL. Harmonic effects caused by large scale PV installations in LV network. In: Proceedings of the 9th international conference on electrical power quality and utilisation (EPQU 2007); 9 – 11 Oct. 2007. p. 1 – 6.

[42] Cataliotti A, Cosentino V, Nuccio S. Static meters for the reactive energy in the presence of harmonics: an experimental metrological characterization. IEEE Trans Instrum Meas 2009;58(8):2574–9.

[43] Singh R, Singh A. Energy loss due to harmonics in residential campus – a case study. In: Proceedings of the 45th international universities power engineering conference (UPEC); Aug. 31 2010 – Sept. 3 2010. p. 1 – 6.

[44] De Capua C, Romeo E. A smart THD meter performing an original uncertainty evaluation procedure. IEEE Trans Instrum Meas Aug. 2007;56(4):1257–64.

[45] Makram EB, Haines RB, Girgis AA. Effect of harmonic distortion in reactive power measurement. IEEE Trans Ind Appl 1992;28(4):782–7.

[46] Shmilovitz D. On the definition of total harmonic distortion and its effect on measurement interpretation. IEEE Trans Power Deliv 2005;20(1):526–8.

[47] Arseneau, R. Harmonic cost allocation with existing and proposed revenue metering methods. In: Proceedings of the 1999 IEEE power engineering society summer meeting, vol. 1; 18 – 22 Jul. 1999. p. 341 – 6.

[48] Suslov KV, Solonina NN, Smirnov AS. Smart meters for distributed filtering of high harmonics in Smart Grid. In: Proceedings of the 2011 international conference on power engineering, energy and electrical drives (POWERENG); 11 – 13 May 2011. p. 1 – 5.

[49] Fugita SD, Fernandes RAS, Suetake M, da Silva IN. Hall sensors applied as transducers to smart meters in the context of power quality. In: Proceedings of the IEEE PES conference on innovative smart grid technologies Latin America (ISGT LA); 15 – 17 April 2013. p. 1 – 5.

[50] Ramírez Muñoz D, Moro Pérez D, Sánchez Moreno J, Casans Berga S, Castro Montero E. Design and experimental verification of a smart sensor to measure the energy and power consumption in a one-phase AC line. Measurement 2009;42(3):412–9.

[51] Cataliotti A, Di Cara D, Emanuel AE, Nuccio S. Current transformers effects on the measurement of harmonic active power in LV and MV networks. IEEE Trans Power Deliv 2011;26(1):360–8.

[52] Sadinezhad Iman, Agelidis Vassilios G. Slow sampling on-line harmonics/interharmonics estimation technique for smart meters. Electric Power Syst Res 2011;81(8).

[53] Dag O, Uçak C, Usta O. Harmonic source location and meter placement optimization by impedance network approach. Electr Eng 2012;94(1):1–10.

[54] Dotta D, Chow JH. Second harmonic filtering in phasor measurement estimation. IEEE Trans Power Deliv 2013;28(2):1240–1.

[55] Reza MS, Ciobotaru M, Agelidis VG. Power system frequency estimation by using a newton-type technique for smart meters. IEEE Trans Instrum Meas 2015;64(3):615–24.

[56] Youhannaei M, Ouni S, Mokhtari H, Honarmand ME, Mehri R, Talebi J. Performance evaluation of energy meters in nonsinusoidal environment based on IEEE 1459 standard. In: Proceedings of the 22nd international conference and exhibition on electricity distribution (CIRED); 10 – 13 June 2013. p. 1 – 4.

[57] Bernieri Andrea, Betta Giovanni, Ferrigno Luigi, Laracca Marco, Schiano Lo Moriello Rosario. Electrical energy metering: some challenges of the european directive on measuring instruments (MID). Measurement 2013;46(9):3347–54.

[58] PL3223 3ph multifunction meter measuring ic. Available from:〈http://www.xiaocheng.com/eng/products/view.php?id=46〉.

[59] Jianyu Zhang; Maofa Gong; Lanbing Li; Yanping Su; Tao Liu. Study on poly phase multifunction energy metering IC. In: Proceedings of the seventh international conference on image and graphics (ICIG); 26 – 28 July 2013. p. 770 – 3.

[60] Atmel M90E36A enhanced poly-phase high-performance wide-span energy metering IC. Available from: 〈http://www.atmel.com/Images/Atmel-46004-SE-M90E36A-Datasheet.pdf〉.

[61] Husheng Li, Rukun Mao, Lifeng Lai, Qiu RC. Compressed meter reading for delay-sensitive and secure load report in smart grid. In: Proceedings of the first IEEE international conference on smart grid communications (smartgridcomm); 4 – 6 Oct. 2010. p. 114 – 9.

[62] McLaughlin S, Holbert B, Fawaz A, Berthier R, Zonouz S. A multi-sensor energy theft detection framework for advanced metering infrastructures. IEEE J Select Areas Commun 2013;31(7):1319–30.

[63] Haynes DD, Corns SM. Timekeeping issues in ultra-quality metering system. IEEE Trans Smart Grid 2014;5(1):392–3.

[64] Ren Wei, Song Jun, Yang Yu, Ren Yi. Lightweight privacy-aware yet accountable secure scheme for SM-SGCC communications in smart grid. Tsinghua Sci Technol 2011;16(6):640–7.

[65] Taneja M. Lightweight security protocols for smart metering. In: Proceedings of the IEEE innovative smart grid technologies – Asia (ISGT Asia); 10 – 13 Nov. 2013. p. 1 – 5.

[66] Huang Jingfang, Wang Honggang, Qian Yi, Wang Chonggang. Priority-based traffic scheduling and utility optimization for cognitive radio communication infrastructure-based smart grid. IEEE Trans Smart Grid 2013;4(1):78–86.

[67] Debnath Ashmita, Singaravelu Pradheepkumar, Verma Shekhar. Privacy in wireless sensor networks using ring signature. J King Saud Univ – Comput Inform Sci 2014 Available online.

[68] Lunkeit Armin, Voss Tobias, Pohl Hartmut. Threat modeling smart metering gateways. In: Proceedings of 2013 European conference on smart objects, systems and technologies (SmartSysTech); 11 – 12 June 2013. p. 1 – 5.

[69] Sikora Axel. Implementation of standardized secure smart meter communication. In: Proceedings of 2013 35th international telecommunications energy conference 'smart power and efficiency' (INTELEC); 13 – 17 Oct. 2013. p. 1 – 5.

[70] Chim T, Yiu S, Li V, Hui C, Zhong J.. PRGA: privacy-preserving recording & gateway-assisted authentication of power usage information for smart grid. IEEE Trans Depend Secure Comput, 99, 1 – 1.

[71] Bartsch Markus. German smart metering and european privacy needs. Security in critical infrastructures today. In: Proceedings of international ETG-congress; symposium 1; 5 – 6 Nov. 2013. p. 1 – 3.

[72] Yuan Yanling, Li Zuyi, Ren Kui. Modeling load redistribution attacks in power systems. IEEE Trans Smart Grid 2011;2(2):382–90.

[73] Deng Pan, Yang Liuqing. A secure and privacy-preserving communication scheme for advanced metering infrastructure. Innovative Smart Grid Technologies (ISGT) 2012:1–5 IEEE PES.

[74] Sergio Salinas, Ming Li, Pan Li. Privacy-preserving energy theft detection in smart grids: a P2P computing approach. IEEE J Select Areas Commun 2013;31(9):257–67.

[75] Chinnow J, Bsufka K, Schmidt AD, Bye R, Camtepe A, Albayrak S. A simulation framework for smart meter security evaluation. In: Proceedings of the 2011 IEEE international conference on smart measurements for future grids (SMFG); 14 – 16 Nov. 2011. p. 1 – 9.

[76] Kaplantzis Sophia, Sekercioglu Y Ahmet. Security and smart metering. In: Proceedings of the 18th European wireless conference, EW; 18 – 20 April 2012. p. 1 – 8.

[77] Kamto J, Lijun Qian, Fuller J, Attia J, Yi Qian. Key distribution and management for power aggregation and accountability in advance metering infrastructure. In: Proceedings of the 2012 IEEE third international conference on smart grid communications (SmartGridComm); 5 – 8 Nov. 2012. p. 360 – 5.

[78] Li Husheng, Gong Shuping, Lai Lifeng, Han Zhu, Qiu RC, Yang Depeng. Efficient and secure wireless communications for advanced metering infrastructure in smart grids. IEEE Trans Smart Grid 2012;3(3):1540–51.

[79] Kim Young-Sam, Heo Joon. Device authentication protocol for smart grid systems using homomorphic hash. J Commun Netw 2012;14(6):606–13.

[80] Kadurek P, Blom J, Cobben JFG, Kling WL. Theft detection and smart metering practices and expectations in the Netherlands. In: Proceedings of the IEEE innovative smart grid technologies conference Europe (ISGT Europe); 11 – 13 Oct. 2010. p. 1 – 6.

[81] Application note 5926 battling threats in the smart grid supply chain. Available from: 〈http://www.maximintegrated.com/en/app-notes/index.mvp/id/5926〉.

[82] Bat-Erdene B, Nam SY, Kim DH. A novel remote detection method of illegal electricity usage based on smart resistance. Futur Inform Technol 2011:214–23.

[83] Shouchao Feng, Ling Zhu, Zhenbo Liu. The zero line current transformer in smart meter. In: Proceedings of the 2012 International Conference on Computer Science and Electronics Engineering (ICCSEE), vol. 2; 23 – 25 March 2012. p. 269 – 72.

[84] Nabeel M, Kerr S, Xiaoyu Ding, Bertino E. Authentication and key management for advanced metering infrastructures utilizing physically unclonable functions. In: Proceedings of the 2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm); 5 – 8 Nov. 2012. p. 324 – 9.

[85] Boccardo DR, Gomes dos Santos LC, da Costa Carmo LFR, Dezan MH, Machado RCS, de Aguiar Portugal S. Software evaluation of smart meters within a legal metrology perspective: a Brazilian case. In: Proceedings of the 2010 IEEE PES innovative smart grid technologies conference Europe (ISGT Europe); 11 – 13 Oct. 2010. p. 1 – 7.

[86] Lixia Zhou, Xun Liao, Shunxin Li, Jincan Yuan. Design and development of the reliability prediction software for smart meters. In: Proceedings of the 2012 international conference on quality, reliability, risk, maintenance, and safety engineering (ICQR2MSE); 15 – 18 June 2012. p. 612 – 6.

[87] Yun-Seok Lee, Eun Kim, Young-Sub Kim, Ha-Yong Jeon, Min-soo Jung. A study on secure chip for message authentication between a smart meter and home appliances in smart grid. In: Proceedings of the 2013 international conference on IT convergence and security (ICITCS); 16 – 18 Dec. 2013. p. 1 – 3.

[88] Application note 5537 smart grid security: recent history demonstrates the dire need. Available from: 〈http://www.maximintegrated.com/en/app-notes/index.mvp/id/5537〉.

[89] Thomas MS, Ali I, Gupta N. A secure way of exchanging the secret keys in advanced metering infrastructure. In: Proceedings of the 2012 IEEE international conference on power system technology (POWERCON); Oct. 30, 2012 – Nov. 2, 2012. p. 1 – 7.

[90] Zhou Jiazhen, Hu RQ, Qian Yi. Scalable distributed communication architectures to support advanced metering infrastructure in smart grid. IEEE Trans Parallel Distrib Syst 2012;23(9):1632–42.

[91] Liu Nian, Chen Jinshan, Zhu Lin, Zhang Jianhua, He Yanling. A key management scheme for secure communications of advanced metering infrastructure in smart grid. IEEE Trans Ind Electron 2013;60(10):4746–56.

[92] Matsumoto T, Kobayashi T, Katayama S, Fukushima K, Sekiguchi K. Information-theoretic approach to authentication codes for power system communications. In: Proceedings of the 2010 IEEE PES transmission and distribution conference and exposition; 19 – 22 April 2010. p. 1 – 7.

[93] Kulkarni P, Gormus S, Fan Zhong, Motz B. A mesh-radio-based solution for smart metering networks,. IEEE Commun Mag 2012;50(7):86–95.

[94] Yan Ye, Hu RQ, Das SK, Sharif H, Qian Yi. An efficient security protocol for advanced metering infrastructure in smart grid. IEEE Netw 2013;27(4):64–71.

[95] Namboodiri V, Aravinthan V, Mohapatra SN, Karimi B, Jewell W. Toward a secure wireless-based home area network for metering in smart grids. IEEE Syst J, vol. 99, p. 1 – 12, 0.

[96] Katti RS, Sule R, Kavasseri RG. WiP abstract: multicast authentication in the smart grid with one-time signatures from sigma-protocols. In: Proceedings of the 2013 ACM/IEEE international conference on cyber-physical systems (ICCPS); 8 – 11 April 2013. p. 239.

[97] Jia W., Zhu H., Cao Z., Dong X., Xiao C. Human-factor-aware privacy-preserving aggregation in smart grid. IEEE Syst J, vol. 99, p. 1 – 10, 0.

[98] Yigit Melike, Cagri Gungor V, Baktir Selcuk. Cloud computing for smart grid applications. Comput Netw 2014;70:312–29.

[99] Yukun Niu, Xiaobin Tan, Shi Chen, haifeng Wang, Kai Yu, Zhiyong Bu. A security privacy protection scheme for data collection of smart meters based on homomorphic encryption,. IEEE EUROCON 1 – 4 July 2013:1401–5.

[100] Giani A, Bitar E, Garcia M, McQueen M, Khargonekar P, Poolla K. Smart grid data integrity attacks. IEEE Trans Smart Grid 2013;4(3):1244–53.

[101] Stegelmann M, Kesdogan D. GridPriv: a smart metering architecture offering k-anonymity. In: Proceedings of the 2012 IEEE 11th international conference on trust, security and privacy in computing and communications (TrustCom); 25 – 27 June 2012. p. 419 – 426.

[102] Wei-Bin Lee, Tzung-Her Chen, Wei-Rung Sun, Ho, KI-J. An s/key-like one-time password authentication scheme using smart cards for smart meter. In: Proceedings of the 2014 28th international conference on advanced information networking and applications workshops (WAINA); 13 – 16 May 2014. p. 281 – 286.

[103] Reinhardt Andreas, Englert Frank, Christin Delphine. Averting the privacy risks of smart metering by local data preprocessing. Pervasive Mob Comput 2015;16(Part A):171–83.

[104] Aziz AFA, Khalid SN, Mustafa MW, Shareef H, Aliyu G. Artificial intelligent meter development based on advanced metering infrastructure technology. Renew Sustain Energy Rev 2013;27:191–7.

[105] Prapasawad C, Pornprasitpol K, Pora W. Development of an automatic meter reading system based on ZigBee PRO Smart Energy Profile IEEE 802.15.4 standard. In: Proceedings of the 2012 IEEE international conference on electron devices and solid state circuit (EDSSC); 3 – 5 Dec. 2012. p. 1 – 3.

[106] Tung Hoi Yan, Tsang Kim Fung, Chui Kwok Tai, Tung Hoi Ching, Chi Hao Ran, Hancke GP, et al. The generic design of a high-traffic advanced metering infrastructure using zigbee. IEEE Trans Ind Inform 2014;10(1):836–44.

[107] Qiu Meikang, Su Hai, Chen Min, Ming Zhong, Yang LT. Balance of security strength and energy for a PMU monitoring system in smart grid. IEEE Commun Mag 2012;50(5):142–9.

[108] Cho Hyun Sang, Yamazaki T, Hahn Minsoo. Determining location of appliances from multi-hop tree structures of power strip type smart meters. IEEE Trans Consum Electron 2009;55(4):2314–22.

[109] Han Shuxia, Qu Wei, Qiu Cheng-jun. The design of electric power control system for oil-pumping unit based on energy metering ADE7758. In: Proceedings of the international conference on information engineering and computer science. ICIECS 2009; 19 – 20 Dec. 2009. p. 1 – 4.

[110] Park Seunghyun, Kim Hanjoo, Moon Hichan, Heo Jun, Yoon Sungroh. Concurrent simulation platform for energy-aware smart metering systems. IEEE Trans Consum Electron 2010;56(3):1918–26.

[111] Ayday E, Rajagopal S. Secure, intuitive and low-cost device authentication for smart grid networks. In: Proceedings of the IEEE consumer communications and networking conference (CCNC); 9 – 12 Jan. 2011. p. 1161 – 5.

[112] Huang Haoran, Duan Zhengang, Lian Xiaoqin. Design of three phase network parameter monitoring system based on 71M6513. In: Proceedings of the control and decision conference (CCDC), 2011 Chinese; 23 – 25 May 2011. p. 3582 – 5.

[113] Te-Kwei Wang, Fan-Ren Chang. Network time protocol based time-varying encryption system for smart grid meter. In: Proceedings of the 2011 ninth

IEEE international symposium on parallel and distributed processing with applications workshops (ISPAW); 26 – 28 May 2011. p. 99 – 104.

[114] O'Connell S, Barton J, O'Connell E, O'Flynn B, Popovici E, O'Mathuna SC, et al. Remote electricity actuation and monitoring mote. In: Proceedings of the 2011 international conference on distributed computing in sensor systems and workshops (DCOSS); 27 – 29 June 2011. p. 1 – 6.

[115] Hindersah H, Purwadi A, Ali FY, Heryana N. Prototype development of single phase prepaid kWh meter. In: Proceedings of the 2011 international conference on electrical engineering and informatics (ICEEI); 17 – 19 July 2011. p. 1 – 6.

[116] Shunhao Hu, Canpei Wu. An intelligent hotel room controller based on power line communication. In: Proceedings of the 2011 international conference on electronics, communications and control (ICECC); 9 – 11 Sept. 2011. p. 1313 – 6.

[117] Kim Sungwook, Young Kwon Eun, Kim Myungsun, Hee Cheon Jung, Ju Seongho, Lim Yong-hoon, et al. A secure smart-metering protocol over power-line communication. IEEE Trans Power Deliv 2011;26(4):2370–9.

[118] Jiho Kim, Wan-Hee Cho, Yongjin Jeong, Ohyoung Song. Intelligent energy management system for smart offices. In: Proceedings of the 2012 IEEE international conference on consumer electronics (ICCE); 13 – 16 Jan. 2012. p. 668 – 9.

[119] Prudhvi P, Bhalodi D, Manohar M, Padidela V, Adapa S. A smart energy meter architecture in Indian context. In: Proceedings of the 2012 2nd Iranian conference on smart grids (ICSG); 24 – 25 May 2012. p. 1 – 6.

[120] Snram V, Nivass SA, Selvam C. Bi-directional energy meters and remote monitoring of energy nodes using LonWorks technology. In: Proceedings of the 2012 4th international conference on intelligent and advanced systems (ICIAS), vol. 2; 12 – 14 June 2012. p. 536 – 9.

[121] Qipeng Ma, Chenxu Duan, Xudong Ding, Tingwei Qian, Peiyong Duan. A design of network prepayment meter reading system based on ESAM. In: Proceedings of the 2012 7th IEEE conference on industrial electronics and applications (ICIEA); 18 – 20 July 2012. p. 686 – 90.

[122] Azasoo JQ, Boateng KO. Smart metering: a GSM approach in Ghana. In: Proceedings of the 2012 IEEE 4th international conference on adaptive science & technology (ICAST); 25 – 27 Oct. 2012. p. 158 – 63.

[123] Afridi MI, Faisal S, Bangash H UD, Ali QW, Arif A. GSM based smart distribution system. IJECE 2012;2(5):589–96.

[124] Wen Hong, Wang Yifan, Zhu Xiping, Li Jianqiang, Zhou Liang. Physical layer assist authentication technique for smart meter system. IET Commun 2013;7(3):189–97.

[125] Xiao Zhifeng, Xiao Yang, Du DH. Exploring malicious meter inspection in neighborhood area smart grids. IEEE Trans Smart Grid 2013;4(1):214–26.

[126] Finster S, Baumgart I. Elderberry: a peer-to-peer, privacy-aware smart metering protocol. In: Proceedings of the 2013 IEEE conference on computer communications workshops (INFOCOM WKSHPS); 14 – 19 April 2013. p. 37 – 42.

[127] Gallo D, Landi C, Luiso M, Bucci G, Fiorucci E. Low cost smart power metering. In: Proceedings of the instrumentation and measurement technology conference (I2MTC), 2013 IEEE international; 6 – 9 May 2013. p. 763 – 7.

[128] Rottondi Cristina, Verticale Giacomo, Capone Antonio. Privacy-preserving smart metering with multiple data consumers. Comput Netw 2013; 57(7):1699–713.

[129] Depuru Soma Shekara Sreenadh Reddy, Wang Lingfeng, Devabhaktuni Vijay, Green Robert C. High performance computing for detection of electricity theft. Int J Electr Power Energy Syst 2013;47:21–30.

[130] Wen Mi, Lu Rongxing, Zhang Kuan, Lei Jingsheng, Liang Xiaohui, Shen Xuemin. PaRQ: a privacy-preserving range query scheme over encrypted metering data for smart grid. IEEE Trans Emerg Top Comput 2013; 1(1):178–91.

[131] Rottondi C, Verticale G, Krauss C. Distributed privacy-preserving aggregation of metering data in smart grids. IEEE J Select Areas Commun 2013; 31(7):1342–54.

[132] Huang Shih-Che, Lo Yuan-Liang, Lu Chan-Nan. Non-technical loss detection using state estimation and analysis of variance. IEEE Trans Power Syst 2013;28(3):2959–66.

[133] Inshil Doh, Jiyoung Lim, Kijoon Chae. Secure aggregation and attack detection for smart grid system. In: Proceedings of the 2013 16th international conference on network-based information systems (NBiS); 4 – 6 Sept. 2013. p. 270 – 5.

[134] Danezis George, Fournet Cédric, Kohlweiss Markulf, Santiago Zanella-Béguelin. Smart meter aggregation via secret-sharing. Proceedings of the first ACM workshop on smart energy grid security 2013 (SEGS '13).

[135] Khan Eraj, Adebisi Bamidele, Honary Bahram. Location based security for smart grid applications. Energy Proc 2013;42:299–307.

[136] Piska S., Shetty M. A java card based approach for smart meter gateway security. In: Proceedings of the innovative smart grid technologies – Asia (ISGT Asia), 2013 IEEE; 10 – 13 Nov. 2013. p. 1 – 5.

[137] Bat-Erdene B, Lee B, Kim MY, Ahn TH, Kim D. Extended smart meters-based remote detection method for illegal electricity usage. IET Gener, Transm Distribut 2013;7(11):1332–43.

[138] Ruixue Sun, Zhiguo Shi, Rongxing Lu, Min Lu, Xuemin Shen. APED: an efficient aggregation protocol with error detection for smart grid communications. In: Proceedings of the global communications conference (GLOBECOM), 2013 IEEE; 9 – 13 Dec. 2013. p. 432 – 7.

[139] Ashok Aditya, Hahn Adam, Govindarasu Manimaran. Cyber-physical security of wide-area monitoring, protection and control in a smart grid environment. J Adv Res 2013;27 Available online.

[140] Khalifa T, Abdrabou A, Naik K, Alsabaan M, Nayak A, Goel N. Split- and aggregated-transmission control protocol (SA-TCP) for smart power grid. IEEE Trans Smart Grid 2014;5(1):381–91.

[141] Fan Chun-I, Huang Shi-Yuan, Lai Yih-Loong. Privacy-enhanced data aggregation scheme against internal attackers in smart grid. IEEE Trans Ind Inform 2014;10(1):666–75.

[142] Faisal MA, Aung Z, Williams JR, Sanchez A. Data-stream-based intrusion detection system for advanced metering infrastructure in smart grid: a feasibility study. IEEE Syst J, vol. 99, p. 1 – 14.

[143] Sangji Lee, Jinsuk Bong, Sunhee Shin, Yongtae Shin. A security mechanism of Smart grid AMI network through smart device mutual authentication. In: Proceedings of the 2014 international conference on information networking (ICOIN); 10 – 12 Feb. 2014. p. 592 – 5.

[144] Cardenas AA, Berthier R, Bobba RB, Huh JH, Jetcheva JG, Grochocki D, et al. A framework for evaluating intrusion detection architectures in advanced metering infrastructures. IEEE Trans Smart Grid 2014;5(2):906–15.

[145] Li Yuancheng, Wang Yiliang. State summation for detecting false data attack on smart grid. Int J Electr Power Energy Syst 2014;57:156–63.

[146] Yu W, Griffith D, Ge L, Bhattarai S, Golmie N. An integrated detection system against false data injection attacks in the smart grid. Secur Commun Netw 2014.

[147] Somkaew W, Thepphaeng S, Pirak C. Data security implementation over ZigBee networks for AMI systems. In: Proceedings of the 2014 11th international conference on electrical engineering/electronics, computer, telecommunications and information technology (ECTI-CON); 14 – 17 May 2014. p. 1 – 5.

[148] Khan MA, Javaid N, Arif M, Saud S, Qasim U, Khan ZA. Peak load scheduling in smart grid communication environment. In: Proceedings of the 2014 IEEE 28th international conference on advanced information networking and applications (AINA); 13 – 16 May 2014. p. 1025 – 32.

[149] Xu Wilsun, Dong Ming, Meira Paulo, Freitas Walmir. An event window based load monitoring technique for smart meters. In: Proceedings of the PES General Meeting Conference & Exposition, 2014 IEEE; 27 – 31 July 2014. p. 1 – 1.

[150] Li H, Lu R, Zhou L, Yang B, Shen X. An efficient merkle-tree-based authentication scheme for smart grid. IEEE Syst J, vol. 99, p. 1 – 9, 0.

[151] Guo Z, Wang ZJ, Kashani A. Home appliance load modeling from aggregated smart meter data. IEEE Trans Power Systems, vol. 99. p. 1 – 9.

[152] Nicanfar H, Jokar P, Beznosov K, Leung VCM. Efficient authentication and key management mechanisms for smart grid communications. IEEE Syst J, vol. 99. p. 1 – 12, 0.

[153] Kalogridis G, Sooriyabandara M, Fan Z, Mustafa MA. Toward unified security and privacy protection for smart meter networks. IEEE Syst J, vol. 99. p. 1 – 14, 0.

[154] Saputro N, Akkaya K. On preserving user privacy in Smart Grid advanced metering infrastructure applications. Secur Commun Netw 2014;7(1):206–20.

[155] Borges F, Muhlhauser M. EPPP4SMS: efficient privacy-preserving protocol for smart metering systems and its simulation using real-world data. IEEE Trans Smart Grid 2014;5(6):2701–8.

[156] MSP430F6779 mixed signal microcontroller. Available from: 〈http://www.ti.com/product/msp430f6779〉.

[157] ADE7880 polyphase multifunction energy metering ic with harmonic monitoring. Available from: 〈http://www.analog.com/en/analog-to-digital-converters/energy-measurement/ade7880/products/product.html〉.

[158] STPM32 single phase metering ics. Available from: 〈http://www.st.com/web/en/catalog/sense_power/FM1963/SC397/SS1214/PF259470〉.

[159] ATM90E26. Available from: 〈http://www.atmel.com/devices/ATM90E26.aspx〉.

[160] Gatsis N, Giannakis GB. Residential load control: distributed scheduling and convergence with lost AMI messages. IEEE Trans Smart Grid 2012;3(2):770–86.

[161] Sivapragash C, Thilaga SR, Kumar SS. Advanced cloud computing in smart power grid. Proceedings of the IET Chennai 3rd International on Sustainable Energy and Intelligent Systems (SEISCON 2012) 27 – 29 Dec. 2012:1–6.

[162] Kuan Zhang, Rongxing Lu, Xiaohui Liang, Jian Qiao, Xuemin Shen. PARK: a privacy-preserving aggregation scheme with adaptive key management for smart grid. In: Proceedings of the 2013 IEEE/CIC international conference on communications in China (ICCC); 12 – 14 Aug. 2013. p. 236 – 41.

[163] Li Depeng, Aung Zeyar, Sampalli Srinivas, Williams John, Sanchez Abel. Privacy preservation scheme for multicast communications in smart buildings of the smart grid. Smart Grid Renew Energy 2013;4(4).

[164] Yang Lei, Chen Xu, Zhang Junshan, Poor HV. Cost-effective and privacy-preserving energy management for smart meters. IEEE Trans Smart Grid 2015;6(1):486–95.

[165] Jishun Jiang, Lanlan Yu. Design of a new three-phase multi-rate watt-hour meter based on singlechip. In: Proceedings of the international conference on computational intelligence and software engineering, 2009. CiSE 2009; 11 – 13 Dec. 2009. p. 1 – 4.

[166] MSP430F6779 mixed signal microcontroller. Available from: 〈http://www.ti.com/product/MSP430F6779〉.

[167] Thoma C, Cui Tao, Franchetti F. Secure multiparty computation based privacy preserving smart metering system. Proceedings of the North American power symposium (NAPS) 9 – 11 Sept. 2012:1–6.

[168] Kirschbaum M, Plos T, Schmidt J-M. On secure multi-party computation in bandwidth-limited smart-meter systems. In: Proceedings of the 2013 eighth international conference on availability, reliability and security (ARES); 2 – 6 Sept. 2013. p. 230 – 5.

[169] Lei Yang, Fengjun Li. Detecting false data injection in smart grid in-network aggregation. In: Proceedings of the 2013 IEEE international conference on smart grid communications (SmartGridComm); 21 – 24 Oct. 2013. p. 408 – 13.

[170] Mustafa MA, Ning Zhang, Kalogridis G, Zhong Fan. DESA: a decentralized, efficient and selective aggregation scheme in AMI. In: Proceedings of the innovative smart grid technologies conference (ISGT), 2014 IEEE PES; 19 – 22 Feb. 2014. p. 1 – 5.