Cyber Security Considerations for Advanced Metering Infrastructure in Smart Grid

Tanvi Mehra, R. K. Pateriya

Abstract— Advanced Metering Infrastructure is a very critical part of Smart Grid that offers bidirectional information flow of vital power related information such as smart metering data and control messages across the entities to provide intelligent real time monitoring of the grid. However, AMI network is susceptible to many cyber vulnerabilities and attacks which could result in unreliable system performance causing false energy estimations or even completely destabilize the grid from its optimal running state. Consequently, proper attention is required towards its cyber security concerns. This paper attempts to provide an overview of AMI communication architecture and focuses on its cyber security requirements and constraints. We also discuss and review the current solutions and possible attack countermeasures.

Index Terms— Advanced Metering Infrastructure, Cyber security, Security requirements, Security challenges, Smart Grid, Smart meter, Wireless network

1 Introduction

THE Advanced Metering Infrastructure (AMI) is the most significant component for wired/wireless communication in Smart Grid. It facilitates the intelligent integration and communication to upgrade the existing electric power grid into smart grid [1].

The Smart Grid serves as a dynamic network for bidirectional energy flows by integrating green energy resources such as wind, tidal and solar energy to supplement centralized higher capacity power generators and incorporates real time communication architecture to control the comprehensive power management system in an automated and intelligent fashion [1], [2]. As illustrated by framework of smart grid in Fig. 1, the system comprises of seven fundamental tasks of bulk generation, transmission, distribution, operation, market, customer and service provider [1].

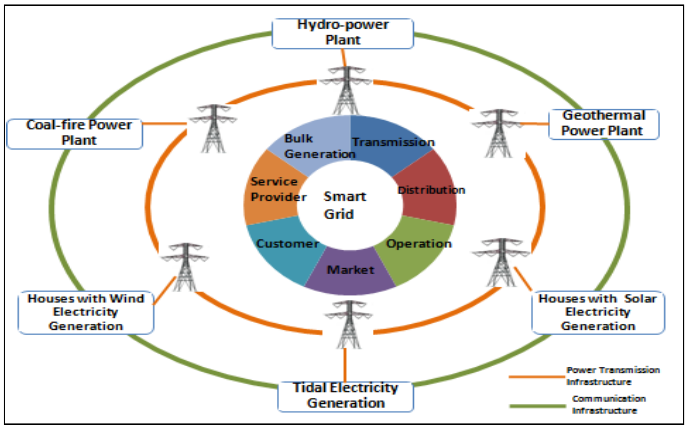

Hydro-power Plant
Coal-fire Power Plant
Geothermal Power Plant
Bulk Generation
Transmission
Distribution
Operation
Market
Customer
Service Provider
Smart Grid
Houses with Wind Electricity Generation
Houses with Solar Electricity Generation
Tidal Electricity Generation
Power Transmission Infrastructure
Communication Infrastructure

Figure 1. Sytem Overview of Smart Grid

The AMI aids to automate the production and distribution of electricity and also limits the power usage in order to enhance the efficiency, reliability and sustainability of the power grid. It comprises of advanced meters (i.e., smart meters) that performs various tasks further than recording power usage. The smart meters collect and analyze the information of energy consumption and demand data from home appliances, communicate and control for optimization of energy management, power quality etc. [1], [3].

AMI establishing a real time two-way communication link between power utility and appliances consuming electricity through a network of smart meters involves a high risk of exploiting this communication architecture for cyber attacks. It has been reported that one of the biggest challenges facing the smart grid development is related to the cyber security of systems [4]. The key demand for the successful deployments of smart grid is the defense against the cyber vulnerabilities and attacks. This paper provides an insight to the security requirements and challenges associated with the AMI in smart grid and the possible counter measures to address them.

The content of the paper is organized as follows. Section 2 provides a background of Advanced Metering Infrastructure. Section 3 explains the AMI communication architecture. Section 4 describes the cyber security concerns of AMI, highlighting the security requirements, constraints and potential countermeasures to deal with security threats. In Section 5, the literature review on the subject is presented and the conclusion is provided in Section 6.

2 Background

Advanced Metering Infrastructure is a conglomeration of systems and networks that records, stores and communicates the energy usage data and provides a suitable link between the end users and electric power utility.

The Advanced Metering Infrastructure is an upgrade of Advanced Meter Reading (AMR) system. In the beginning, AMR systems were introduced in Smart Grid to provide accurate meter reading data and to reduce the overall costs. The AMR systems are mostly confined to data collection process with one-way transmission functions and do not support two-way

- *Tanvi Mehra is currently pursuing masters degree program in Computer Science & Engineering in Maulana Azad National Institute of Technology, Bhopal, India. E-mail: tanvi.mh@gmail.com*
- *R. K. Patreiya is Associate Professor in Deptt. of CSE, Maulana Azad National Institute of Technology, Bhopal, India. E-mail: pateritark@gmail.com*

data interactions [5].

Fig. 2 shows the architecture of traditional AMR system connecting Remote Management centre, concentrator, collection terminals, power meters and other instruments in a tree network topology through three layers of communication network [5].

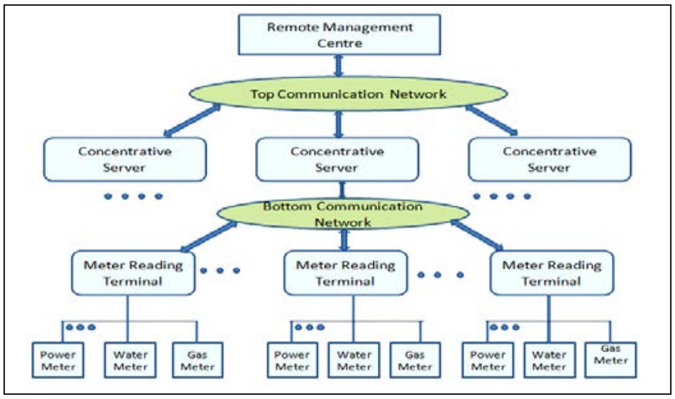
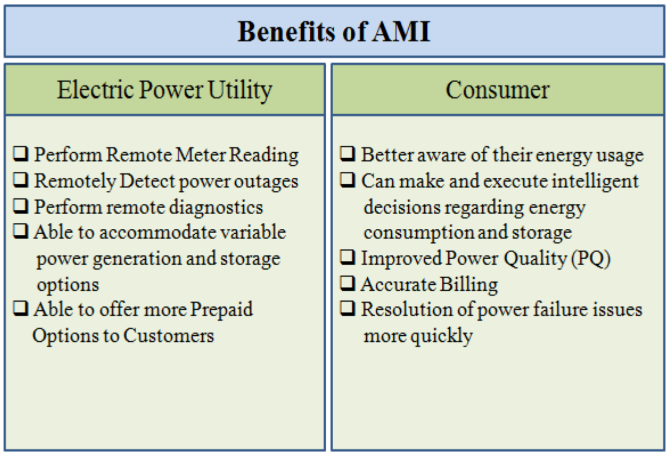


Fig. 2. Network Architecture of traditional AMR system

Advanced Metering Infrastructure uses AMR systems to collect the metering data from end users and provides additional functionality to implement demand response system by facilitating bidirectional communication capability. The increase in understanding of the advantages of integrating two-way information flow between the utility data centre, consumers and their residential loads has directed the evolution of AMI [6].

The AMI aids two fold benefits to the system operators and end users together. The Fig. 3 gives an insight of the advantages provided by the AMI to the customer and the utilities [8], [9].



Benefits of AMI

Electric Power Utility	Consumer
❑ Perform Remote Meter Reading ❑ Remotely Detect power outages ❑ Perform remote diagnostics ❑ Able to accommodate variable power generation and storage options ❑ Able to offer more Prepaid Options to Customers	❑ Better aware of their energy usage ❑ Can make and execute intelligent decisions regarding energy consumption and storage ❑ Improved Power Quality (PQ) ❑ Accurate Billing ❑ Resolution of power failure issues more quickly

Fig. 3. Network Architecture of traditional AMR system

3 SMART GRID AMI COMMUNICATION ARCHITECTURE

Fig. 4 shows a commonly used AMI communication architecture in smart grid, which is generalized from the literature [10], [11], [12], [13].

In Smart Grid, the electric power is delivered to consumers through two components viz., the transmission substations (TS) and a number of distribution substations (DS). The AMI communication architecture is introduced in the lower distribution network, (i.e. from the distribution substation placed in different regions) connecting the entities of Smart Grid together through different network technologies.

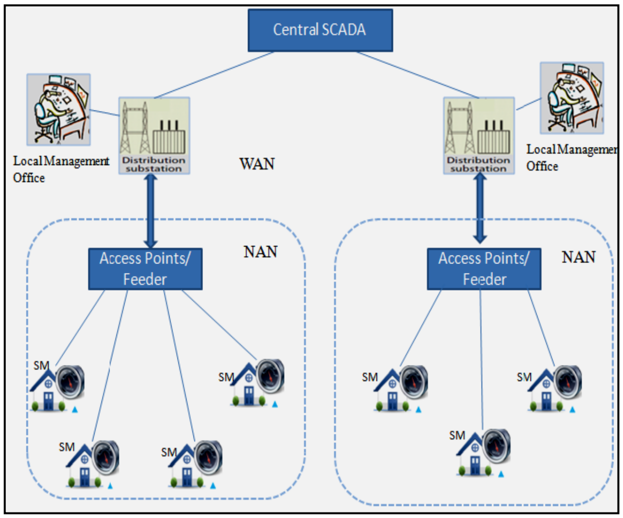


Fig. 4. Smart Grid AMI Communication System Architecture

The Advanced Metering Infrastructure comprises following components [12]:

- **Smart Meter:** The smart meter collects and sends the meter reading data periodically to the control centre and thus monitors and optimize the power consumption. A smart meter itself consists of three main components viz., a meter to record the energy generated or consumed, a computer to process and log the data, and a modem to connect to the network.
- **Gateway/Access Points:** It acts as an interface between the smart meter and the control centre. It forwards the control commands and meter reading data disseminated by the control centre and smart meters respectively.
- **Control Centre:** It receives the real time metering information from the network, performs the data storage and processing to generate the control commands to monitor and regulate the smart power generation, transmission and distribution throughout the grid.
- **Communication Architecture:** It facilitates the bidirec communication path among the entities of AMI for disseminating the metering and management messages.

Due to its importance, AMI is gaining more and more attention towards the communication mechanisms to be deployed. The communication infrastructure of AMI is an amalgamation of different network technologies including both wireline as well as wireless mechanisms. Wired technologies for the AMI network include Ethernet, Power Line Communications (PLC) or Data over Cable Service Interface Specification (DOCSIS) as preferred choices. Whereas, Worldwide Interoperability or Microwave Access (WiMAX), Bluetooth, 802.11s and cellular standards, such as 3G, 4G, and LTE are the promising wireless technologies.

We have considered each base station to be deployed for a specific service area, communicating with the smart meters in its realm. As shown in the Fig. 4 the AMI communication network is divided into a number of hierarchical networks classified according to the geographical domains and features:

- **Wide Area Network (WAN):** It provides the connectivity among WAN base station, its local management office, Central SCADA system and Access Point/feeder acting as a NAN Gateway. The WAN uses mostly wired communication such as fiber optical technologies or wireless broadband such as WiMax technologies as a backbone network to provide long range, high speed data and bulk delivery across domains [13].
- **Neighborhood Area Network (NAN):** NAN facilitates communication between Access Point/feeder and smart meters which play the role of HAN gateway. This network covers a few hundreds of nodes in its premises. This network is implemented using wireless communication technologies such as cellular systems, multihop wireless networks due to its advantages of low cost, reduced complexity and providing access extension without requiring cables to accommodate data pipeline.
- **Home Area Network (HAN):** The network connects all the intelligent home appliances with the smart meter to monitor and optimize their power consumption. In Fig. 4, a HAN network is simply represented by a smart meter node associated with each terminal consumer. The HAN requires short range, typically low bandwidth network. The most prominent network technologies include Bluetooth, IEEE 802.11(WiFi), ultra wideband (UWB), 802.15.4 ZigBee and 6LoWPAN [8].

The smart meters located at the customer’s premises send the meter reading data to the Local management office associated with each DS via Access Points or Feeders serving as a gateway or forwarding station. The Access points/feeders also work the other way round i.e., it communicates the control commands or management messages from the base station to the smart meters to optimize the power consumption of all intelligent home appliances. The local management office serves as a computer centre to its associated DS. The meter readings of each consumer is collected at the local management office and aggregated to further transmit them to the Central SCADA system for data processing, storage and demand analysis to optimize the power generation and distribution.

4 CYBER SECURITY OF AMI

The cyber vulnerabilities associated with the AMI places a direct consequence on reliable and efficient operation of smart grid. There is a diverse range of motivations to target an attack on the electric grid with intensions varying from economic gains (for e.g., minimizing electricity bills), to pranks (for e.g., reset meters) to disruption of the grid by criminals or even terrorists [14].

According to the Electric Power Research Institute (EPRI) report [4], “Cyber security is a critical issue due to the increasing potential of cyber attacks and incidents against this critical sector as it becomes more and more interconnected. Cyber security must address not only deliberate attacks, such as from disgruntled employees, industrial espionage, and terrorists, but inadvertent compromises of the information infrastructure due to user errors, equipment failures, and natural disasters. Vulnerabilities might allow an attacker to penetrate a network, gain access to control software, and alter load conditions to destabilize the grid in unpredictable ways.”

4.1 AMI Security Requirements

The following description addresses some of the important security requirements of AMI communication network.

4.1.1 Confidentiality

Confidentiality refers to the ability of preventing access to sensitive data (e.g., smart meter data) from unauthorized users. It is related to maintaining privacy or keeping data secret from being disclosed to illegitimate parties [17].

In the context of data security of AMI, the privacy of smart meter data is more important than that of the pricing information as it contains the consumption and other energy related information of individual appliances in consumer premises and can expose the consumer habits and behavior [14]. Also, the AMI network must ensure the confidentiality of messages being transmitted to the smart meters or the utility control centre through the network from being disclosed to unauthorized or malicious parties.

4.1.2 Integrity

Integrity is the ability of smart grid components to ensure that the information is not modified in transit by any unauthorized person or system. It relates to maintaining the accuracy and consistency of messages being transmitted.

Ensuring integrity means guarding the information from ‘undetected’ modifications whether in transit or by accidental errors or deliberate modifications by disgruntled employees at AMI headend or control centre. The data in AMI network can be attacked for integrity by false data injection attack [27], message replay or message delay [18].

Further, with respect to the messages in AMI, the integrity of price information is more significant than metering data as for example, if an attacker modifies the informed price to be negative; it may result in a sudden increase in power demand which may destabilize the whole electric power grid.

4.1.3 Availability

The availability of the system components and the information being shared is critical for the smooth functionality of smart grid. It refers to the ability of authorized participants to obtain access to certain resources (e.g., electricity service) whenever required [17].

Since the AMI data is the most crucial part of smart grid [19] for the efficiency, sustainability and reliability of the system, thus places a high demand on its availability. In the context of system components, the unavailability of gateways involves serious impact on the stability of the smart grid. For instance, if the access to key gateways is lost, then the customers would be unable to get the pricing signals or the control commands that may even destabilize power grid operations.

4.1.4 Authentication

The authentication is the ability to ensure the participating entities in the communication are whom they claim to be. It involves the verification of validity or identity of data and the system entities (for e.g., service subscriber) [14]. Data authentication is essential to prevent the illegitimate nodes to gain access to the AMI communication network. Also, to perform the managerial responsibilities such as network reprogramming, it is mandatory to verify the authenticity of the respective entity.

4.1.5 Authorization

Authorization is the process of specifying the right to certain actions (for e.g., subscribing to a particular service or accessing the meter readings) [17]. It is concerned with the access control e.g., right to generate control command for power plant control system. After the entity has successfully been identified and authenticated, the next step is to verify its information or resource access and privilege to execute actions. Broadly speaking, it discriminates a legitimate user from an illegitimate one [18].

4.1.6 Non- repudiation

Non-repudiation refers to the ability to prevent a user who carried out a particular action (such as transmission of a message or subscribing to a value added service) from denying what he/she has done [16]. Thus, it provides an undeniable proof of the integrity and origin of data.

In the context of AMI, non-repudiation is an important requirement for every aspect including metering data accountability, pricing data and management messages at gateways and utility control centre [14]. The AMI network should also account for any repudiation of information delivered through it.

4.2 AMI Security Constraints

To develop a security solution for Advanced Metering Infrastructure, a number of security constraints must be taken into account. The constraints influencing the design of a security framework for AMI are discussed below:

- The gateways and smart meters are susceptible to threats owing to their physical locations as well as software and network attacks. Further, the control centre, though placed in a protected environment, is prone to compromises by discontented employees who have scrupulous acquaintances to cause undetected harms to the system.
- As AMI comprises a variety of network modules, each having its unique features, communication mechanisms and limitations. Therefore, the security technology emphasizes a layered cyber security architecture providing a complete range of solutions that complies with differing needs of respective network domains.
- The entities in smart grid AMI system are a blend of devices from numerous commercial and network providers. It requires a lot of efforts to model a standardized security framework that accompanies with agreements across different vendors and legacy systems [16].
- The devices and networks in AMI communication system have their own capabilities in terms of storage, processing, bandwidth and throughput. The security solutions for the AMI communication system must ensure lower cryptographic overheads and should reduce the computation cost. Thus, the verification methodologies should be light weight and their computation must be affordable to the traffic density.

4.3. Countermeasures

In this section, we identify the potential countermeasures to deal with the security threats and attacks.

4.3.1 Key Management

Key management is a basic mechanism for providing data communication security. To ensure the privacy and authenticity, the secret keys or authentic public keys can be established prior to the communication process [14].

The key management system for AMI should address the scalability issue of large scale communication network across domains of smart grid. It should also ensure flexibility to support hybrid transmission modes including unicast, multicast and broadcast with proper key management operations such as key generation, key refresh, key recovery etc. and also considering the capability of smart grid devices [14], [20]. Nian, Lin and Yanling [20] propose a key management framework to deal with these challenges. The NIST documents report [21] specifies the issues with key management system and provides the guidelines for its design considerations.

4.3.2 Secure Routing Protocols

The diverse interconnected AMI communication network with numerous entities places new challenges to the network layer of communication protocol stack for its routing aspect [19].

The attacks on routing protocols may disrupt the complete logical connectivity among the smart grid entities. The security protocols must be designed considering the requirements of different modules of AMI communication network such as HAN, NAN and WAN serving numerous applications of smart grid. Thus a secured framework for routing protocols presents a promising solution for the security of the AMI communication system.

4.3.3 Secure Data Aggregation

The data aggregation presents one possible solution to address the constraints of low processing and storage capability of AMI system components and low bandwidth capacity of AMI wireless networks module. It takes the advantage of small sized packets traversing from smart meter nodes to the control centre via tree network topology.

Aggregation can be performed using a number of potential techniques such as concatenating several packets under a common header or applying an aggregation function like sum, average etc. [19]. Hence it reduces the transmission overheads by eliminating the identical header information. While carrying out secure data aggregation, the protection for confidentiality of aggregated packets must be taken into account as they contain a large volume of sensitive information [18]. Bartoli et al. proposed a lossless aggregation protocol [22] for AMI communication system while maintaining both per hop as well as end to end security.

4.3.4 Secure Network Architecture

For the successful evolution of smart grid, secure and reliable communication architecture plays the most crucial role. Moreover, the AMI network involves the transmission of real-time power related information for the management of complex power system which requires on-time and accurate message delivery.

A secure network architecture design must emphasize on providing reliable end-to-end communication, strong network topology, secure forwarding, and Denial of Service (DoS) and jamming defense to alleviate attacks and attain high availability [14].Wenye and Zhuo in [17] provides a review on two proposed secure network architectures that includes Trust Computing based architecture [24], [25] and Role based network architecture.

Thus, it has been observed that any single security scheme cannot address the entire security issues of AMI and also being cost-effective at same time. Table 1 lists some basic security properties for smart grid AMI network and other general cryptographic mechanism followed to prevent the attacks on them [17].

TABLE 1: CYBER SECURITY PROPERTIES AND APPROACHES IN AMI

Security Property	Commonly used to cryptographic mechanism to prevent the attack
Confidentiality	Encryption and Decryption
Integrity	Hash Function
Authentication	Passwords or involving a certification agent(CA)
Authorization	Either identity-based(access control list) or token –based(capability based authorization)
Non-Repudiation	Digital signature

5 REATED WORK

The NIST SGIP, in particular NIST IR 7628 and the AMI Security Task Force of the UCA International Users Group (UCAIug), are providing "best practice" guidelines for securing future AMI systems [26]. Some of the possible solutions for the security of AMI communication architecture proposed by different authors are as follows:

- In [11], Robin Berthier et al. use detection as a complete approach to develop a comprehensive monitoring solution through a detailed study of different threats targeting an Advanced Metering Infrastructure. They emphasize on the fact that continuous monitoring is required to maintain the security of the system. Their study aims at understanding the issues relating to threat models of AMI, components to be monitored constraints and monitoring architecture to be deployed. The authors consider specification-based approach as the most promising detection technology among others. They propose hybrid architecture for integrating an Intrusion Detection System in AMI architecture that comprises of isolated sensor nodes to monitor and report malicious incidents, and access points are required to host additional data processing capability to store core specification based detection technology and to aggregate decentralized alerts.
- In [22], Hernandez-Serrano Juan et al. proposed a security-communication trade-off for Smart Grid AMI by proposing a secure lossless aggregation protocol facilitating per-hop as well as end-to-end security and which is also energy efficient. In their work, the end-to-end security is achieved by attaching a packet with a header containing security control information and data being encrypted with secret key shared with the gateway. To provide per hop security, the use of timestamps & MIC is done at PHY/MAC layer. The evidences provided in the work, suggest the use of this possible solution when the noise in the network is not high.
- Another work by Ye Yan, Yi Qian and Hamid Sharif [23] proposed a secure and reliable innetwork collaborative scheme for smart grid AMI communications in which the authors aim to provide trust services, data privacy and integrity by the use of authentication and encryption keys established prior to data communication between the nodes in AMI communication system. Their method prevents potential cyber attacks and unauthorized network access by employing remote authentication key shared with remote authentication server placed at local management office and a mutual authentication key shared with neighboring smart meter in secure AMI communication network for data encryption to ensure data privacy of smart meter reading and management messages.

  However to avoid the wireless interferences with the increases in number of hops, the method in [23] requires the participating nodes' transmission to be scheduled in a pre-defined order which is determined when a smart meter node joins the communication network. Thus the nodes are highly interdependent on each other for ensuring proper data privacy and to lower the end to end delay.

6 CONCLUSION

The Advanced Metering Infrastructure is the heart of smart grid which facilitates the communication path all the way from the appliances consuming electric power at the end user premises to the electric utility control centre through its different network domains viz., HAN, NAN and WAN. The operational efficiency and reliability of Smart Grid relies on the security and reliability of AMI system.

The architecture of Advanced Metering Infrastructure requires an integral security framework for smooth and reliable functioning of smart grid and to mitigate the cyber vulnerabilities. Such security technology demands a comprehensive solution considering the security aspect of every entity such as device, data and network architecture involved in the infrastructure. In this paper, we described the background and communication architecture of AMI and discussed the concerned security requirements. After summarizing the security constraints of AMI, we have also identified the possible countermeasures and reviewed the related work in this field.

REFERENCES

[1] W. Wang, Y. Xu and M. Khanna “A survey on the communication architectures in smart grid” Elsevier’s Computer Networks Journal, vol.55, issue 15, pp 3604-3629, Oct 2011, http://dx.doi.org/10.1016/j.comnet.2011.07.010

[2] M . Kolhe, “Smart Grid: Charting a New Energy Future: Research Development and Demonstration”, The Electricity Journal, vol. 25, issue 2, pp. 88-93, 2012, doi: : 10.1016/j.tej.2012.01.018.

[3] D.Niyato and P. Wang “Cooperative Transmission for Meter Data Collection in Smart Grid”, IEEE Communications Magazine, vol. 50, issue 4, pp 90-95, April 2012, doi: 10.1109/MCOM.2012.6178839

[4] Report to NIST on Smart Grid Interoperability Standards Roadmap EPRI, Jun. 17, 2009 [Online]. Available: http://www.nist.gov/smartgrid/InterimSmartGridRoadmapNISTRestructure.pdf

[5] L.Li, H.Xiaoguang, H. Jian and H. Ketai, “Design of new architecture of AMR system in Smart Grid” , IEEE Conference on Industrial Electronics and Applications , 2011, doi: 10.1109/ICIEA.2011.5975925

[6] NETL Modern Grig strategy Powering our21st-Century Economy, “Advanced Metering Infrastructure” Feb 2008 [Online]. Available:http://www.netl.doe.gov/smartgrid/referenceshelf/whitepapers/AMI%20White%20paper%20final%20021108%20(2)%20APPROVED_2008_02_12.pdf

[7] A. Hahn and M. Govindarasu, “Cyber Attack Exposure Evaluation Framework for the Smart Grid”, IEEE Transactions on Smart Grid, vol. 2 , issue 4, Dec 2011, 10.1109/TSG.2011.2163829

[8] Z. Md. Fadlullah, A. Takeuchi, N. Iwasaki, Y. Nozaki “Toward Intelligent Machine-to Machine Communications in Smart Grid”, IEEE Communications Magazine, vol. 49, issue 4, pp 60-65, April 2011, doi: 10.1109/MCOM.2011.5741147

[9] D. Niyato, L. Xiao, P. Wang “Machine-to-Machine Communications for Home Energy Management System in Smart Grid", IEEE Communications Magazine , vol. 49, issue 4, pp53-59, April 2011

[10] F. Li, W. Qiao , H. Sun, H. Wan, J. Wang, Y. Xia, Z. Xu, P. Zhang: “Smart Transmission Grid: Vision and Framework”, IEEE Transactions on Smart Grid, vol. 1, issue 2, pp 168-177, Sept 2010, doi: 10.1109/TSG.2010.2053726

[11] R. Berthier, W. H. Sanders, H. Khurana “Intrusion Detection for Advanced Metering Infrastructures: Requirements and Architectural Directions” in proceedings of First IEEE International Conference on Smart Grid Communications, pp 350-355, Oct 2010, doi: 10.1109/SMARTGRID.2010.5622068

[12] Y. Yan, Y. Qian, H. Sharif, David Tipper “A Survey on Cyber Security for Smart Grid Communications”, IEEE Communications Surveys & Tutorials, vol. 14, issue 4, pp 998-1010, Fourth Quarter 2012, doi: : 10.1109/SURV.2012.010912.00035

[13] S. Kaplantzis and Y. A. Sekercioglu “ Security and smart metering”, 18th European Wireless Conference, April 2012

[14] A.R. Metke and R.L. Ekl “Security Technology for Smart Grid Networks”, IEE Transaction on Smart Grid, vol 1, issue 1, pp99-107, June 2010

[15] Y. Mo, T.H. Kim, K. Brancik, D. Dickinson, H.Lee A. Perrig and B. Sinopli, “Cyber–Physical Security of a Smart Grid Infrastructure”, Proceedings of the IEEE, vol.100, issue 1, Jan 2012, doi: 10.1109/JPROC.2011.2165269

[16] F.M. Cleveland, “Cyber security issues for Advanced Metering Infrastructure (AMI)” IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, 2008, doi: 10.1109/PES.2008.4596535

[17] W. Wang, Z. Lu “Cyber security in the Smart Grid: Survey and challenges”, Elsevier’s Computer Networks Journal, vol. 57, issue 5, pp 1344-1371, April 2013, http://dx.doi.org/10.1016/j.comnet.2012.12.017

[18] D. He, C. Chen, J. Bu, S. Chan, Y. Zhang and M. Guizani “Secure Service Provision in Smart Grid Communications”, IEEE Communications Magazine, vol. 50, issue 8, pp53-61, August 2012, doi: 10.1109/MCOM.2012.6257527

[19] N. Saputro ,K. Akkaya and S. Uludag “A survey of routing protocols for smart grid communications”, Elsevier’s Computer Networks Journal, vol.56, issue 11,pp 2742–2771, July 2012

[20] S. Das, Y. Ohba, M. Kanda and D. Famolari, “A key management framework for AMI networks in smart grid”, IEEE Communications Magazine, vol. 50, issue, pp 30-37, Aug 2012, doi: 10.1109/MCOM.2012.6257524

[21] NIST, Smart grid cyber security strategy and requirements. Aug. 2010.[Online]. Available:http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf

[22] A. Bartoli, J. Hernandez-Serrano, M. Soriano, M. Dohler, A. Kountouris, D. Barthel “Secure Lossless Aggregation for Smart Grid M2M Networks”, First IEEE International conference on Smart Grid Communications, pp 333-338, Oct 2010, doi: 10.1109/SMARTGRID.2010.5622063

[23] Ye Yan, Yi Qian, H. Sharif “A Secure and Reliable In-network Collaborative Communication Scheme for Advanced Metering Infrastructure in Smart Grid”, IEEE Wireless Communications and Networking Conference (WCNC), pp 909-914, March 2011, doi: 10.1109/WCNC.2011.5779257

[24] N. Kuntze, C. Rudolph, M. Cupelli, J. Liu and A. Monti, “Trust infrastructures for future energy networks”, IEEE Power and Energy Society General Meeting (PES ’10), July 2010, doi: 10.1109/PES.2010.5589609

[25] P. McDaniel, S. McLaughlin, “Security and privacy challenges in the smart grid”, IEEE Security and Privacy, pp 75–77, May-June2009, doi: 10.1109/MSP.2009.76

[26] D.E. Nordell “Terms of Protection”, IEEE Power and Energy Magazine, vol. 10, issue 1, Feb 2011, doi: 10.1109/TKDE.2007.190746.

[27] Y. Liu, P. Ning, and M. Reiter, “False data injection attacks against state estimation in electric power grids,” ACM Conference on Computer and Communications, doi: 10.1145/1653662.1653666