An Analysis of Smart Grid Attacks and Countermeasures

Zubair A. Baig and Abdul-Raoof Amoudi
King Fahd University of Petroleum & Minerals, Dhahran 31261, Saudi Arabia
Email: zbaig@kfupm.edu.sa; g201003240@kfupm.edu.sa

Abstract—The threat of malicious attacks against the security of the Smart Grid infrastructure cannot be overlooked. The ever-expanding nature of smart grid user base implies that a larger set of vulnerabilities are exploitable by the adversary class to launch malicious attacks. Extensive research has been conducted to identify various threat types against the smart grid, and to propose counter-measures against these. Work has also been done to measure the significance of threats and how attacks can be perpetrated in a smart grid environment. Through this paper, we categorize these smart grid threats, and how they can transpire into attacks. In particular, we provide five different categories of attack types, and also perform an analysis of the various countermeasures thereof proposed in the literature.

Index Terms—countermeasures, cyber-threats, smart grid security.

I. Introduction

Smart Grids (SGs) have emerged as a very crucial platform for provisioning timely, efficient, and uninterrupted power supply to consumers. At the same time, through support from the underlying smart infrastructure, consumers are able to optimize electricity usage by receiving constant and accurate feedback on usage patterns from the smart meters. The expansive and ubiquitous presence of diverse devices that comprise a smart grid invariably exposes its vulnerabilities for exploitation by the adversary class to launch malicious attacks.

Numerous attacks of various categories may be perpetrated against the entire SG or against specific components therein. The first step towards defending against such attacks is there identification and appropriate detection. Through this paper, we attempt to categorize various attack types and countermeasures that exist against the SG. In particular, we categorize attacks based on their respective victim service or device, as well as attack type. The five categories of smart grid cyber-attacks and countermeasures that we highlight through this paper are listed as follows:

1. Supervisory Control and Data Acquisition (SCADA) attacks,
2. Smart Meter Attacks,
3. Physical Layer Attacks,
4. Data Injection and Replay Attacks, and
5. Network-based Attacks.

In Table I, an overview of security properties affected by the various SG attacks, and the network location where such attacks are perpetrated, is provided.

TABLE I. Attack Types with Descriptions

Attack type	Which security property is affected?	Victim location
SCADA	Confidentiality, denial of service, integrity	Home area networks
Smart meter	Confidentiality, integrity, availability, non-repudiation	Home area/neighborhood area networks
Physical layer	Data integrity, denial of service, confidentiality	Home Area/neighborhood area/ wide area networks
Data injection and replay attacks	Confidentiality	Home area/neighborhood area/ wide area networks
Network-based	Availability, confidentiality	Home area/ neighborhood area/ wide area networks

The rest of this paper is organized as follows: Section II provides a detailed cyber-security requirement summary for the SG. We provide descriptions of various SCADA security threats and proposed countermeasures, in Section III. Smart meter-specific attacks and countermeasures are discussed in Section IV. In Section V, we provide detailed analysis of attacks that are perpetrated against the physical layer of the SG. Data Injection and Replay Attacks are discussed in Section VI. In Section VII, we study and report network-based attacks. Finally, we provide concluding remarks in Section VIII.

II. Smart Grid Cyber Security Requirements

The requirements for cyber security in the smart grid infrastructure can be categorized into the following aspects; cyber-security requirements, typical cyber-attacks, and countermeasures [1] [2]. Ref. [3] identifies the main source of information security risks to exist at six vulnerable points of the smart grid: Power station, Power distribution network, Advanced Measurement Systems, Electric vehicles, Indoor Internet users, and Operation networks of the power transmission systems. Refs [4] and [5] highlight the cyber-security vulnerabilities and attacker entry points to the smart grid infrastructure.

Manuscript received June 15, 2013; revised July 30, 2013.
Corresponding author email: zbaig@kfupm.edu.sa.
doi:10.12720/jcm.8.8.473-479

According to the National Institute of Standards and Technology (NIST), the three key cyber-security requirements for the SG are: availability, integrity, and confidentiality. The following are some typical cyber-attacks which may adversely affect SG operations: denial of service (DoS) and distributed denial of service (DDoS) attacks, wherein, the aim is to diminish the availability of the SG system by preventing message delivery between SG devices. Malicious software based attacks may directly or indirectly compromise the availability, integrity, and confidentiality of the SG. Identity spoofing attacks allow adversaries to impersonate authorized SG users. Man-in-the-middle, message replay, and network spoofing are examples of identity spoofing attack. Password pilfering attacks are perpetrated against data confidentiality. Common methods used for this attack include: password guessing, social engineering, dictionary attacks, and password sniffing. Eavesdropping attacks affect data confidentiality of the SG communication channel through sniffing of IP packets on the LAN or intercepting wireless transmission on the home area network. Intrusions occur when an illegitimate user gets access to a cyber-system and obtain unwanted access to critical back-end servers. Side-channel attacks aim to retrieve the cryptographic keys. Power analysis attacks, electromagnetic analysis attacks, and timing attacks are common side-channel attacks. Smart meters and in-house devices of SG are vulnerable to this attack which could result in violation of customer privacy, usage information, passwords, and administrative access to SG system [4], [5].

To avoid the aforementioned typical cyber-attacks, the International Electro-technical Council (IEC) has proposed a set of appropriate countermeasures: Technical solutions include: encryption, access control, anti-virus, firewall, Virtual Private Networks, intrusion detection systems (IDS), etc. From a security management viewpoint, solutions include, key management, risk assessment of assets during-attack coping and post-attack recovery, security policy exchange, security incident and vulnerability reporting, etc. Slammer and Stuxnet worms are examples of real cyber-security incidents.

In Ref. [2], the authors identify major cyber-security challenges as: Internetworking, Security policy and operations, Security services, Efficiency and scalability, and differences between legacy and smart grid networks in terms of security. In Fig. 1 we provide the standard smart grid architecture, with attack categories highlighted at appropriate locations of the architecture.

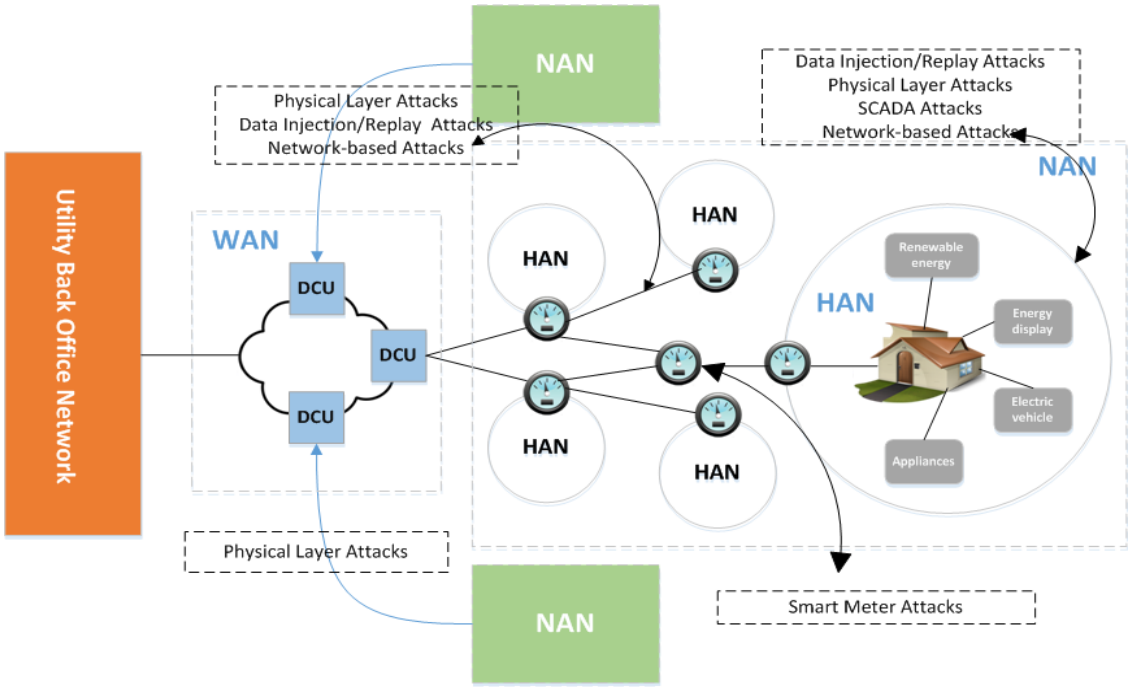

Figure 1. Smart grid communication architecture with attacks illustrated.

III. SCADA Security Concerns

Integration of the power grid with computing devices and networks has had a profound effect on the security of the smart grid. The vulnerabilities in the power grid are a known concern [6]. The integration of power system devices with backend servers and invariably the Internet, have led to the exposure of the smart grid to a wide-range of cyber attacks. One such system that has received attention is the Supervisory Control and Data Acquisition (SCADA). The key attacks that may target critical smart grid infrastructure resources through SCADA can be summarized as follows [6]:

A. Platform Vulnerabilities

Known security holes in existing corporate and backend networks and computing resources are exploitable to target smart grid devices. If an operating system patch is not installed, the adversary can compromise the computing system of the smart grid, to launch an attack against SCADA devices. Similarly, applications that are vulnerable, and are not having a front-end firewall or intrusion detection system, will provide the ideal platform to the adversary for attacking the smart grid. Other potential vulnerabilities include software-based attacks, which exploit weaknesses in the programs that run on the SCADA system resources. Some examples include buffer overflow and Denial of Service, wherein, the inherent ability of the software to constantly request hardware resources for program execution, are exploited beyond the capability of the system. Similarly, a large set of requests for resource allocation at the end-servers may lead to a Denial of Service against legitimate users, invariably affecting the consumer confidence on the utility provider.

B. Policy Vulnerabilities

In general, weak policies that may be defined by security managers have been a key cause of concern. A similar threat exists for information systems that are interconnected with smart grid SCADA Devices. If a weak password leads to the compromise of a system by an attacker, the policy administrator is accountable. It is therefore imperative to have strong security policies in place to ensure that exploitable weaknesses due to weak policies, are nonexistent.

C. Network Vulnerabilities

Network layer devices pose a significant threat to the smart grid infrastructure. A network device configured based on weak security policies may lead to compromise of the smart grid through ingress and egress network holes, which connect SCADA devices with the central network of the smart grid infrastructure. Tampering of IP packets at the network device level, through source/destination address spoofing, fragmented message interruption, packet flag alteration, and outstation data resetting, are a few examples of how mal-configured network-layer devices can pose a serious threat to the smart grid.

IV. Smart Meter Attacks and Countermeasures

The smart meter is the central connecting point between a user's home network and the utility provider (see Fig. 1). Moreover, the electricity usage readings of a household are monitored and subsequently transmitted to the data center of the utility company, on a regular basis by the smart meter. Therefore, the security of the smart meter is of utmost importance to the overall security of the smart grid infrastructure. A summary of smart meter attacks against the four key pillars of information security are outlined below [7]:

A. Confidentiality

Attacks targeting confidentiality are attempts to steal information that should be kept secret or shared only between trusted parties. Examples of such attacks are: reading device's memory, altering the control program of a smart meter, spoofing/sniffing of payload, and message replay attacks. Several countermeasures have been proposed to diminish the effect of data confidentiality breach within a smart meter. These include: replacing secret keys that the smart meter shares with a data concentrator unit in a neighborhood area network, Device reconfiguration/resetting to remove the traits of the malicious attacks, including secret key resetting, and replacing the actual device. The *privacy* of user data is of utmost concern in the smart grid. The electricity usage pattern of a given household may lead to disclosure of several sensitive parameters; consumer habits (invariably sellable to marketing and spam operators), whether the consumer is at home or away traveling [8]. Such information can expose information to competitors of the utility service provider [9].

B. Integrity

An attack against a smart meter's integrity takes place when legitimate data of the smart meter is tampered with, replaced, or deleted, before its transmission to the data concentrator unit of a neighborhood area network. The data is manipulated by the adversary either locally i.e. within the victim's computing resource or memory, or remotely through forging/injection/deletion of messages. The adversary may inject fictitious data into the smart meter communication channel to either portray increased electricity consumption of a household, or to reduce it. In both cases, the loss is bore by the legitimate end-users and/or the utility provider.

Message replay attacks may be launched with one of two intentions. The utility provider may receive the same smart meter readings from a household, as previous ones. As a result, increased usage of electricity of a household may go unreported. Similarly, a forging attack to reduce the reported electricity usage data from a household may benefit the end users, at the cost of loss to the utility provider. Several techniques exist to reduce the effect of smart meter integrity attacks. The most common approach being to generate and maintain secret keys of reasonable length (based on current technological trends) between the sender and receiver of the electricity usage data. Such an approach will help ascertain that a message authentication code (MAC) will verify the message integrity at the receiver's end.

C. Availability

A smart meter is also vulnerable to attacks against its continuing availability. Some common examples of such attacks are: switching off the device, jamming communication channel, Denial-of-Service against domain name servers (DNS) at the corporate network, and spoofing. Considering the ZigBee security mode

being disabled in a smart meter, it is possible to invoke a remote switch off request, to demand a smart meter be shut down. Consequently, the household electricity usage is unreported until the smart meter is restarted. Jammed communication channels will have similar consequences as the previous attack. Modifying the secret keys stored within a smart meter will prevent decryption of secure messages transmitted by the meters to the data concentrator units and end-servers. For all three scenarios, the availability of the smart meter is affected.

Countermeasures against such attacks include: replacement of compromised or tampered smart meters, changing the channel frequency for message transmission, updating the secret keys, and enabling the security mode of the ZigBee standard.

D. Non-Repudiation

Such attacks are attempts by the adversary to deny any wrongdoing. For instance, a compromised smart meter may transmit an incorrect reading to the utility provider, and claim to have not done so. If the smart meter is using a secret key for data encryption, non-repudiation is enforced inherently, as no other entity is expected to possess a copy of the same secret key. On the contrary, the lack of a secret-key based mechanism will encumber identification of such an attack.

A common reason for attacks against the smart meter [10] is manipulation of the meter configuration. The meter must therefore be secure enough to withstand both hardware as well as software-based attacks, that attempt to modify its configuration. The large scale deployment of smart meters (Number of smart meters = Number of households), in a metropolitan city, demand enough security, to prevent a large-scale catastrophe through such attacks. A quantum cryptography-based approach for data confidentiality in the SG is proposed in [11].

V. Physical Layer Attacks and Countermeasures

In Ref. [12], the authors propose a wireless communication architecture for the Smart Distribution Grid (SDG), and the security framework for this communication architecture is analyzed. Several design rules are formulated to secure the SDG framework:

1) Security measures must be considered at all protocol layers,
2) Time critical messages must be protected through a deployed security mechanism, and
3) All wired communication paths must be leveraged to strengthen security of the wireless communication networks.

The authors identify threats against the SDG from the wireless channel as follows:

1) Jamming,
2) Eavesdropping by nodes from outside the channel,
3) Eavesdropping by malicious nodes from within the wireless medium, and
4) Launching attacks from within the wireless network of the SDG.

The following security measures were proposed for cyber-security of the SDG:

1) Anti-jamming technique
2) Physical layer security to disable eavesdropping
3) Effective authentication schemes to block network access by malicious nodes
4) Secure protocols to prevent inside attackers

A detailed analysis of the physical layer attacks is given as follows [12] [13]:

A. Eavesdropping

Wireless signals are carried in open space, and are susceptible to eavesdropping by an adversary. Sensitive information from a smart meter can easily be observed, and assessed through such an attack. Low-cost eavesdroppers exist in the market, to convenience launch of such attacks. Data encryption is an approach towards protecting sensitive information from revelation to the adversary. However, if a certain pattern is depicted by the transmitted data, an intelligent adversary may still be able to decipher the message content. For instance, if a household is unoccupied, the electricity usage will dwindle. If the smart meter is programmed to communicate with the data concentrator unit only when a certain threshold of energy usage is crossed, or if the message length to be transmitted is directly proportional to energy consumption, then a pattern of activity of the household may be construed.

B. Jamming

The main goal of this attack is to prevent the smart meters from communicating with the utility provider, through jamming of the wireless medium with noise signals. Such attacks can be classified into two types: i) Proactive jamming, wherein the jammer can emit noise signals continuously to completely block a wireless channel, and (ii) Reactive jamming, wherein the jammer first eavesdrops on the radio channel and launches the attack only when signals are sensed on the channel. As a result of such an attack, the legitimate smart meter can be affected into two ways: (i) the channel will be tagged as "busy" for any carrier sensing done by a legitimate smart meter, and (ii) the smart meter may be prevented from receiving packets. It is non-trivial to differentiate between reactive jammer attacks that may be result from routine communication signals and from adversary-initiated signals.

C. Injecting Requests/ Restricting Access

The main goal of this attack is disrupt the routine operations at the MAC layer of the smart meter. The attacker prevents the smart meters from initiating legitimate MAC operations or causes packet collision. This attack is highlighted as follows: (i) it is similar to reactive jamming; in which the attack is launched based with the intent to block the communication channel, (ii) it

targets a multi-user access channel, and (iii) the attacker sets its own backoff timer to be very short in length, so that the channel prioritizes access to the adversary each time it wishes to communication, denying access to legitimate smart meters of the smart grid.

D. Injection Attacks

Unlike the previous two attacks that rely on bogus signals, this attack inserts formatted messages into the wireless network. We may highlight this attack as follows: (i) the adversary mimics either a legitimate sender or a receiver to get unauthorized access to a wireless network, and (ii) this attack is similar in property to the TCP-SYN flooding attack wherein, the victim's resources are overwhelmed through processing of fictitious messages received.

Such an attack can be prevented through appropriate security mechanisms in place, to ensure message authentication.

VI. Data Injection and Replay Attacks

Another class of malicious attacks in the smart grid is the data injection and replay attack. False data injection attacks occur when falsified data is injected into the smart meter or neighborhood area measurements observed by the network operator. Such attacks target the smart grid infrastructure, particularly measurement and monitoring sub-systems with the aim of manipulating meter and phasor measurements, so as to misguide the operation and control of the utility provider [14]. In Refs. [14], [15], and [16], an attempt is made towards intelligently analyzing smart grid data for possible data injection. The proposed detection technique for such an attack does an estimate on the state of the system from the observed measurements and computes the residual between the observed and the estimated measurements.

Message replay attacks occur when an attacker gains an elevated privilege to smart meters and can thus inject control signals into the system. In order to launch such an attack the adversary needs to (a) capture and analyze the data transmitted between appliances and smart meters to gain the customer's characteristics of power usage, and (b) fabricate and inject false control signals into the system. The aim of the replay attack is: (a) to steal energy by rerouting power to another location, and (b) cause physical damage to the system. The well-known example of such an attack is Stuxnet.

In Ref. [17], a scheme is proposed for detecting message replay attacks in the smart grid. The household devices are treated as linear time invariant systems, with the smart meter entrusted the task of observing the household devices. A state estimator based on Kalman filters is employed for testing the minimum variance that is observed in actual device readings when compared to expected readings. A detector device is tasked with providing a decision on the observed readings, and confirming any anomalous activity that might be affecting the smart grid. Not only is the scheme adaptable for a single household, rather, the authors have also proposed the use of a single detector and estimator for a group of households in the neighborhood. The replay attack is defined simply as a modification to the control signal which is transmitted by a consumer device to the smart meter.

In [18], a graph theory-based approach towards detecting attacks against state estimator perturbations. The whole power system is modeled as a graph constituted of buses, transmission lines and smart meters. The state estimation is performed in centralized manner by the control system center. The goal of estimation is to recover the full system state. Upon injection of adversarial data, the state does not remain the same. This is verified by measuring the Minimum Mean Square Error (MMSE), which will invariably be higher in the presence of injected malicious data. Higher the injected energy is, the more likely that the attack is detected by the control center. Based on the Generalized Likelihood Ratio Test (GLRT), suspect meters are confirmed as injecting malicious data into the network, through simple optimization. The algorithm operates in polynomial time and finds the smallest unobservable attacks that cause the highest damage to the state estimations.

VII. Network-Based Attacks

The man-in-the-middle is a notorious example of topology attacks of a Smart Grid [19]. This attack happen when the adversary intercepts network data (e.g., breaker and switch states) and meter data from remote terminal units, fabricates part of these, and forwards the modified version to the control center. In the absence of data alerts in the modern power systems the enemy could succeed to modify both network and meter data elaborately such that they are consistent with the "target" topology.

In Ref. [20], a fusion-based defense technique is proposed for identifying attacks in the smart grid based on feedback received from individual nodes in the network. Through the support of the necessary communication protocol, each node is required to communicate with a centralized fusion center to convey their individual observations. It is highlighted in the paper, that intentional attacks may be targeted to only a specific subset of nodes of the smart grid, and therefore feedback from all nodes is essential for accurately detecting these attacks. A game theoretic analysis is subsequently provided, wherein, the attacker is treated as one player and the defender as another. Based on the notion that the attacker will intend to compromise the most critical nodes, the defense strategy is to ensure that timely local observation by individual critical nodes, and subsequent communication of findings to the centralized fusion center, is essential.

Time Synchronization Attacks [21]: Critical operations of Smart Grid such as fault detection and event location estimation are heavily depends on precise timing

information. Time Synchronization Attack (TSA) is the well-known example of an attack that could target the timing information in the Smart Grid Infrastructure (SGI). Three applications of phasor measurement units (PMU) are affected by such an attack, namely, transmission line fault detection, voltage stability monitoring, and event localization.

In Ref. [22], the effects of Denial of Service (DoS) attacks against the load frequencies of smart grids, is studied. Smart grid data measured by remote terminals is sent to centralized control centers. If the communication channel between these sensors and the control center is attacked i.e. incapacitated from delivering messages to the destination, the DoS attack can significantly affect the smart grid operations. The adversary an launch such an attack on the communication channel by jamming the channel through injecting a large numbers of packets. The power system is represented as a linear time invariant model. For a switched linear system, if the computed Eigenvalues for the system matrix fall outside the unity circle, then a DoS attack is identified.

VIII. Conclusions

A smart grid infrastructure attack does not affect the consumers alone, rather, the utility providers' business as well. There is a plethora of threats against the smart grid infrastructure, which may transpire into attacks based on the benefit they will provide to the adversary. We have categorized all such attacks into five distinct classes, for ease in identification and analysis. Countermeasures against all such attacks have also been studied and reported in the paper. Extensive research work is still needed to ensure that the smart grid is highly secure against the adversarial threat, without affecting the consumer confidence in the utility provider, and without significantly inconveniencing the consumers through deployment of strong security controls.

Acknowledgment

The authors wish to King Fahd University of Petroleum & Minerals for its continuing support to conduct research.

References

[1] Y. Yang, L. Tim, S. Sezer, K. McLaughlin, and H. F. Wang, "Impact of cyber-security issues on Smart Grid," in *Proc. 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies*, Manchester ,Dec 2011, pp. 1-7.

[2] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," *IEEE Commun. Surveys Tuts.*, vol.14, no. 4, pp. 998-1010, 2012.

[3] Z. Zhang, H. Liu, S. Niu, and J. Mo, "Information security requirements and challenges in smart grid," in *Proc. 6th IEEE Joint International Information Technology and Artificial Intelligence Conference*, Chongqing, Aug 2011, pp. 90-92.

[4] M. Apurva and K. Himanshu, "Towards addressing common security issues in smart grid specifications," in *Proc. 5th International Symposium on Resilient Control Systems*, Aug 2012, pp. 174-180.

[5] Y. Mo, T. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, "Cyber–physical security of a smart grid infrastructure," in *Proc. IEEE*, vol. 100, no. 1, Jan 2012, pp. 195-209.

[6] I. Ghansa, "Smart grid cyber security potential threats, vulnerabilities, and risks," *Technical Report*, California Energy Commission, May 2012.

[7] V. Roberto, Y. Ender, and R. Carroline, "Smart grid security a smart meter-centric perspective," in *Proc. 20th Telecommunications Forum*, Nov 2012, pp. 127-130.

[8] H. Khurana, M. Hadley, L. Ning, and D. A. Frincke, "Smart-grid security issues," *IEEE Security & Privacy Mag.*, vol. 8, no. 1, pp. 81-85, Jan-Feb 2010.

[9] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE Security & Privacy Mag*, vol. 7, no. 3, pp. 75-77, May-June 2009.

[10] F. Skopik and M. Zhendong, "Attack vectors to metering data in smart grids under security constraints," in *Proc. IEEE 36th Annual Computer Software and Applications Conference Workshops*, Izmir, July 2012, pp. 134-139.

[11] M. Xin and C. Xi, "Cyber security infrastructure of smart grid communication system," in *Proc.China International Conference on Electricity Distribution*, Sept 2012, pp. 1-4.

[12] X. Wang and P. Yi, "Security framework for wireless communications in smart distribution grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 809–818, 2011.

[13] L. Eun-Kyu, G. Mario, and O. Y. Soon, "Physical layer security in wireless smart grid," *Communications Magazine, IEEE*, vol. 50, no. 8, pp. 46-52, August 2012.

[14] A. Rahman and M-R. Hamed, "False data injection attacks with incomplete information against smart power grids," in *Proc. IEEE Global Communications Conference*, Dec 2012, pp. 3153-3158.

[15] O. Mete, E. Inaki, V. Fatos, K. Sanjeev, and P. Vincent, "Smarter security in the smart grid," in *IEEE Third International Conference on Smart Grid Communications (SmartGridComm)*, Tainan, Nov. 2012, pp. 312-317.

[16] H. Yi, E. Mohammad, N. Huy, Z. Rong, H. Zhu, L. Husheng, and S. Lingyang, "Bad data injection in smart grid: attack and defense mechanisms," *Communications Magazine, IEEE*, vol. 51, no. 1, pp. 27-33, January 2013.

[17] T. Thien-Toan, S. Oh-Soon, and L. Jong-Ho, "Detection of replay attacks in smart grid systems," in *Proc. International Conference on Computing, Management and Telecommunications*, Jan 2013, pp. 298-302.

[18] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on smart grid state estimation: attack strategies and countermeasures," in *Proc. IEEE Smart Grid Comm*, Gaithersburg, MD, Oct 2010, pp. 220-225.

[19] K. Jinsub and T. Lang, "On topology attack of a smart grid," in *IEEE PESInnovative Smart Grid Technologies*, Feb 2013, pp. 1-6.

[20] P. –Y. Chen, S.-M. Cheng, and K.-C. Chen, "Smart attacks in smart grid communication networks," *IEEE Commun. Mag.*, vol. 50, no. 8, pp. 24-29, Aug 2012.

[21] Z. Zhenghao, G. Shuping, D. D. Aleksandar, and L. Husheng, "Time synchronization attack in smart grid: Impact and analysis,"*IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 87-98, March 2013.

[22] L. Shichao, L. P. Xiaoping, and S. E. Abdulmotaleb, "Denial-of-service (dos) attacks on load frequency control in smart grids," in *Proc. IEEE PES Innovative Smart Grid Technologies*, Feb 2013, pp. 1-6.

ZubairA. Baig graduated with highest distinction from the computer engineering department at KFUPM in 2002. He obtained an M.S. in

electrical and computer engineering from the University of Maryland, College Park, U.S.A. in 2003. He received his Ph.D. in computer science from Monash University, Australia in 2008, with the thesis topic being modeling and detection of distributed denial of service attacks in Wireless Sensor Networks.

Dr. Baig worked as an information security specialist with Fraud management technologies, Melbourne, from Sept. 2007 till Sept. 2008, and was a postdoctoral research fellow with the School of mathematical sciences, RMIT, Melbourne, from Sept. 2008 till February 2009. He is currently an assistant professor of computer engineering at KFUPM, Dhahran. He has over 33 published Journal and Conference papers in the areas of Network and Information Security (including Attack Modeling and Defense Techniques, and Intelligent computing. He has been involved in 7 funded projects, focusing on Network and Information Security.

Dr. Baig is a member of the IEEE. He was awarded the IEEE best student award in 2002.

Abdul-Raoof Al-Amoudy is a graduate student working towards his M.S. in computer engineering at KFUPM, Dhahran, Saudi Arabia.