Cyber Security for Smart Grid – The Backbone of Social Economy

Vandana Rohokale[1] and Ramjee Prasad[2]

[1]*SKN Sinhgad Institute of Technology and Sciences (SKNSITS), Lonavala, Maharashtra, India*
[2]*Center for TeleInFrastruktur, Aalborg University, Aalborg, Denmark*
Email: vmr.301075@gmail.com; prasad@es.aau.dk

Received 15 January 2016; Accepted 25 January 2016;
Publication 13 August 2016

Abstract

Ever-growing population of people and new electronic gadgets demand huge electricity. Existing power grids mostly use non-renewable energy sources for electricity generation which is unidirectional energy flow. Aging equipments and manual meter reading, power line failure detection and power quality measurements result in lot of power losses and delays. Smart Grid assures modern, computerized and automated electricity power generation, distribution and management. It also ensures energy efficiency with quality improvement and reliability. But since it involves some kind of wired and wireless communication, there are the chances of enormous vulnerabilities. Electricity theft, authentication, authorization, trust ranking, distributed denial of service attack, man in the middle attack are the real challenges for smart grid. Cyber Security should ensure security for smart grid system with appropriate levels of trust, privacy and security. This paper puts forth the security challenges for smart grid and discusses about possible security solutions.

Keywords: Cyber Security, Smart Grid, Power Grid, etc.

Journal of Cyber Security, Vol. 5, 55–76.
doi: 10.13052/jcsm2245-1439.514

1 Traditional Electricity Power Grid

Today's electric power grid system is working with traditional equipments and is using conventional techniques for power generation, transmission, distribution, and consumption. For electricity power generation large scale power plants are used which are mainly running with non-renewable energy sources like gas, oil, coal, nuclear, hydro plants, etc. The power generation plants using coal, oil and nuclear emit hazardous gases which adds to the pollution levels to the environments. These power plants are based on the centralized approach. These power plants are usually located far away from the residential zones due to the danger of hazards. These conventional power generation mechanisms are lacking in the scalability, due to which there are limitations on the connections to be provided. Also, it does not involve the use of cooperation strategies.

For power transmission lines, there is least priority for the special requests made on telephone because it is difficult for the traditional electricity system to reroute the power to other territorial zones. On the distribution front, the present power grid has very much limited monitoring and control resources because of manual operations. Due to the sluggish local monitoring and control mechanisms, the whole system has become less efficient. Present metering infrastructure contains old meters which do not facilitate any communications with the central entities. Also, it involves manual meter readings which have lot of system flaws. On the power consumption side, the load adjustment is done manually which contains delays and inefficiencies. The important tasks such as power quality management, power failure searches, and power supply restoration are to be performed manually. This results in low data rate communication system which is prone to vulnerabilities and various attacks. Traditional electricity power grid system is depicted in Figure 1(a). Power flow in the conventional system is unidirectional from power generation plans to the consumers. The old equipments and power line infrastructure is prone to the additional power losses. It ultimately affects the overall power quality and availability of the electricity power in the emergency situations [1].

2 Smart Grid

Smart Grid has come up with the combination of the renewable energy sources like solar and wind energy with the conventional non-renewable energy sources such as coal, oil, gas, nuclear and hydro power generation plants. Smart grid encourages the extended penetration of small scale power

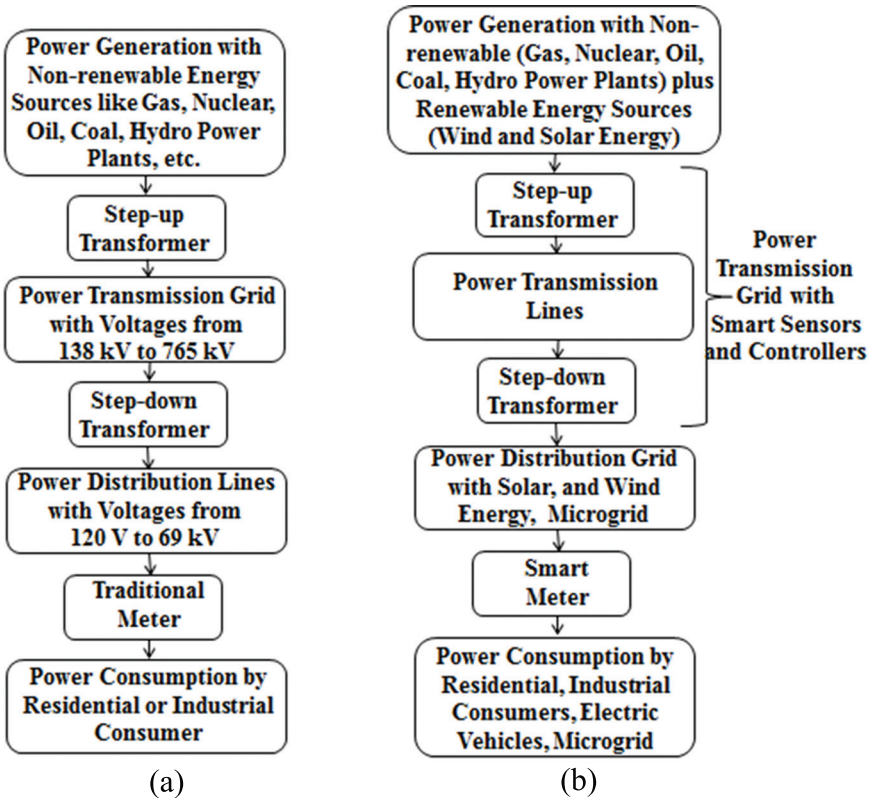

Figure 1 (a) Traditional electricity power grid system, (b) Smart grid system.

generation plants. The whole structure of electricity power generation is highly distributed in nature. Consumer centric approach is introduced with the smart grid that ensures the small scale power generation power plants to be located close to the consumers. Smart grid also ensures reduction in greenhouse gases with major usage of renewable energy sources. Each and every entity of smart grid is to be controlled and connected with the data communication networks. The emergency electricity routing requests can be submitted through the broadband connections. With the use of intelligent software, such electricity reroute requests can be handled automatically. Also power flow can be balanced appropriately with the computerized smart grid with great ease.

Demand and supply ratios can be well-adjusted with the automation in smart grid. Grid status and power quality knowledge can be maintained

and updated. Manual control and monitoring gets replaced with modern and automated systems for fault location searching, isolation provision and broken service restoration. Traditional unidirectional meters are replaced with bidirectional communication facilitating smart meters which can help in optimized monitoring and control of overall system from generation, transmission to distribution. Automated meter reading with the wireless communication aids is possible. It results into overall cost reduction with energy efficiency. Smart sensors and controllers with advanced and high speed communication infrastructure will surely maintain the optimized and uninterrupted power flow from generation to consumption sites [1]. Heterogeneous nature and self-healing capabilities of smart grid is going to be a great revolution for mankind. As illustrated in Figure 1(b), smart grid assures more automated, flexible and cost effective electricity flow from generation plants to consumer utilities. Consumer is facilitated to store the electricity when the costs are less and make use of it later or sell when the costs are relatively more. This kind of duplex service was lacking in traditional power grids. Smart Grid is a perfect blend of non-renewable energy sources with renewable energy sources for power generation, transmission, distribution with various modern data communication networks.

3 Security Threats to Smart Grid

Emerging Smart Grid is nothing but the intelligent and interconnected version of electricity power distribution network. Main goals of Smart Grid are to improve quality, efficiency and reliability in the generation and distribution of electricity, to support green information and communication technology (ICT) by reducing pollution effect through power grid, and to facilitate consumers to optimize their energy consumption. Various possible attacks at each stage of Smart Grid are depicted in Figure 2. Corresponding to the necessary security goals, three high level security objectives are taken into consideration such as availability, integrity and confidentiality. Availability ensures timely and reliable access to the smart grid for the use of necessary information. Lack of availability may lead in deflation of the power delivery activities. Integrity guarantees the authenticity and non-denial of the important information. Loss of integrity may result in the incorrect power management decisions. Confidentiality safeguards authorization of the private and proprietary information. Secret information should not be disclosed to individual users or public [2].

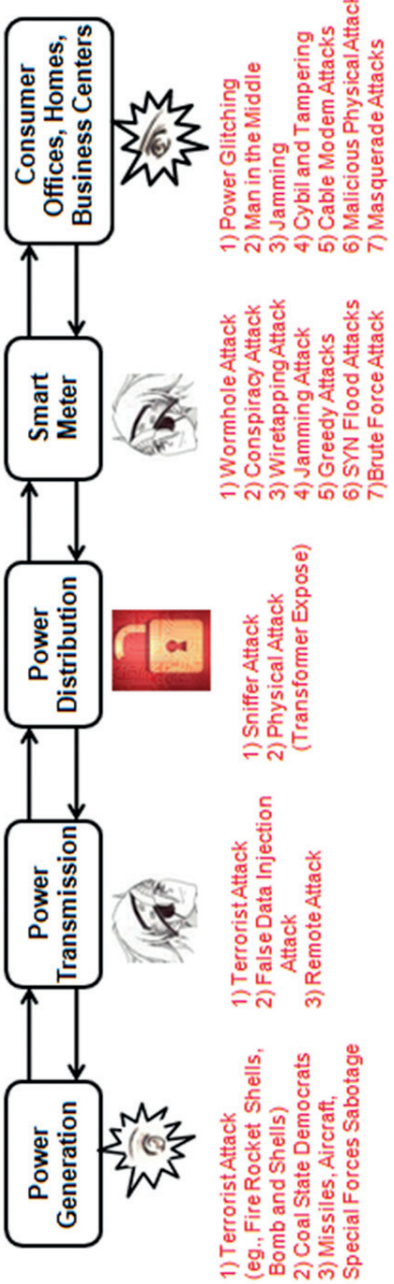

Figure 2 Possible cyber attacks on each stage of smart grid.

3.1 Smart Grid Infrastructure

Smart Grid infrastructure is a combination of various physical and cyber systems as depicted in Figure 3. From electricity power generation, distribution till consumption, it makes use of various wired and wireless networks such as Zigbee, PLC, Z-wave, IEEE 802.11, WiMAX, etc. [3]. These physical and cyber systems have different security threats such as electricity thefts, BOTNETs, data mining threats, threats to SCADA control system, online billing transaction threats, cloud computing faults, incident handling threats, information security threats, etc. it is very much essential to take into account the possible threat related to each and individual interface and design robust security solution for it. Different privacy related issues are there which can lead to the loss of trust of the consumers. Integrated cyber physical security solutions are very much necessary to bring the smart grid vision into reality. Convergence of wired and wireless services with heterogeneous security approach is needed to be developed.

Smart Grid suffers from various security issues. State of the art cyber physical security issues for smart grid are summarized in Table 1. Various parameters such as false data injection, survivability to intrusions, end to end access control and protection, delay sensitivity, power quality and voltage issues over long distance transmissions are considered here with different mechanisms for respective issue.

Estimation and decision techniques from information theory are found to be appropriate for various threats and other issues. Quality, reliability and efficiency are the basic requirements from the end users. User centric approaches are in much demand due to forthcoming user centric fifth generation (5G) communication technology. Privacy and trust are the major concerns from the consumer point of view. Green ICT standards are needed to be adopted while designing security protocols for each interface of the Smart Grid. Large scale storage capability with proper security measures is the essence of next generation social economy. Plug in hybrid electric vehicles can greatly save fuel consumption with the reduction in atmospheric pollution levels. Sensors are the tiny entities with limited battery, memory and computing capabilities. For such sensors, light weight security solutions are needed. Controllers should be redesigned with intelligence embedded into them. Present power grid system involves large amount of delays in almost every stage from generation, transmission, distribution, to consumption. Modernized Smart Grid ensures delay reduction with the help of automation techniques with smart objects with Internet of Things (IoT) and Machine to Machine Communication (M2M).

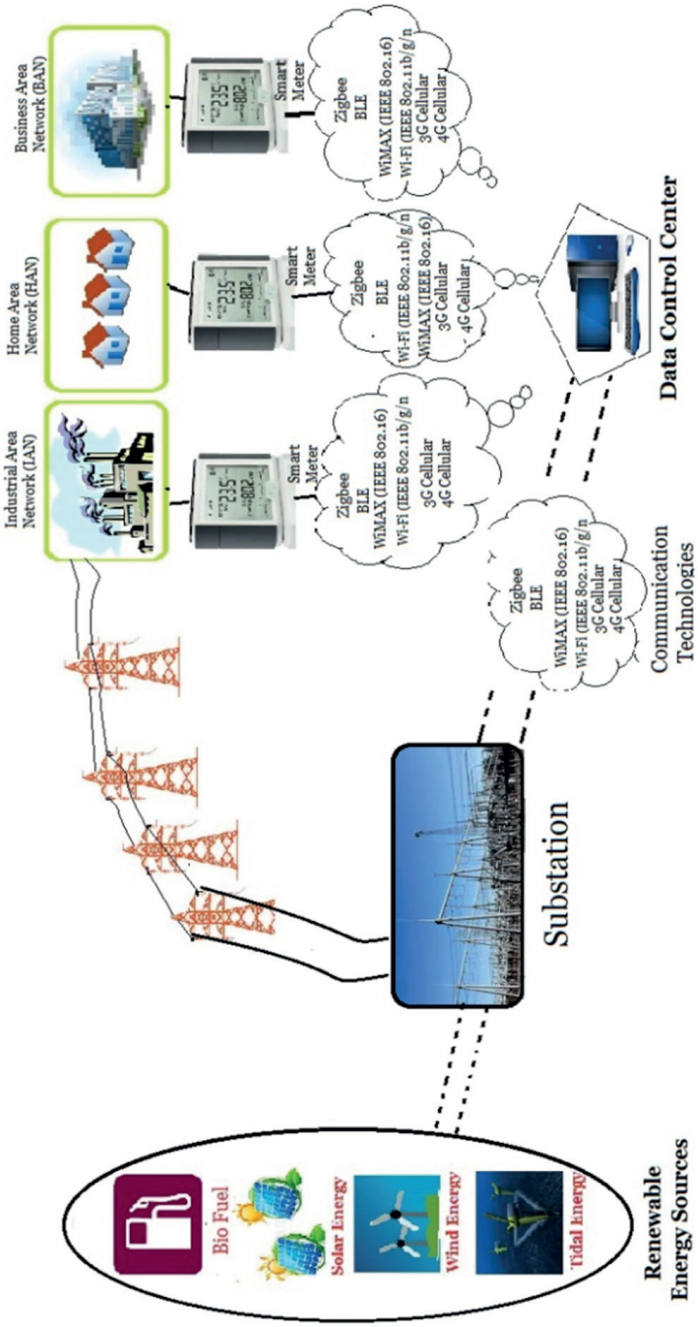

Figure 3 Smart grid infrastructure with communication networks.

Table 1 Smart grid security issues – state of the art

Technique/Algorithm	Parameters					
	False Data Injection (FDI) Attack	Survivable to Intrusions	End-to-End Access Protection	Malicious Cyber Attacks	Delay-Sensitivity	Power Quality and Voltage Issues
State Estimation Model Technique [4]	Yes	Yes		Yes		
State Estimation Model Technique [5]	Yes	Yes				
State Estimation Model Technique [6]	Yes	Yes				
Framework demonstrated a significant improvement in three unsupervised intrusion detection algorithms [7]		Yes		Yes		
Framework with a structured approach to define and analyse security related metrics for intrusion tolerant systems for each individual host in the network [8]		Yes		Yes		
Framework for risk management in major technological and health domains have been proposed [9]	Yes					
TQOS (Trustworthiness-based QoS) routing protocol is adopted. calculate the performance cost using certain encryption algorithm for building a secure route [10]			Yes		Yes	Yes
Efficient aggregation protocol with error detection, named APED, for secure smart grid communications [11]		Yes	Yes			
Coupling of ID based authentication and PKI mechanism, which offers mutual authentication between Smart devices [12]	Yes		Yes			
A key management scheme for secure data communications in a smart grid system that can support unicast, multicast and broadcast communications [13]	Yes	Yes	Yes	Yes		

Table 1 Continued

A mechanism to efficiently resist Denial-of-Service (DOS) attacks [14]	Yes	Yes	Yes	Yes		
Encryption key management mechanism for end-to-end security in the AMI [15]	Yes	Yes	Yes	Yes		
A new model for smart grid protection using biologically inspired concepts [16]	Yes	Yes	Yes	Yes		
A mechanism to access keys in the hardware module without any password [17]		Yes	Yes	Yes		

3.2 Smart Controllers with SCADA

Smart grid physical infrastructure design considers parameters such as power interruptions, quality of power and voltage related issues. Cyber infrastructure consists of communication network and supervisory control and data acquisition (SCADA) for control and reliable data communication. SCADA control center is supposed to monitor safety, reliability, secure exchange of data with high-speed, etc. Smart grid infrastructure is complex and critical therefore it can be easily targeted by attackers by introducing malicious software for interruption in power or manipulation in data. Security is major concern in smart grid. For security system designer, it is important to understand three key concepts confidentiality, integrity, and availability (CIA). For providing security tools such as authentication, authorization, and nonrepudiation can be used. Smart grid communication is bidirectional communication system therefore flow is bidirectional i.e., from control center to customer and customer to control center.

Smart grid infrastructure consists of physical infrastructure for transmission of electricity and communication network infrastructure for providing communication and control. Complexity of smart grid increases due to communication system formed by combination of hardware and software, therefore security of this system is critical issue. Attacker can attack on information and introduces false data in measurements in smart meter. For control and monitoring of critical infrastructures smart grid system uses Supervisory Control and Data Acquisition (SCADA) systems as shown in Figure 4. Control network is connected to consumer network using standard protocols such as TCP/IP therefore system is vulnerable to threats [4–6].

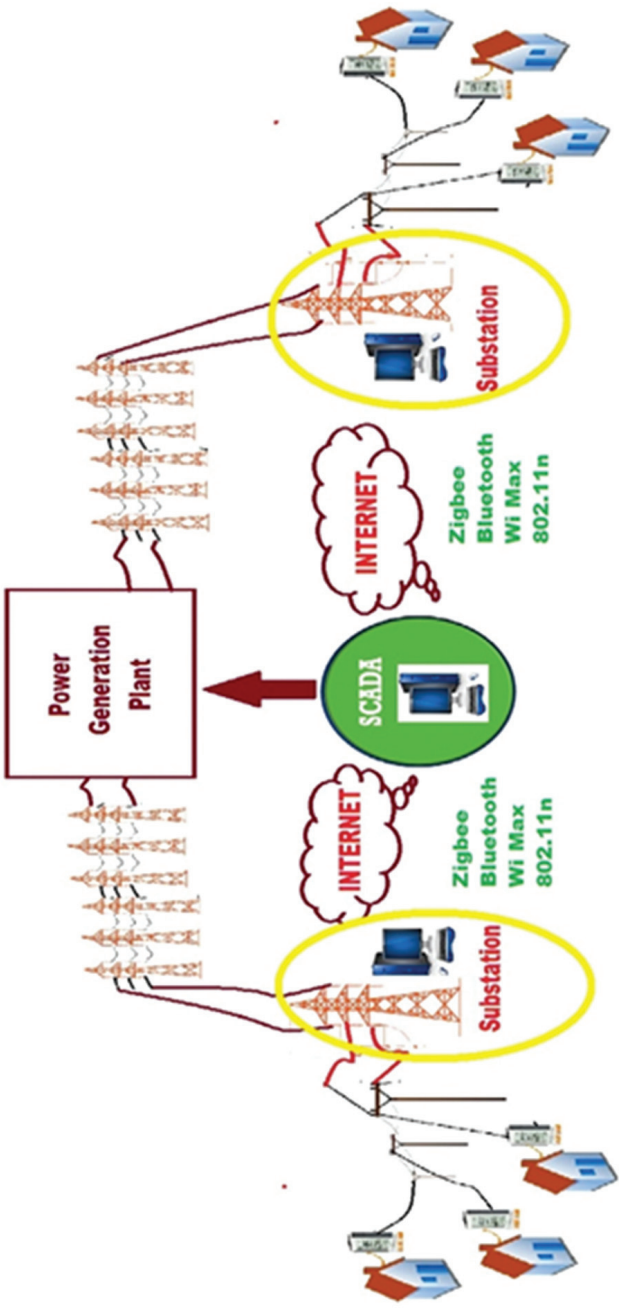

Figure 4 Smart grid infrastructure with SCADA.

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 Home Area Network (HAN), Neighbourhood Area Network (NAN) and Wide Area Network (WAN) serving numerous applications of smart grid. Thus a secured framework for routing protocols presents a promising solution for the security of the advance metering infrastructure (AMI) communication system. Secure Data Aggregation is also good method for security. 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 center 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. 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. Bartoli et al. in his research work in [17] has proposed a lossless aggregation protocol for AMI communication system while maintaining both per hop as well as end to end security.

For the successful evolution of smart grid, secure and reliable communication architecture is going to 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. Wenye and Zhuo provide a review on two proposed secure network architectures that include trust computing based architecture 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 the same time [2].

3.3 Advanced Metering Infrastructure (AMI)

Advanced metering infrastructure (AMI) is an architecture for programmed and bidirectional cooperative communication between a smart utility meter with an IP address and a utility company. The purpose of an AMI is to provide

service to service providers with real-time data of meter reading measurements to calculate power utilization by consumer.

Consumers can also get information about energy usage and billing information at any time. This information is shared via complex communication network therefore, eavesdropper can attack to hack information or to modify measured data. There are three primary threats to AMI: customer attacks, insider attacks, and terrorist or nation-wise attacks. These threats of cyber security result in loss of integrity and availability to the AMI system or to the bulk electric grid controls. System impacts range from increased peak usage up to widespread outages. AMI attacks could cause low to moderate local and regional consequences as a result of the system impacts. The risk of national harm is low to moderate but will increase as AMI market penetration increases. The lowest level highest probability threat to AMI implementations is the modification in measured consumer meter reading. Next threat with high probability is the insider attack whose motivation is financial. After The threats by international groups or terrorist groups are high levels with low-probability threats.

Figure 5 shows benefits of AMI [18]. AMI is beneficial for both consumers and electric power utility system. For the electric power utility system, AMI

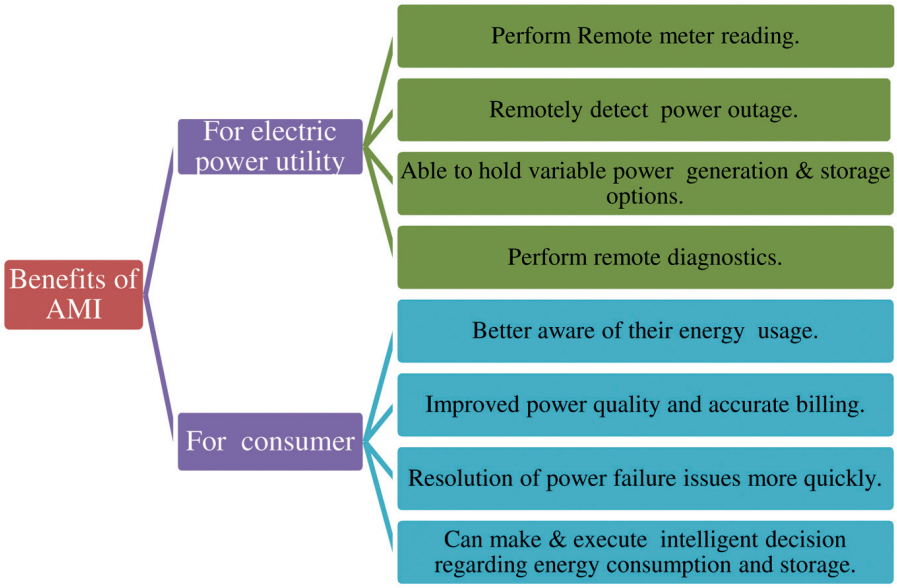

Figure 5 Benefits of advanced metering infrastructure (AMI).

can perform some operations such as meter reading, power outage detection and diagnostics remotely. Consumers can easily get awareness about their energy usage with better quality and accuracy. With AMI, power failure issues can be solved very quickly.

Advanced Metering Infrastructure plays vital role in real time monitoring of Smart bidirectional information flow of power related information i.e. smart metering data and control messages. Smart Grid network is vulnerable to many cyber threats and attacks which could result in unreliable system performance. Appropriate security technique is required to deal with cyber security concerns. Table 2 shows state of the art security methodologies for AMI.

Table 2 Security provisions for AMI in smart grid

Algorithm/Methodology	Reliability Scalability Efficiency	Confidentiality	Integrity	Availability	Accountability	Privacy/ Latency
Simple Cryptographic Algorithm (Novel KMS) [18]	E	√	√			P
Channel management algorithms, transmission interface-selection algorithm [19]	R, S					LL
IEEE 802.11s, proactive Path Request (PREQ) message of 802.11s standard (improves packet delivery ratio and throughput significantly) [20]	S, E, R					
Distributed algorithm, ECC algorithm symmetric key cryptography with the use of Bloom's key pre distribution scheme [21]	R, E	√	√	√		L
AMI Sec Checker, auth-algorithm [22]	E, S		√			P
WSN related methodology [23]	S, E, R					L
Sophisticated cryptographic algorithms, (SQUARE) method [24]	√	√	√	√	√	P
Mining Algorithms (data stream mining) (IDS) [25]	S, E, R	√	√	√		P
Polynomial time algorithm [26]	R, E					P
Secure Hash Algorithm. IT security architecture [27]	R, E	√	√	√		P, L
XACML Defines Combining Algorithms [28]						P

*Reliability = R, Scalability = S, Efficiency = E, Privacy = P, Latency = L, Low Latency = LL.

Intelligent Smart Grid should provide reliability, efficiency, scalability, privacy and security. But from the Table, it is clear that it provides reliability, efficiency, scalability but the performance degrades due to lack of privacy and security provisions.

Cyber security properties and approaches to be used in AMI are elaborated in Table 3 below [29].

3.4 Smart Meters

For periodic measurements of electricity consumption and regular communication of this information to power grid for record and billing purposes, the smart meters are used. Smart meter ensures two way communications between consumer meter and power grid central system. Table 4 summarises the possible attacks on smart meter and the probable security solutions for the respective attacks [30].

4 Secure Metering Schemes

The advanced metering infrastructure provides the competent and secure metering schemes. For security purpose, many researchers use cryptographic techniques, secure function evaluation technique, threshold cryptography and secret sharing technique. Following are different techniques for security in metering scheme.

The general framework for a secure metering scheme contains following things as shown in Figure 6.

- Secret sharing – It provides threshold metering schemes. It also provides dynamic multi threshold metering schemes.
- Client authentication – For security purpose the authentication based metering schemes are implemented by using digital signature schemes.

Table 3 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.
Availability	Provide whatever resources required.
Accountability	Accountable communication protocols using the proposed architecture.

Table 4 Smart meter attacks and probable solutions

Sr. No.	Possible Attacks on Smart Meters	Probable Security Solution
1	Physical Attacks such as battery change, removal, and modification	Integrity of Meter Data
2	Remote connect or disconnect meters and incorrect outage reporting by third entity apart from Grid system	Detection of unauthorised changes on meter
3	Changing of customer bills through metering database breaches	Authorization of all the accesses to/from AMI networks
4	Malicious Intruders in residential areas	Access Control to all customer interfaces
5	Unwarranted energy related data disclosure on communication links	Validation of notified information, Improved security of hardware and software upgrade
6	Incorrect billing or unwarranted service for plug in hybrid electric vehicles	Establishment of Electric Vehicle Standards
7	Replay attacks and revoked access to show insecure time information	Use phasor measurement units
8	Tampering of event log timestamps	Adoption of forensic technologies for accurate temporal logs
9	Damage of remote terminal units	Use of available fraud detection algorithms and models

- Micropayment – The micropayment provides security for online services.
- Pricing via processing – These schemes offer lightweight security.
- Threshold computation of a function – The problem of this approach is that known implementations of threshold computations are far too inefficient in terms of computation and communication to be applicable for metering.

Followings are the different techniques which are used for security purpose in advanced metering infrastructure.

a. Key Management Scheme (KMS) Cryptographic algorithms are chosen for key generation.
b. Identity based cryptography (ID based authentication protocol).

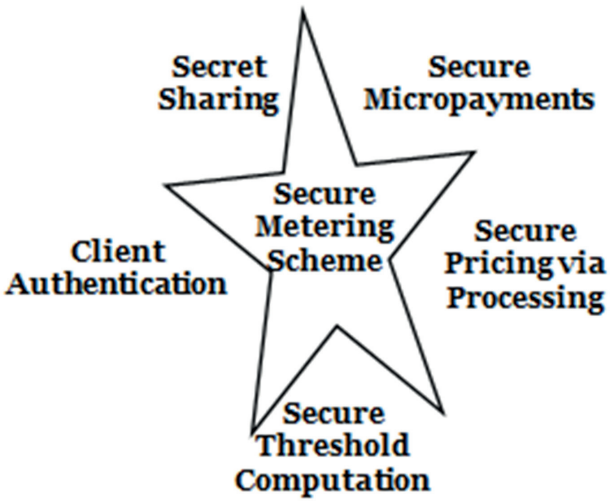

Figure 6 General secure metering scheme.

c. Probabilistic asymmetric key encryption algorithm.
d. Scalable Key Management (SKM) scheme by combining identity based cryptosystem and efficient key tree technique.
e. Physically Unclonable Function (PUF) technology hardware based.
f. Authenticated symmetric encryption algorithm.

KMS is used to solve the problem of security in smart meters but still it is not able to solve all the problems. ID based authentication protocols which provide source authentication, data integrity, non-repudiation services, confidentiality and privacy. Probabilistic asymmetric key encryption algorithm provides good confidentiality, privacy and integrity. SKM scheme provides efficiency in computation, reduces communication cost, more flexibility. PUF provides confidentiality and integrity.

5 Conclusions and Future Scope

For the security of cyber physical systems in smart grid, control and security technique co-designs are in huge demand. Overall interfaces in the smart grid system are needed to be developed with utmost care. Electricity power generation units with renewable or non-renewable energy sources, power transmission, distribution to substations and till consumer smart meters, every interface is of great importance. Electricity smart grid system as whole

is closely associated with consumers for household appliances, business customers or other office infrastructures consist of large amount of database related to personal information of the consumers. This leads to various privacy concerns. Strong countermeasures are necessary to battle these security breaches against consumer trust and privacy. Researchers have lot of research opportunities and directions with the security issues and features provided in this paper.

References

[1] Quang-Dung Ho, Yue Gao, Gowdemy Rajalingham, Tho Le-Ngoc, "Wireless Communication Networks for the Smart Grid", Springer Briefs in Computer Science, Springer, 2014.

[2] Wenye Wang, Zhuo Lu, "Cyber security in the Smart Grid: Survey and challenges", Elsevier Computer Networks, Vol. 57, pp. 1344–1371, 2013.

[3] Al-Omar B, Al-Ali AR, Ahmed R, et al., "Role of information and communication technologies in the smart grid", Journal of Emerging Trends in Computing and Information Sciences, Vol. 3, Issue-5, pp. 707–716, 2012.

[4] Mohammad Ashiqur Rahman, Ehab Al-Shaer, and Mohammad Ashfaqur Rahman, "A Formal Model for Verifying Stealthy Attacks on State Estimation in Power Grids" IEEE Symposium on Smart Grid, Cyber Security, and Privacy, Smart GridComm 2013.

[5] Ognjen Vukovic and Gyorgy Dan "Detection and Localization of Targeted Attacks on Fully Distributed Power System State Estimation" IEEE Symposium on Smart Grid Cyber Security and Privacy, SmartGridComm 2013.

[6] Gabriela Hug*, Member, IEEE*, and Joseph Andrew Giampapa "Vulnerability Assessment of AC State Estimation With Respect to False Data Injection Cyber-Attacks" IEEE Transactions On Smart Grid, Vol. 3, No. 3, September 2012.

[7] Abdulmohsen Almalawi, Zahir Tari, Adil Fahad and Ibrahim Khalil "A Framework for Improving the Accuracy of Unsupervised Intrusion Detection for SCADA Systems" 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications.

[8] Hui Wang, Suman Roy, Amitabha Das, and Sanjoy Paul, "A Framework for Security Quantification of Networked Machines", Infosys Technologies during June–July 2009.

[9] Riadh W. Y. Habash, Voicu Groza, Dan Krewski, Greg Paoli,"A Risk Assessment Framework for the Smart Grid" IEEE Electrical Power and Energy Conference (EPEC), 2013.
[10] Ziyuan Cai, Yizhou Dong, Ming Yu, and Mischa Steurer "A Secure and Distributed Control Network for the Communications in Smart Grid" IEEE Conference on Smart Grid Security, 2011.
[11] Ruixue Sun, Zhiguo Shi, Rongxing Lu, Min Lu, and Xuemin (Sherman) Shen "APED: An Efficient Aggregation Protocol with Error Detection for Smart Grid Communications", Ad Hoc and Sensor network Symposium, Globcom 2013.
[12] Sangji Lee, Jinsuk Bong, Sunhee Shin, Yongtae Shin, "A Security Mechanism of Smart Grid AMI Network through Smart Device Mutual Authentication" Information technology Research Center, Korea, 2013.
[13] Xuelian Long, David Tipper, Yi Qian, "An Advanced Key Management Scheme for Secure Smart Grid Communications", IEEE Symposium Smart Grid Cyber Security and Privacy, SmartGridComm 2013.
[14] Daojing He, Sammy Chan, Yan Zhang, Mohsen Guizani, Chun Chen and Jiajun Bu "An Enhanced Public Key Infrastructure to Secure Smart Grid Wireless Communication Networks" IEEE Network January/ February 2014.
[15] Seung-Hyun Seo, Xiaoyu Ding and Elisa Bertino "Encryption Key Management for Secure Communication in Smart Advanced Metering Infrastructures" IEEE Symposium Smart Grid Cyber Security and Privacy, SmartGridComm 2013.
[16] S. M. A. Mavee, E. M. Ehlers "A Multi-Agent Immunologically-Inspired Model for Critical Information Infrastructure Protection", IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 2012.
[17] Daewon Kim, Jeongnyeo Kim, and Hyunsook Cho, "An Integrity-Based Mechanism for Accessing Keys in A Mobile Trusted Module" IEEE ICTC 2013.
[18] Abdulmohsen Almalawi, Zahir Tari, Adil Fahad and Ibrahim Khalil, "A Framework for Improving the Accuracy of Unsupervised Intrusion Detection for SCADA Systems" 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 2013.
[19] Nian Liu, Jinshan Chen, Lin Zhu, Jianhua Zhang, Yanling He "A Key Management Scheme for Secure Communications of Advanced Metering Infrastructure in Smart Grid", IEEE Transactions On Industrial Electronics, Vol. 60, No. 10, October 2013.

[20] Hoi Yan Tung, Kim Fung Tsang, Kwok Tai Chui, Hoi Ching Tung, Hao Ran Chi, Gerhard P. Hancke, and Kim Fung Man "The Generic Design Of A High-Traffic Advanced Metering Infrastructure Using Zigbee", IEEE Transactions on Industrial Informatics, Vol. 10, No. 1, February 2014.

[21] Nico Saputro and Kemal Akkaya Department of Computer Science Southern Illinois University Carbondale "An Efficient ARP for Large-scale IEEE 802.11s-based Smart Grid Networks", IEEE Symposium Smart Grid Cyber Security and Privacy, 2013.

[22] Binod Vaidya, Dimitrios Makrakis, Hussein Mouftah "Secure and robust multipath routings for advanced metering infrastructure", Springer Science+Business Media, 2013.

[23] Mohammad Ashiqur Rahman and Ehab Al-Shaer,"A Declarative Logic-Based Approach for Threat Analysis of Advanced Metering Infrastructure" Springer International Publishing Switzerland, 2013.

[24] Omowunmi M. Longe, Khmaies Ouahada, Hendrick C. Ferreira, and Suvendi Rimer, "Wireless Sensor Networks and Advanced Metering Infrastructure Deployment in Smart Grid", Springer 167–171, 2014.

[25] Husam Suleiman, Davor Svetinovic "Evaluating the effectiveness of the security quality requirements engineering (SQUARE) method: a case study using smart grid advanced metering infrastructure", Springer Verlag London Limited, 2012.

[26] Mustafa Amir Faisal, Zeyar Aung, John R. Williams, and Abel Sanchez "Securing Advanced Metering Infrastructure Using Intrusion Detection System with Data Stream Mining", Springer-Verlag Berlin Heidelberg 2012.

[27] Hsiao-Ying Lin, Wen-Guey Tzeng, Shiuan-Tzuo Shen, and Bao-Shuh P. Lin, "A Practical Smart Metering System Supporting Privacy Preserving Billing and Load Monitoring", Springer Verlag Berlin Heidelberg 2012.

[28] David von Oheimb, "IT Security Architecture Approaches for Smart Metering and Smart Grid", Springer-Verlag Berlin Heidelberg 2013.

[29] Peter Ebinger, José Luis Hernández Ramos, Panayotis Kikiras, Mario Lischka, and Alexander Wiesmaier, "Privacy in Smart Metering Ecosystems", Springer-Verlag Berlin Heidelberg 2013.

[30] U.S. NIST, "Guidelines for smart grid cyber security," NIST IR-7628, Aug. 2010, available at: http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7628.

Biographies

V. M. Rohokale received her B.E. degree in Electronics Engineering in 1997 from Pune University, Maharashtra, India. She received her Masters degree in Electronics in 2007 from Shivaji University, Kolhapur, Maharashtra, India. She received her Ph.D. degree from CTIF, Aalborg University, Denmark under the guidance of Prof. Ramjee Prasad. She is presently working as Dean R&D at SKN Sinhgad Institute of Technology and Sciences (SKNSITS), Lonavala, Maharashtra, India. Her research interests include Cooperative Wireless Communications, AdHoc and Cognitive Networks, Physical Layer Security, Information Theoretic security and its Applications, Cyber Security, etc.

R. Prasad is currently the Director of the Center for TeleInFrastruktur (CTIF) at Aalborg University, Denmark and Professor, Wireless Information Multimedia Communication Chair. Ramjee Prasad is the Founder Chairman of the Global ICT Standardisation Forum for India (GISFI: www.gisfi.org) established in 2009.

GISFI has the purpose of increasing of the collaboration between European, Indian, Japanese, North-American and other worldwide standardization activities in the area of Information and Communication Technology (ICT) and related application areas. He was the Founder Chairman of the HERMES

Partnership – a network of leading independent European research centres established in 1997, of which he is now the Honorary Chair. He is a Fellow of the Institute of Electrical and Electronic Engineers (IEEE), USA, the Institution of Electronics and Telecommunications Engineers (IETE), India, the Institution of Engineering and Technology (IET), UK, Wireless World Research Forum (WWRF) and a member of the Netherlands Electronics and Radio Society (NERG), and the Danish Engineering Society (IDA).

He is also a Knight ("Ridder") of the Order of Dannebrog (2010), a distinguished award by the Queen of Denmark. He has received several international award, the latest being 2014 IEEE AESS Outstanding Organizational Leadership Award for: *"Organizational Leadership in developing and globalizing the CTIF (Center for TeleInFrastruktur) Research Network"*.

He is the founding editor-in-chief of the Springer International Journal on Wireless Personal Communications. He is a member of the editorial board of other renowned international journals including those of River Publishers. Ramjee Prasad is a member of the Steering committees of many renowned annual international conferences, e.g., Wireless Personal Multimedia Communications Symposium (WPMC); Wireless VITAE and Global Wireless Summit (GWS). He has published more than 30 books, 900 plus journals and conferences publications, more than 15 patents, a sizeable amount of graduated Ph.D. students (over 90) and an even larger number of graduated M.Sc. students (over 200). Several of his students are today worldwide telecommunication leaders themselves.