A Survey on Smart Grid Metering Infrastructures: Threats and Solutions

[†] Rasel Mahmud, *Student Member, IEEE*, [Ψ] Ranganath Vallakati, *Student Member, IEEE*, [Ψ]
Anupam Mukherjee, *Student Member, IEEE*, [Ψ] Prakash Ranganathan, *Senior Member, IEEE*,
[†]Arash Nejadpak, *Member, IEEE*
[†]Power Electronics and Energy Laboratory, Department of Electrical Engineering
Universitv of North Dakota. Grand Forks. ND
[Ψ] Secure Cyber Physical Energy Systems and Data Sciences Laboratory, Department of Electrical Engineering
University of North Dakota, Grand Forks, ND

Abstract— **Without a reliable metering and communication infrastructure, the smart grid could become a catastrophe to national security and economy. A true smart grid infrastructure should detect all existing and predict future threats through intrusion detection methods. Smart grids are susceptible to various physical and cyber-attack as a result of communication, control and computation vulnerabilities employed in the grid. The paper provides a comprehensive study on types of threats and solutions on smart grid communication and metering infrastructures. As a part of this survey, the smart grid metering infrastructures susceptibilities and recommended remedial actions are identified. In addition, the paper details types of known attacks on existing metering infrastructure and defensive methodologies.**

Keywords—smart meter, advanced metering infrastructure (AMI), Intrusion detection;

I. Introduction

Smart Meters (SM) are significant components in Smart Grids (SG) that measure, gather and transmit information of the energy consumption at the distributed house-holds. Smart Metering System (SMS) along with the other smart devices in a household can act wisely in order to save power. Numerous literatures are being published describing a number of attacks against smart grid and its infra-structure [1], [2], [3], [4]. A group of researchers found that SMs used in Spanish Utilities have re-programmable memory chips and runs on flawed code. The only security level used in that SMs is symmetric AES-128 encryption scheme which is easy to break by brute-force-attack injecting malicious command. Once the Smart Meter is compromised, household power supply can be controlled by unauthorized persons, even that SM can be used as an entry point to launch attack against the power system by inserting "Network Worms"[5][6][7][8]. In 2012, an information security firm SecureState released an open-source frame work "Terminator" for security testing of SM. The Terminator program can communicate with the SMs having C12.19 communication protocol via ANSI type-2 optical probe with a serial interface [9]-[10]. In [11], authors report that a hacker was able to automatically detect and report the consumption information by SMs within short range of distance with an inexpensive RTL-SDR dongle. At the 28th Chaos Computing Congress hacker conference, German researchers were able to send incorrect energy data back to a utility company compromising the SMs [14]. Two hackers were able to hack the private keys of encrypted data in the onboard Firmware and using the meter's unique identifier were able to transmit spoof messages back to utility company [12]. Energy fraud taking the leverage of badly implemented encryption was demonstrated in Hack in Paris 2014 where in one case old packets was successfully re-injected into the network and in another case Smart Meter string ID was replaced with funny one "Hack in Paris" [13].

Communication based attacks are classified based on the type of communication channels and protocols the SMs use to communicate with the Home Area Network (HAN), Neighboring Area Network (NAN) and the SG. SMS can be breached through many entry points that may compromise data integrity and privacy [2]. The situation can be very dangerous, if the attacker gets access to the crypto key of all the smart meters of a utility by attacking the head-end and modifies the keys. At this point, attacker can interrupt the supply to thousands of consumers that can cause devastating effect on the livelihood, health, safety of people and business. A secured SMS should be able to do two things: 1) prevents most of the cyber/physical attack and 2) provide reasonable recovery/survivability mechanism. There are several motivations behind SM Attack [14]: 1) eavesdropping, 2) energy theft, 3) swanky attackers: The attacker may want to exhibit their ability or knowledge, 4) Active Attacker: Smart meter hacking may be part of larger blended terrorist attack on the whole power system, and 5) intrusive data management agencies. Attack on AMI can be mainly differentiated into two categories as attack on: 1) physical system and 2) communication system (see figure 1).

Several literatures have been published proposing different types of solutions to the security problems that have been discovered. In [15], the working process of Advanced Metering Infrastructure (AMI) has been discussed. The technical and governance considerations for SM usage in day to day life have been investigated in [1] dealing with variety of concerns such as technology, and security costs and benefits using SMs. A survey on cyber security concerning the smart grid infrastructure was published in [16].

This paper is organized as follows: section II explains about the possible physical attacks; section III explain multiple types of communication system attacks on the SMS. Section IV describes the SM security framework and section V provides the conclusion of the paper.

978-1-4799-8802-0/15/$31.00 ©2015 IEEE

II. Physical Attacks

Even though, researchers built several mechanisms and encryption systems to protect the data from the attackers, recent physical attack on the electrical sub-station (in California) raised an alarm on how existing physical systems are vulnerable [3]. According to Federal Energy Regulatory Commission (FERC), an attack on just 9 out of more than 55,000 transmission substations all over the United States would push the whole country into darkness [4]. This threat might look feasible only for the large scale plants, but it is equally important to protect individual devices in the SG, as any vulnerability can have a cascading effect on the entire power system. As Smart Meters (SMs) are the connecting point between the utilities and the customers, it is a vital component by monitoring and transmitting the electrical usage parameters. If these equipment are viable for tampering, it could lead to disasters as grid operators lack the most basic and essential information on the power consumption at the distribution level [17].

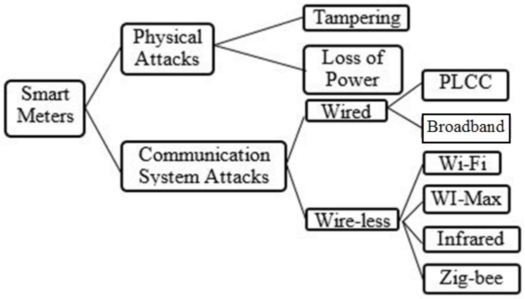

Figure 1. Classification of attacks on Smart Metering System

A. *Tampering*

Tampering of metering can be intentional and unintentional modification of the equipment in such a way that it affects the normal functioning of the equipment. A recent study indicates that an average of $2000 is spent on recovering the tempering [18]. Figure 2 shows the different types of physical attacks that can be applied onto the SMS. Tampering can be done in different ways. Some of them are as follows:

1. Physical damage to the SM.
2. Manipulation of data on a local memory chip on-board the SM where different data, i.e., password mechanisms, encryption algorithms, and authentication keys related to SM, are stored [19].
3. Access to communication link. An access to fiber communication system can result in the failure of the SMs to communicate with the grid operators which is the fundamental task of a SM.

Available solutions for Physical tampering

As discussed earlier about the possibilities of how some of the physical attacks can happen on the AMI, it is also required to have some solutions for the known problems. In [17], authors proposed a AMI Intrusion Detection System to detect theft-related behaviors. Figure 2 provides possible solutions to a list of potential problems in AMI.

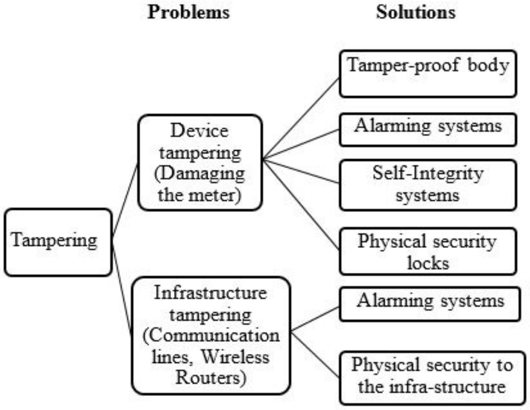
Problems
Solutions
Tampering
Device tampering (Damaging the meter)
Infrastructure tampering (Communication lines, Wireless Routers)
Tamper-proof body
Alarming systems
Self-Integrity systems
Physical security locks
Alarming systems
Physical security to the infra-structure

Figure 2. Classification of different types of physical attacks

The solutions to device and infrastructure tampering are as follows:

1. **Tamper-proof system:** The outer cover of meter should be durable and strong so that they can't be damaged. All manufacturers should make sure that their SMs are safe against the known adversaries[19].
2. **Alarm Systems:** All the SMs must be equipped with sensors (heat, pressure etc...) so that whenever any kind of attack takes place on SM, the sensors can trigger some kind of sound alarms, E-mail or SMS alerts to the system operators and also the consumers.
3. **Self-Integrity systems:** A SM should be designed in such a way that it should self-erase all the data that is stored on the device's local memory in parallel to sending SOS to the operators about the situation so that its integrity is protected [19].
4. **Physical locks:** All the SMs are to be physically locked so that they are not easily reachable other than the authorized personnel.
5. **Development cycle inspection:** The development cycle of firmware should be extremely security-focused with frequent walk-through and security assessment by third parties to identify any design and implementation flaw. It is possible to modify the firmware in the development cycle so that the SM can be compromised in later time. Even the firmware located in the flash memory can be reprogrammed by a skilled attacker having insider knowledge [3].

III. Communication System Attacks

SG refers to the conventional electrical power grid but with the capabilities of digital communications, controls, self-healing and decision making skills. There are a number of communication systems that are being utilized and can be utilized in future for connecting SMs. Some of them are wired communication systems while some are wireless systems. The references [20]-[21] surveyed the different types of communication systems and protocols available for SG and AMI. Based on this categorization of whether they are connected physically or not, methods of communication as divided as: 1) wired, and 2) wireless.

In the following sections, communication channels and corresponding attacking schemes which might be possible for specific communication channels are discussed.

A. Wired Communication Channels

"Wired" communication systems use physical links between different equipment providing channels of communication between them. Wired communication channels can be: 1) Power Line Carrier Communications (PLCC), and 2) Optical Fiber Communication (OFC)

1) Power Line Carrier Communication (PLCC)

PLCC can be defined as a technology which uses the already laid electrical conductors as a medium to transmit digital signals from one place to another assuming that both of the places are equipped with the corresponding technology [22][23].

Advantages of PLCC:

1. Supports Substation and Grid Control Functions (SCADA)
2. Communicates over power lines
3. Short/long distance transmission can be achieved with less interference

2) Optical Fiber Communication

The method of transmitting information through an optical fiber using light as a medium is called OFC.

Advantages of OFC:

1. It is almost impossible to tap a signal being sent on a fiber without physically cutting it because the fibers have no effect of electro-magnetic fields. Also, because of non-conductivity, cables are almost passive to any kinds of interferences [21].
2. High-band width and ease of installation

Attacks on SMs through PLCC:

Power lines are generally left exposed and they are not covered. Any attacker with portable equipment such as current transformer can extract information tapping high frequency waves. The other drawback in PLCC is that the information transmitted from SM is not encrypted. As the information is in plaintext format, once connected and isolated, information will be directly available for the attacker.

Available solutions:

1. Cryptography: All the SM manufacturers should implement privacy and integrity controls to protect SM data which needs to confidential [24].

Attacks on SMs through OFC:

1. In-band Jamming is the technique of using a high power transmitter to kill the signal on an OFC cable. It can perform different things such as degrade the strength of the signal or completely kill it.
2. Out-of-band Jamming is another kind of technique which exploits crosstalk in optical components. Any adversary who knows the optical amplifier bands can inject signals at different wavelengths but within the amplifier pass band. Thus, without detecting the attack, gain is provided to each signal which would corrupt the signal completely.
3. Using of Splitters and Couplers, one can tap into the system without actually breaking it.

Available Solutions:

1. Power Detection and Intrusion Detection Systems: Whenever a jamming attack happens, the power of the signal at the receiver would increase rather than getting attenuated; A threshold detector. Intrusion detection systems are generally available for data layer protection. But the little known fact is that there are systems which can offer some protection for physical layer taps too.

B. Wireless communication systems

Wireless communication networks are used with SMs to communicate between SM and control center and also between the SM and the devices serving under the smart meter. Types of wireless communication protocols are shown in figure 2. Table 1 describes the different types of wireless communication systems available, their advantages, disadvantages and available solutions for the concerned problems.

IV. SM SECURITY FRAMEWORK

A. Smart Meter Security Requirements

Unified system level security framework for SM needs a collaborative effort. All the stakeholders related to SM should work in unison and close collaboration to make system more secured. Stakeholders associated SM data can be categorized as 1) Customers 2) Grid Operators 3) Energy Providers 4) Billing Companies 5) Third party value added services 6) Government agencies [23]. Each stakeholder has its own security requirements. The sensitive objects that need protection in SMs are 1) Smart Meter Readings 2) Control Commands of SMs 3) Bill Information 4) Customer's personal information [14]. Based on these different stakeholder and sensitive objectives, the security requirements of SMs can be classified as: 1) confidentiality, 2) Integrity and Availability, and 3) Non-Repudiation.

1. Confidentiality

Confidentiality is considered a synonym to privacy that ensures that SM readings, and commands do not fall into the wrong hands. The only way that the utilities can increase the confidentiality of consumers on the usage of SMs is through addressing the privacy and security concerns. A few concerns have been addressed in [25]. A Privacy Preserving Metering and Aggregation (PPMA) system is one of the most important security concerns for SM. In [26], an approach on preserving the privacy of SM data with multiple data consumers is presented. A 15 minute sampling period for SM data collection is sufficient enough to predict what's happening in a household [27]. Privacy preserving issues may come from Automatic Appliance Control (AAC) or Demand Response (DR) domains [28]. Available PPMA techniques can be grouped as 1) battery, 2) Cryptographic Schemes 3) Anonymity and 4) Disturbance. The rechargeable battery based approach uses different algorithms to mask the appliance usage signature of the end

TABLE1. VULNERABILITIES AND SOLUTIONS TO TYPES OF WIRELESS COMMUNICATIONS TECHNOLOGIES

Technology	Advantage	Vulnerabilities	Available Solutions
Wi-Fi	Open Standard, High throughput Strong Home market penetration Low cost Relatively secure communication	Traffic Analysis, Passive and active eavesdropping, Man-in-the-middle attack, session hijacking, and replay attacks.	Two way authentication, encryption.
ZigBee [29]	high reliability, self-configuration and self-healing, Low power consumption, low cost	Jamming, Message capturing and tampering, Exhaustion	1. A utility gateway device between HAN and SM, authentication, encryption
Mobile Communications and Femtocells	Consistent coverage in office or home, less power consumption	Network and service availability disruption, Fraud and service theft, Privacy and confidentiality disruption	Two way authentication, encryption
WiMAX [21]	High data rate (1 Gbps for stationary users), Low latency, Advanced Quality of Service (QoS), Sophisticated security	Ranging Attack (DoS attack, downgrading attack, water torture attack), Power Saving Attack, man-in-the-middle attack, Replay theft of service attack, Traffic analysis techniques	Encryption, Intrusion detection schemes, access control to specific applications
Long Term Evolution (LTE)	Less Interference , Resource efficient [30]	Attacks on the air interface, Attacks on the e-NB, Attacks against the core network	Two way authentication, encryption, introduction of mobile virtual network operator (MVNO),

user. Researches related to PPMA with Cryptographic Schemes include homomorphic encryption, Secure Multiparty Communication (SMPC) [31], Attribute-Based Encryption (ABE) [28] in cryptographic domain. Anonymity is achieved by assigning pseudonymous identifier (ID) to the SM rather than its unique ID through trusted escrow service. The idea behind addition of disturbance in the SM reading to enhance its privacy lies on certain random disturbance.

The first work on PPMA was done by Garcia and Jacobs [32] where they used a combination of Paillier's additive homomorphic encryption on aggregated energy consumption data. Human factor aware PPMA was considered in [31], where the authors have proposed a basic scheme and an advance scheme to hide the human activity information from the aggregated meter readings. A dynamic Programming framework was adopted in [33] to mask the energy usage pattern through battery charging and discharging. An attribute-based encryption (ABE) key variant based on existing cryptographic primitives was suggested in [28] for the design and implementation of privacy preserving protocol. Confidentiality of SM data stored in cloud storage was studied in [34]. A privacy preserving range query (PaRQ) scheme was applied over the encrypted metering data so that only the authorized requester can request a query. Camenisch-Lysyanskaya (CL) signature based linkable anonymous credential protocol was constructed in [35] to provide privacy as well as the security properties of authentication and traceability of faulted SM. Taking the advantage of enhanced network coding technology, [36] looks into the problem of privacy considering the Cyber-Physical Systems (CPS) aspect where anonymity, un-linkability, un-detectability and un-observability of communications were addressed.

While designing privacy aware SM systems, computationally expensive cryptosystems should be avoided as there are limitations of bandwidth and computational capacity.

2. *Integrity and Availability*

Integrity and availability are intertwined in such a way that if one is compromised, the other will follow. The best way to defend integrity and availability in SM is lightweight strong encryption and authentication system. The key Management Schemes (KMS) which have been designed for IT systems are not suitable for use in SMS due to the reason [37] that SMS and AMI are heterogeneous networks having interconnected devices with different computation, storage and communication capability. In SMs, KMS must accommodate these imbalances along with the feature of high reliability and scalability. A Diffie-Hellman (DH) exchange based lightweight message authentication scheme was presented in [38] for the secure communication of the SMs which are distributed at different hierarchical network in Smart Grid communication framework. The authors in [39] proposed a novel KMS combining Needham-Schroeder authentication protocol based symmetric key technique and elliptic curve public key technique to eliminate the known threats including man-in-the-middle attack and the replay attack. However, it is shown in [40] that the KMS proposed in [39] is susceptible to man-in-the-middle attack. A key distribution protocol for Smart Grid network was introduced in [40] using trusted third party. In order to maintain confidentiality and integrity of messages exchanged between SMs and its stakeholders, a key management scheme based on Physically Un-clonable Function (PUF) technology was proposed in [41] for hardware based authentication of smart meters and efficient key management. Key graph based key management framework was constructed in [42] with three different key management process keeping in mind the storage and computational constraints of SMs. [37] identifies that the KMS proposed in [43] suffers from de-synchronization attack and lacks scalability due to inefficient key management. Combining the techniques of identity-based crypto-system and efficient key tree, a scalable key management (SKM) was proposed in [37].

3. *Non-Repudiation*

Non-Repudiation can be seen as a subset of authentication where the origin of data, command can be assured with high degree of probability. In [44], a mutual inspection strategy was presented to resolve this issue between SM and data aggregator though it does not consider the case of data communication between SM and home appliance. Both of these issues were addressed in [45], where two separate accountable communication protocols were used based on peer review strategy.

B. Smart Meter Intrusion Detection Scheme

Intrusion Detection Scheme (IDS) is the second line of defense against SM security threats after the deployed security mechanism fail to protect them. Depending on the detection criteria of intrusion in SM, two kinds of IDS can be designed. They are, specification based and anomaly based. [30] classifies IDS as Host based Intrusion Detection Systems (HIDS) and Network Based Intrusion Detection Systems (NIDS). In the context of SM, HIDS will provide protection in a certain SM or HAN and NIDS will provide protection for NAN or WAN. By embedding the temporal behavior of attacks in neural network, [46] proposed an IDS to maximize the detection rate of probe or reconnaissance attack which tries to steel information from a network. Anomaly in network traffic is a strong indication of network intrusion. Intense researches are going on in applying machine learning applications in IDS as they can provide useful information about compromised SMs. An unsupervised IDS was developed in [47] where network traffic datasets were automatically labeled. Then a Genetic Algorithm (GA) based approach was used to process those labeled traffic to generate the most appropriate intrusion detection results. [48] uses a particle swarm optimization technique (PSO) in IDS. SM data are collected by data aggregator where the data are stored in a database. Based on the matrix concept, malicious data transaction assessment in database was proposed in [49]. A cunning attack on SM may alter the network traffic in such a way that it may seem normal to data aggregator. Under this scenario, a collective anomaly detection procedure is required for IDS. If a SM is compromised, it's better to sandbox that SM so that the attack cannot spread beyond that not SM. A suite of inspection algorithm were proposed in [50] to explore the malicious meter inspection (MIM) problem. [14] Classifies energy theft detection schemes in three categories: classification based, state based and game theory based. Many vendor specific threat detection mechanisms are also in place to detect SM security threat. Network Compliance Manager (NCM) of Cisco can work throughout a multivendor network infrastructural to identify, manage and counter security threats by configuration management and software change [51]. HP ArcSight ESM has a fraud detection rule which looks for any unexpected reading or possible SM tempering [34].

V. Conclusion

As more and more utilities are adapting for Smart Meter technologies, security concerns are increasing exponentially day by day. The conventional security mechanisms for hardware, cyber space, and communication network are not adequate enough for SMS as they have additional set of constraints, such as limited memory and processing power, heterogeneous network architecture and physical exposure of the SM. The different aspects of security vulnerabilities of SM with its solutions, limitations, and future scopes are discussed in this paper. To effectively thwart attacks on SM, security solutions for SM should be designed considering the constraints associated with SMS and power system as these SMs are part broader smart grid infrastructure.

References

[1] W. Wang and Z. Lu, "Cyber security in the Smart Grid: Survey and challenges," Comput. Networks, vol. 57, no. 5, pp. 1344–1371, Apr. 2013.

[2] G. Kalogridis, M. Sooriyabandara, Z. Fan, and M. a. Mustafa, "Toward unified security and privacy protection for smart meter networks," IEEE Syst. J., vol. 8, no. 2, pp. 641–654, 2014.

[3] K. Tweed, "Attack on California Substation Fuels Grid Security Debate," IEEE spectrum, 2014. [Online]. Available: http://spectrum.ieee.org/energywise/energy/the-smarter-grid/attack-on-california-substation-fuels-grid-security-debate.

[4] K. Tweed, "Attack on Nine Substations Could Take Down U.S. Grid," IEEE spectrum, 2014. [Online]. Available: http://spectrum.ieee.org/energywise/energy/the-smarter-grid/attack-on-nine-substations-could-take-down-us-grid.

[5] "Spanish smart meters easy to hack - E & T Magazine." [Online]. Available: http://eandt.theiet.org/news/2014/oct/smart-meters-hacking-spain.cfm.

[6] https://plus.google.com/109505191482335442706/posts, "Hacking Smart Electricity Meters To Cut Power Bills."

[7] "Smart meters can be hacked to hit the National power network | Security Affairs." [Online]. Available: http://securityaffairs.co/wordpress/29353/security/smart-meters-hacking.html.

[8] "BBC News - Smart meters can be hacked to cut power bills." [Online]. Available: http://www.bbc.com/news/technology-29643276.

[9] "Smart meter hacking tool released | ZDNet." [Online]. Available: http://www.zdnet.com/smart-meter-hacking-tool-released-7000001338/.

[10] "Tools."[Online].Available: ttp://www.securestate.com/Research and Innovation/Pages/Tools_test.aspx.

[11] "Using SDR to Read Your Smart Meter | Hackaday." [Online]. Available: http://hackaday.com/2014/02/25/using-sdr-to-read-your-smart-meter/.

[12] "Kim Davis - The Future City Will Be Vulnerable | Future Cities." [Online]. Available: http://www.ubmfuturecities.com/author.asp?doc_id=526872.

[13] "Hack in Paris 2014 Wrap-Up Day #2 | /dev/random." [Online]. Available: http://blog.rootshell.be/2014/06/27/hack-in-paris-2014-wrap-up-day-2/.

[14] R. Jiang, R. Lu, Y. Wang, J. Luo, C. Shen, and X. S. Shen, "Energy-Theft Detection Issues for Advanced Metering Infrastructure in Smart Grid," Tsinghua Sci. Technol., vol. 19, no. 2, pp. 105–120, 2014.

[15] R. Rashed Mohassel, A. Fung, F. Mohammadi, and K. Raahemifar, "A survey on Advanced Metering Infrastructure," Int. J. Electr. Power Energy Syst., vol. 63, pp. 473–484, Dec. 2014.

[16] M. P. McHenry, "Technical and governance considerations for advanced metering infrastructure/smart meters: Technology, security, uncertainty, costs, benefits, and risks," Energy Policy, vol. 59, pp. 834–842, Aug. 2013.

[17] S. McLaughlin, B. Holbert, A. Fawaz, R. Berthier, and S. Zonouz, "A Multi-Sensor Energy Theft Detection Framework for Advanced Metering Infrastructures," IEEE J. Sel. Areas Commun., vol. 31, no. 7, pp. 1319–1330, Jul. 2013.

[18] "GE Multilin: Products - Meters." [Online]. Available: file:///C:/Users/Admin/AppData/Local/Temp/Rar$EX48.093/References/7. GE Multilin Products - Meters.htm.

[19] J. Alderson, "Advanced Metering Infrastrucre attack methodology," 2009.

[20] A. Mahmood, N. Javaid, and S. Razzaq, "A review of wireless communications for smart grid," Renew. Sustain. Energy Rev., vol. 41, pp. 248–260, Jan. 2015.

[21] D. Bian, M. Kuzlu, M. Pipattanasomporn, and S. Rahman, "Analysis of communication schemes for Advanced Metering Infrastructure (AMI)," in 2014 IEEE PES General Meeting | Conference & Exposition, 2014, pp. 1–5.

[22] "IEEE Guide for Power-Line Carrier Applications." p. 0_1–, 1981.

[23] Wenshu Zhang and Liuqing Yang, "SC-FDMA for uplink smart meter transmission over low voltage power lines," in 2011 IEEE International Symposium on Power Line Communications and Its Applications, 2011, pp. 497–502.

[24] A. Francillon and C. Castelluccia, "Code injection attacks on harvard-architecture devices," in Proceedings of the 15th ACM conference on Computer and communications security - CCS '08, 2008, p. 15.

[25] E. McKenna, I. Richardson, and M. Thomson, "Smart meter data: Balancing consumer privacy concerns with legitimate applications," Energy Policy, vol. 41, pp. 807–814, Feb. 2012.

[26] C. Rottondi, G. Verticale, and A. Capone, "Privacy-preserving smart metering with multiple data Consumers," Comput. Networks, vol. 57, no. 7, pp. 1699–1713, May 2013.

[27] "Smart Meter Data: Privacy and Cybersecurity: Brandon J Murrill: 9781490524993: Amazon.com: Books." [Online]. Available: http://www.amazon.com/Smart-Meter-Data-Privacy-Cybersecurity/dp/1490524991.

[28] D. Li, Z. Aung, J. Williams, and A. Sanchez, "P3: Privacy Preservation Protocol for Automatic Appliance Control Application in Smart Grid," IEEE Internet Things J., vol. 1, no. 5, pp. 414–429, Oct. 2014.

[29] N. C. Batista, R. Melício, and V. M. F. Mendes, "Layered Smart Grid architecture approach and field tests by ZigBee technology," Energy Convers. Manag., vol. 88, pp. 49–59, Dec. 2014.

[30] E. Yaacoub and A. Abu-Dayya, "Automatic meter reading in the smart grid using contention based random access over the free cellular spectrum," Comput. Networks, vol. 59, pp. 171–183, Feb. 2014.

[31] W. Jia, H. Zhu, Z. Cao, X. Dong, and C. Xiao, "Human-Factor-Aware Privacy-Preserving Aggregation in Smart Grid," IEEE Syst. J., vol. 8, no. 2, pp. 598–607, Jun. 2014.

[32] B. J. Flavio D. Garcia, "Privacy-Friendly Energy-Metering via Homomorphic Encryption," Secur. Trust Manag., vol. 6710, pp. 226–238, 2011.

[33] L. Yang, X. Chen, J. Zhang, and H. V. Poor, "Cost-Effective and Privacy-Preserving Energy Management for Smart Meters," IEEE Trans. Smart Grid, vol. 6, no. 1, pp. 486 – 495, 2014.

[34] M. Wen, R. Lu, K. Zhang, J. Lei, X. Liang, and X. Shen, "PaRQ: A Privacy-Preserving Range Query Scheme Over Encrypted Metering Data for Smart Grid," IEEE Trans. Emerg. Top. Comput., vol. 1, no. 1, pp. 178–191, Jun. 2013.

[35] F. Diao, F. Zhang, and X. Cheng, "A Privacy-Preserving Smart Metering Scheme Using Linkable Anonymous Credential," IEEE Trans. Smart Grid, vol. 6, no. 1, pp. 461–467, 2015.

[36] E. Topics and I. N. Computing, "Enhanced Network Coding to Maintain Privacy in Smart Grid Communication," IEEE Trans. Emerg. Top. Comput., vol. 1, no. 2, pp. 286–296, 2013.

[37] Z. Wan, G. Wang, Y. Yang, and S. Shi, "SKM□: Scalable Key Management for Advanced Metering Infrastructure in Smart Grids," IEEE Trans. Ind. Electron., vol. 61, no. 12, pp. 7055–7066, 2014.

[38] M. M. Fouda, Z. M. Fadlullah, and N. Kato, "A Lightweight Message Authentication Scheme for Smart Grid Communications," IEEE Trans. Smart Grid, vol. 2, no. 4, pp. 675–685, Dec. 2011.

[39] D. Wu and C. Zhou, "Fault-Tolerant and Scalable Key Management for Smart Grid," IEEE Trans. Smart Grid, vol. 2, no. 2, pp. 375–381, Jun. 2011.

[40] J. Xia and Y. Wang, "Secure Key Distribution for the Smart Grid," IEEE Trans. Smart Grid, vol. 3, no. 3, pp. 1437–1443, Sep. 2012.

[41] M. Nabeel, S. Kerr, and E. Bertino, "Authentication and key management for Advanced Metering Infrastructures utilizing physically unclonable functions," in 2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm), 2012, pp. 324–329.

[42] N. Liu, J. Chen, L. Zhu, J. Zhang, and Y. He, "A Key Management Scheme for Secure Communications of Advanced Metering Infrastructure in Smart Grid," IEEE Trans. Ind. Electron., vol. 60, no. 10, pp. 4746–4756, Oct. 2013.

[43] N. Liu, J. Chen, L. Zhu, J. Zhang, and Y. He, "A Key Management Scheme for Secure Communications of Advanced Metering Infrastructure in Smart Grid," IEEE Trans. Ind. Electron., vol. 60, no. 10, pp. 4746–4756, 2013.

[44] D. H.-C. Du, "Non-repudiation in neighborhood area networks for smart grid," IEEE Commun. Mag., vol. 51, no. 1, pp. 18–26, Jan. 2013.

[45] J. Liu, Y. Xiao, S. Member, and J. Gao, "Achieving Accountability in Smart Grid," IEEE Syst. J., vol. 8, no. 2, pp. 493–508, 2014.

[46] O. Al-Jarrah and A. Arafat, "Network Intrusion Detection System using attack behavior classification," in 2014 5th International Conference on Information and Communication Systems (ICICS), 2014, pp. 1–6.

[47] F. J. Aparicio-Navarro, K. G. Kyriakopoulos, and D. J. Parish, "Automatic Dataset Labelling and Feature Selection for Intrusion Detection Systems," in 2014 IEEE Military Communications Conference, 2014, pp. 46–51.

[48] N. Cleetus and D. K. A, "Multi-objective functions in particle swarm optimization for intrusion detection," in 2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2014, pp. 387–392.

[49] R. A. Haraty and M. Zbib, "A matrix-based damage assessment and recovery algorithm," in 2014 14th International Conference on Innovations for Community Services (I4CS), 2014, pp. 22–27.

[50] Z. Xiao, Y. Xiao, and D. H.-C. Du, "Exploring Malicious Meter Inspection in Neighborhood Area Smart Grids," IEEE Trans. Smart Grid, vol. 4, no. 1, pp. 214–226, Mar. 2013.

[51] "Grid Security - Industry Solutions." [Online]. Available: http://www.cisco.com/web/strategy/energy/smart_grid_security.html.