Towards A Secure Network Architecture for Smart Grids in 5G Era

Firooz B. Saghezchi*, Georgios Mantas†, José C. Ribeiro†, MS Al-Rawi*, Shahid Mumtaz†, Jonathan Rodriguez*†
*Departamento de Eletrónica, Telecomunicações e Informática (DETI), Universidade de Aveiro, Portugal
†Instituto de Telecomunicações, Campus Universitário de Santiago, 3810-193 Aveiro, Portugal
Email: *{firooz, al-rawi, jonathan}@ua.pt
†{gimantas, jcarlosvgr, smumtaz, jonathan}@av.it.pt

***Abstract*—Smart grid introduces a wealth of promising applications for upcoming fifth-generation mobile networks (5G), enabling households and utility companies to establish a two-way digital communications dialogue, which can benefit them both. The utility can monitor real-time consumption of end-users and take proper measures (e.g., real-time pricing) to shape their consumption profile or to plan enough supply to meet the foreseen demand. On the other hand, a smart home can receive real-time electricity prices and adjust its consumption to minimize the daily electricity expenditure of the household, while meeting the energy need and the satisfaction level of the dwellers. Smart Home applications on mobile devices (e.g., smart phones, tablets, etc.) are another promising use case of smart grid communications, where a user can remotely control his/her appliances, while he/she is away at work or on his/her way home. Although these emerging services can evidently boost the efficiency of the electricity market and the satisfaction of a utility's subscribers, they also introduce new attack surfaces making the grid and utilities vulnerable to financial losses or even physical damages. In this paper, we propose an architecture to secure smart grid communications incorporating an Intrusion Detection System (IDS), composed of different components collaborating with each other to detect price integrity or load alteration attacks in different segments of an Advanced Metering Infrastructure (AMI).**

***Index Terms*—Smart Grid; Smart Home; AMI; IoT; M2M; Security; Intrusion Detection; Price Integrity; Load Alteration.**

I. Introduction

Electric energy and telecommunications are two key ingredients to fuel future economy and smart cities, and the coincidence of the smart grid era with the introduction of fifth-generation mobile networks (5G) can bring about an unprecedented opportunity to offer a myriad of promising mobile applications, notably Advanced Metering Infrastructure (AMI), Demand Response, Vehicle-to-Grid (V2G), and Smart Home [1], [2]. In one hand, 5G is revolutionising mobile communications providing pervasive and ultra-broadband *fiber-like* experience for everyone and everything to consume emerging mobile services, such as three dimensional (3D) or ultra-high-definition video sharing, Machine-Type Communications (MTC) [3], Intelligent Transportation System (ITS) [4], and Smart Home[5], [6]. Apart from expected 10 Gbps peak data rate and accommodating 1000 times more data traffic, hosting more than 50 billion online *things* (e.g., vehicles, sensors, wearable devices, smart home appliances, etc.) is another prime target for 5G, bringing about the true Internet of Things, where tens to hundreds of devices will serve every single citizen [7].

On the other hand, smart grid is transforming today's power network to an intelligent grid by radically changing the way electricity is produced, transmitted, or consumed, supporting two-way power and information flows between the grid and the end-consumers. In particular, smart grid entails the expansion of the legacy control and communications infrastructures, supporting mostly the generation and transmission systems (e.g., Supervisory Control And Data Acquisition (SCADA)) all the way down to the distribution networks and the end consumers' premises in order to connect the whole supply chain of the industry. To this end, AMI is being deployed around the globe to bridge the gap between the utilities and the end users, establishing two-way communication links between them. This will permit efficient and automatic load management or control and the accommodation of promising smart grid solutions, notably Distributed Energy Resources (DER) (e.g., wind, solar, etc.), distributed micro-storage devices, V2G, electric transportation, and Demand Response (DR) programs [8], [9].

Incorporation of AMI, however, increases the attack surface and makes the grid more vulnerable to potential cyberattacks from malicious users to sabotage electricity infrastructure, cause blackouts, or incur financial losses for either the consumers or the utilities [10], [11], [12]. To address these challenges, we need to revisit the existing security measures taking into account not only the information security (i.e., confidentiality, integrity, and availability) but also the impacts of potential security breaches on the stability and security of the power supply [13], [14], [15]. We should also take into consideration that unlike the legacy SCADA systems, which are mostly proprietary-based solutions, AMIs are predominantly Internet-based networks, creating new attack vectors for any malicious user who simply has access to the Internet.

In this paper, we propose a secure network architecture to protect the grid against price integrity or load alteration attacks. The main component of the network architecture is an Intrusion Detection System (IDS) distributed at different parts of the network, including Home Area Network (HAN), Neighbourhood Area Network (NAN), and AMI constructing a collaborative IDS. It can exploit signature-based, Machine Learning (ML), or Statistical techniques to build normal

profiles for communications or for electricity consumption at different parts of the power network. Measuring these attributes in real-time and contrasting them against these normal profiles, the IDS will detect any intrusion in order to take proper security measures to neutralise potential threats.

The rest of this paper is structured as follows. Section II reviews the related work. Section III illustrates smart grid communications, and Section IV highlights their potential vulnerabilities against cyberattacks. Section V presents our proposed IDS to detect any potential intruder and to take appropriate security measure in case an anomaly is detected. Finally, Section VI concludes this paper and draws guidelines for future research.

II. Related Work

Previous research efforts to address security attacks on smart grids can be attributed to three major streams: attacks on SCADA systems, attacks on power market operations, and attacks on AMI and DR programs [16].

Attacks on SCADA systems have widely been investigated. Among others, Liu et al., in [17], study false data injection attacks against state estimation in power systems. In [18], the authors study how attackers can launch a coordinated data injection attack to circumvent the bad data detection algorithms. In [19], Esmalifalak et al. study bad data injection attack and defence mechanisms in electricity markets.

As for the second stream, there are several previous research efforts addressing either Denial-of-Service (DoS) or integrity attacks on the operation of power markets, notably Li and Han, in [20], address a jamming attack against the price signalling, where the attacker keeps jamming the price signal until the demand is adequately altered in a predictive direction. Then, the attacker ceases jamming and lets the market reach a new equilibrium. Capitalizing on the likelihood of short-term price drop (rise), the attacker can make profit by selling (buying) short in the market. Addressing a different type of attack, in [21], Xie et al. investigate integrity attacks on the market operation quantifying potential profits for the attacker as well as the revenue loss for a utility from launching such attacks.

Finally, the last thread of work on smart grid security is dedicated to attacks against AMI and demand-side management (DSM) programmes. Lying in this stream, Ma et al. study the impact of a DoS attack on demand bidding information submitted by consumers to influence the electricity prices towards their own benefit [22]. Tan et al., in [23], research the impact of two specific types of integrity attacks on real-time prices advertised to the smart meters, namely *scaling* and *delay* attacks. In the former the prices are compromised by a scaling factor, while in the latter, they are corrupted by the timing information so that the meters will use the old prices. They show that the stability of a Real-Time Pricing (RTP) programme can seriously be threatened if the adversary reduces the price or provides an old price to over half of the consumers, e.g., by delaying the price signal. Furthermore, Mohsenian-Rad and Leon-Garcia, in [16], address an Internet-based load altering attack on distribution networks and evaluate its impact on overflowing the distribution lines.

As power grid is getting more and more interconnected utilising modern ICT solutions, intrusion detection becomes an important concern for the grid's safety and stability. An experiment was conducted by US Department of Energy in March 2007, where an attack is remotely launched against the control system of a generator destabilising and forcing it to shake and smoke [24]. In general, there are three main techniques for IDS, namely signature-based, anomaly-based and specification-based. The first approach looks for known patterns of malicious behaviour using a database of predefined signatures. The second approach is based on constructing a profile from normal behaviour using ML or statistical algorithms and detecting any deviation from this normal profile using statistical measures. Finally, the last approach is based on setting logical rules and specifications [25]. The authors, in [25], study the threats targeting AMIs by highlighting practical needs for an IDS. Furthermore, the authors in [26] discuss the security requirements and vulnerabilities of AMI and propose an IDS for the NAN (Fig. 3). Zhang et al. in [27] propose a distributed IDS for AMIs incorporating Support Vector Machine (SVM) and Artificial Immune System (AIS).

However, despite these studies, our knowledge about mechanisms to detect integrity attacks on price signal and appropriate measures to counteract against such attacks is far from being complete.

III. Smart Grid Communications

A. Demand Response and Real-Time Pricing

Economists have long advocated that exposing consumers to the real-time price fluctuations in the wholesale electricity market can considerably enhance the market's economic efficiency [28]. To this end, RTP programmes advertise real-time prices to the end-users and monitor their instantaneous consumption [29], [2]. This entails the expansion of the legacy control and communications infrastructures supporting mostly the generation and transmission systems (e.g., SCADA), all the way down to the distribution networks and consumers' premises in order to connect the whole supply chain of the industry. To this end, AMI [25] is being deployed around the globe to bridge the gap between the utility companies and the end users, establishing two-way communication links between the distribution companies and the consumers' facilities. This will permit the grid to efficiently match the supply and demand and to accommodation promising technologies such as DERs (e.g., wind, solar, etc.), distributed micro-storage devices, electric transportation, and DR programmes [8], [9].

B. M2M Communications and IoT Solutions for Smart Grid

Capitalising on Machine-to-Machine (M2M) communications and Internet-of-Things (IoT) solutions, smart grid is transforming legacy power systems to an intelligent network. It is connecting stakeholders across the whole supply chain of the electricity industry spanning from generation units and substations to electric utilities and end consumers enabling the grid to

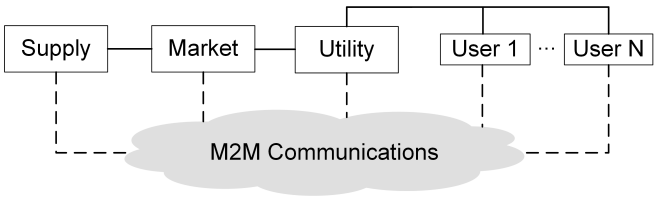

Fig. 1. Smart grid; solid and dashed lines depict the power and information flow, respectively.

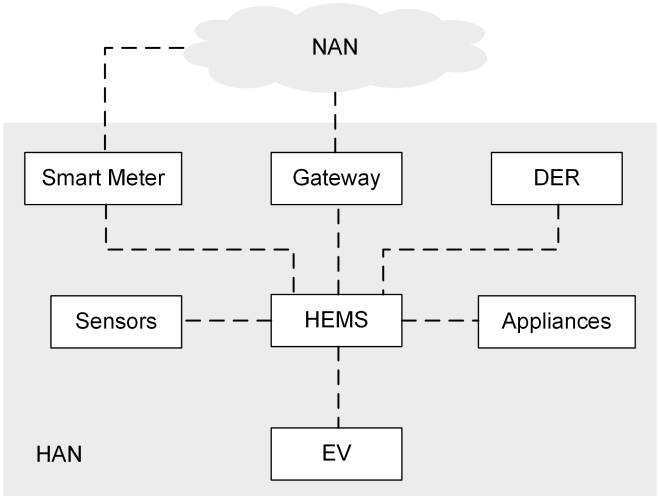

Fig. 2. Home Area Network (HAN)

operate more efficiently and more reliably [9], [30] (see Fig. 1). M2M communications and IoT solutions are to connect smart buildings and smart homes as well as their appliances through a Smart Home Energy Management System (HEMS), serving as a gateway, to a utility company's command and control centre at the power distribution network level [31] as illustrated by Fig. 2. Two-way M2M communications are being established between households and electric utilities to help better utilise electricity infrastructure supporting smart metering, demand response, and the integration of distributed energy resources into the grid, among others. Utilities will be able to set a more dynamic time-dependent or even demand-dependent tariff, e.g., Time-of-Use (ToU), Critical Peak Pricing (CPP), RTP, etc., to influence consumers' consumption habit. They might monitor total demand in real-time and based on demand and supply variations, alter short-term retail prices to either encourage or discourage users to consume energy in a given interval. On the other hand, smart appliances can receive price information in or close to real-time and based on it and the user's preferences, can choose optimal intervals for their operations so as to minimise the energy cost of the household without compromising the satisfaction level of inhabitants [32].

An AMI consists of a WAN connecting several NANs (Fig. 3) to a utility company where the consumers in each neighbourhood are connected through a *collector* that aggregates the metering or demand bidding information from its HAN clients

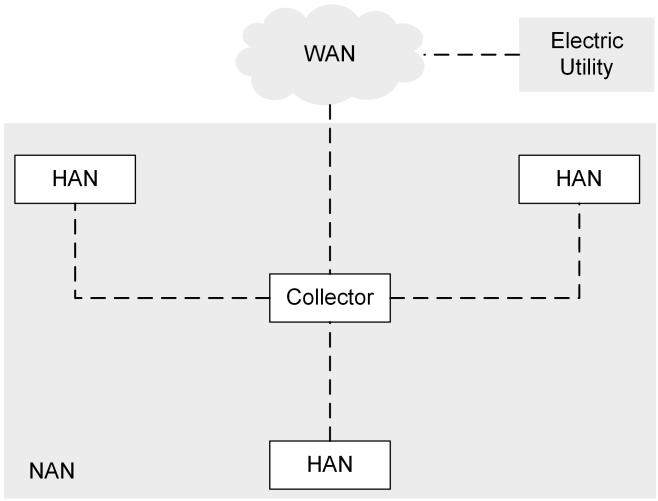

Fig. 3. Neighbourhood Area Network (NAN)

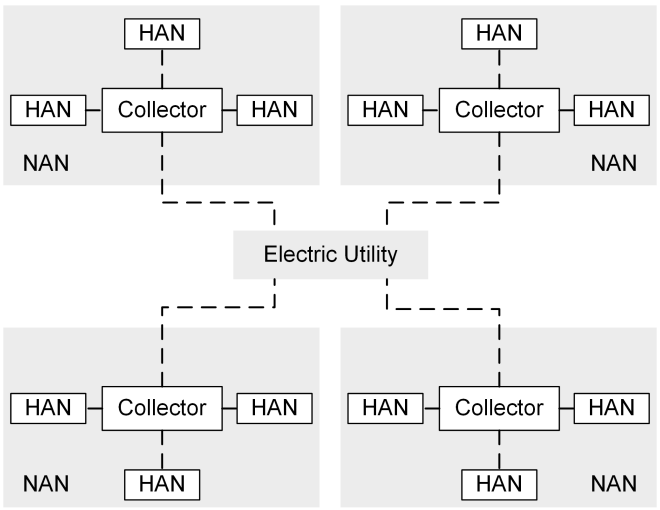

Fig. 4. Advanced Metering Infrastructure (AMI)

[33] (see Fig. 4). In order to have a common terminology, throughout this paper, we refer to those communication links that connect the collectors to the HANs as *access* links, while referring to the links connecting the collectors to the WAN as *backhaul* links.

C. Smart Metering

Advanced Metering Infrastructure (AMI) is the underpinning communication infrastructure for smart grid. Apart from cost efficient automatic metre reading, it allows carrying critical control signals, as well as billing information, from the control centre to the consumers and more granular interval metering information (e.g., measured every 15 min, half-hourly, hourly, etc.) in the reverse direction. This real-time monitoring of the energy consumption can help utilities stabilise the voltage and frequency throughout the grid to ensure the necessary power quality at the consumers premises. It further allows them to detect any unauthorised usage in a timely and

TABLE I
COMPARISON OF DIFFERENT APPROACHES FOR INTRUSION DETECTION

	Signature	**ML**	**Statistical**
Complexity	Low	Moderate-High	Low-Moderate
Privacy issues	Yes	No	No
Accuracy	High	Moderate	Moderate
Unknown attacks	No	Yes	Yes

efficient manner. On the other hand, this interval metering along with real-time interactions between utilities and their subscribed users can increase the energy efficiency awareness of the users and help implement energy conservation policies, in case of supply shortage.

AMI can help the adoption of distributed micro storage (e.g., using batteries) [34] to store energy when there is an excess of supply and consume it or even sell it back to the grid when there is a supply deficit. The users may also harvest energy from renewable sources such as wind or solar, run a micro CHP unit, or even use their EVs as a mobile storage unit for electricity to more actively participate in demand response programmes (i.e., V2G) [35], [36], [37]. In this regard, it is essential to integrate these renewable resources taking into consideration the intermittent nature of these resources [38] and to develop charging/discharging strategies for distributed storage units or for EVs so as to assure the grid's stability.

IV. SECURE NETWORK ARCHITECTURE

The introduction of AMI, however, makes the grid easily accessible and vulnerable to potential cyberattacks from malicious users. For instance, an attacker may launch a Denial of Service (DoS) or a false data injection attack against the supervisory control and data acquisition (SCADA) system or against different parts of AMI, including HAN, NAN, and WAN either to mislead the controller and destabilise the grid or to cause physical damage or financial losses. To address these security concerns, in this section, we describe our secure network solution with an IDS distributed in different parts of the information network supporting a smart grid.

An intruder may attack different parts of an AMI, depending on her resource availability. For instance, she might have limited resources and so target only a limited number of links or specific part of the AMI. That is, the attack may target only the access links of a NAN or backhaul links or even a HAN. Serving to a DR program (e.g., RTP, CPP, etc.), these access links carry the pricing information from the utility company to HANs, while carrying back the *quantity* of electricity consumed by the households. Providing HAN, NAN, or WAN with an IDS can help improve system security by detecting intrusions.

An IDS is responsible for detecting any security breach. The signature-based techniques rely on known patterns in the communication packets based on the first few bytes of the packet payload and are mostly used by propriety based solutions, where an updated list of signatures for any known security attack is maintained, and the signature of a given packet is always contrasted against these signatures. However, these techniques suffer from two major drawbacks: (i) they might violate user privacy due to checking packet payloads; and (ii) they are vulnerable against new attacks since they lack any signature in the database. Table I summarises the main techniques for intrusion detection, highlighting their strengths and shortcomings.

To alleviate these problems, statistical and ML based learning algorithms are increasingly incorporated by IDSs, where a set of training data is used for training a learning algorithm. A trained statistical algorithm builds a normal profile for the features and contrasts any given example against this normal profile to see whether it represents an anomaly or not. On the other hand, an ML algorithm requires training examples from both normal and compromised behaviour and classifies training examples into classes using supervised or unsupervised learning algorithms. These techniques can also be exploited for learning the statistics of the voltage or frequency of the AC power at different distribution buses to detect any anomaly in the system. For instance, if the attacker tries to run many high consumption loads at the same time, it can be detected by monitoring the frequency of the system, which is normally 50 Hz or 60 Hz depending on the region. Any drop from this base frequency implies excess in demand and consequent deterioration in the power quality which should be compensated by bringing enough capacity on line or isolating the attacked region from the grid. Therefore, the IDS monitors the demand and supply balance in real time and checks if there is any sudden increase (drop) in the demand, which in turn implies the existence of price or load alteration attack in the AMI.

As illustrated by Figs. 5, 6, and 7, different IDS systems can be designed for different parts of an AMI, where these components can collaborate for further performance improvement. For instance, when an anomaly is detected in one part of the network, the associated IDS can report it to other IDSs in order to take appropriate actions at different layers of AMI (i.e., HAN, NAN, and WAN). As smart grid paves the way towards a competitive electricity market, price integrity attacks can seriously harm the demand and supply balance, leading to grid instability which may impact the economy and life by causing blackouts across a large geographic region or catastrophic consequences of physical damages to different parts of the grid.

V. CONCLUSION

As a concrete example of IoT, smart grid is about to attract a considerable market for 5G, helping electric utilities better manage electricity supply and demand and residential consumers better manage their energy consumption and expenditure. The smart grid will not only be reliant on mature M2M and IoT technologies as the enabler to support effective remote management and demand response, but will also require new approaches to ensure system security as the grid is increasingly connected to the Internet. However, the introduction of this supporting information network introduces new attack vectors raising security concerns for the grid. In this paper, we

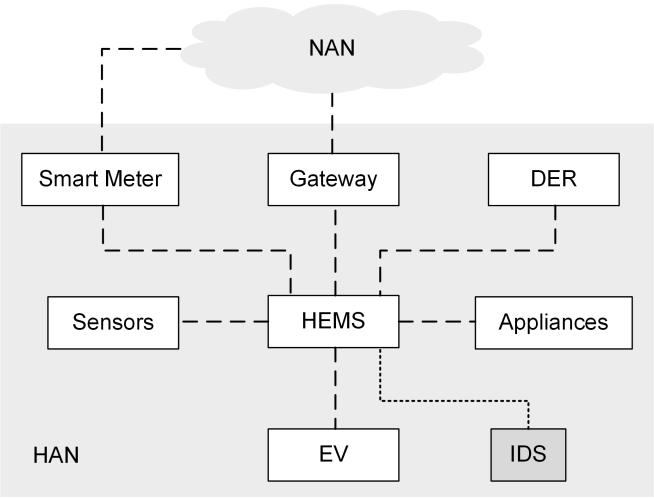

Fig. 5. HAN with IDS

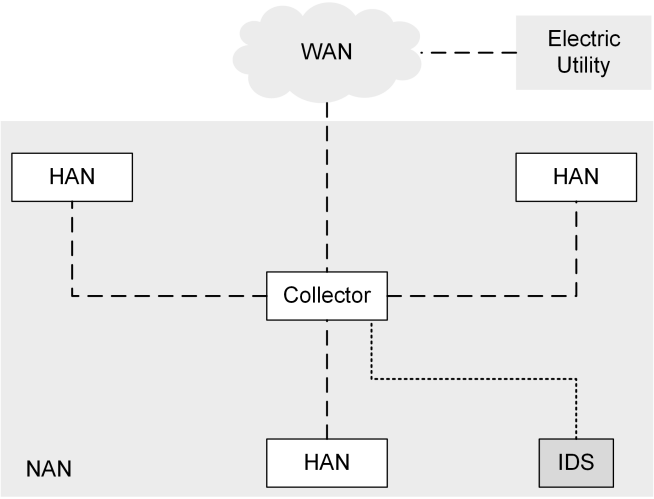

Fig. 6. NAN with IDS

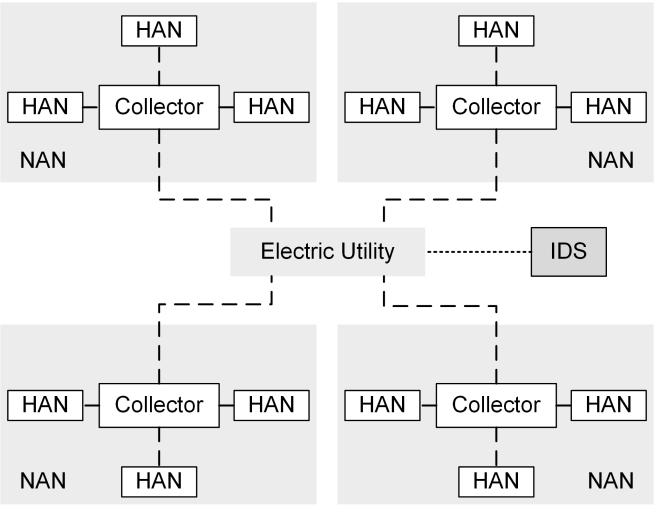

Fig. 7. AMI with IDS

discussed how incorporation of an IDS can help improve these security concerns and proposed a secure network architecture for AMI to detect attacks against the integrity of price or consumption information exchanged between a utility and its subscribed users. For future work, we plan to design and implement an IDS distributed in different parts of the AMI in order to detect DoS attacks and false price injection attacks on demand response programmes.

REFERENCES

[1] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid — the new and improved power grid: A survey," *IEEE Communications Surveys Tutorials*, vol. 14, no. 4, pp. 944–980, Fourth 2012.

[2] F. B. Saghezchi, F. B. Saghezchi, A. Nascimento, and J. Rodriguez, "Game-theoretic based scheduling for demand-side management in 5G smart grids," in *Computers and Communication (ISCC), 2015 IEEE Symposium on*, July 2015, pp. 8–12.

[3] F. B. Saghezchi, J. Rodriguez, S. Mumtaz, A. Radwan, W. C. Y. Lee, B. Ai, M. T. Islam, S. Akl, and A.-E. M. Taha, *Drivers for 5G*. John Wiley & Sons, Ltd, 2015, pp. 1–27. [Online]. Available: http://dx.doi.org/10.1002/9781118867464.ch1

[4] V. Sucasas, G. Mantas, F. B. Saghezchi, A. Radwan, and J. Rodriguez, "An autonomous privacy-preserving authentication scheme for intelligent transportation systems," *Computers & Security*, vol. 60, pp. 193 – 205, 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404816300463

[5] G. Mantas, D. Lymberopoulos, and N. Komninos, "Integrity mechanism for ehealth tele-monitoring system in smart home environment," in *2009 Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, Sept 2009, pp. 3509–3512.

[6] ——, "Security in smart home environment," *Wireless Technologies for Ambient Assisted Living and Healthcare: Systems and Applications*, pp. 170–191, 2010.

[7] F. B. Saghezchi, A. Radwan, and J. Rodriguez, "Energy-aware relay selection in cooperative wireless networks: An assignment game approach," *Ad Hoc Networks*, pp. –, 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1570870516303286

[8] A. Ipakchi and F. Albuyeh, "Grid of the future," *Power and Energy Magazine, IEEE*, vol. 7, no. 2, pp. 52–62, March 2009.

[9] H. Farhangi, "The path of the smart grid," *Power and Energy Magazine, IEEE*, vol. 8, no. 1, pp. 18–28, January 2010.

[10] K. Moslehi and R. Kumar, "A reliability perspective of the smart grid," *Smart Grid, IEEE Transactions on*, vol. 1, no. 1, pp. 57–64, June 2010.

[11] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," *Communications Surveys Tutorials, IEEE*, vol. 14, no. 4, pp. 998–1010, Fourth 2012.

[12] A. Metke and R. Ekl, "Security technology for smart grid networks," *Smart Grid, IEEE Transactions on*, vol. 1, no. 1, pp. 99–107, June 2010.

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

[14] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-physical system security for the electric power grid," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 210–224, Jan 2012.

[15] C.-W. Ten, G. Manimaran, and C.-C. Liu, "Cybersecurity for critical infrastructures: Attack and defense modeling," *Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on*, vol. 40, no. 4, pp. 853–865, July 2010.

[16] A.-H. Mohsenian-Rad and A. Leon-Garcia, "Distributed internet-based load altering attacks against smart power grids," *Smart Grid, IEEE Transactions on*, vol. 2, no. 4, pp. 667–674, Dec 2011.

[17] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, pp. 13:1–13:33, Jun. 2011.

[18] S. Cui, Z. Han, S. Kar, T. Kim, H. Poor, and A. Tajer, "Coordinated data-injection attack and detection in the smart grid: A detailed look at enriching detection solutions," *Signal Processing Magazine, IEEE*, vol. 29, no. 5, pp. 106–115, Sept 2012.

[19] M. Esmalifalak, G. Shi, Z. Han, and L. Song, "Bad data injection attack and defense in electricity market using game theory study," *Smart Grid, IEEE Transactions on*, vol. 4, no. 1, pp. 160–169, March 2013.

[20] H. Li and Z. Han, "Manipulating the electricity power market via jamming the price signaling in smart grid," in *GLOBECOM Workshops (GC Wkshps), 2011 IEEE*, Dec 2011, pp. 1168–1172.

[21] L. Xie, Y. Mo, and B. Sinopoli, "Integrity data attacks in power market operations," *Smart Grid, IEEE Transactions on*, vol. 2, no. 4, pp. 659–666, Dec 2011.

[22] C. Ma, D. Yau, and N. Rao, "Scalable solutions of markov games for smart-grid infrastructure protection," *Smart Grid, IEEE Transactions on*, vol. 4, no. 1, pp. 47–55, March 2013.

[23] R. Tan, V. Badrinath Krishna, D. K. Yau, and Z. Kalbarczyk, "Impact of integrity attacks on real-time pricing in smart grids," in *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, ser. CCS '13. New York, NY, USA: ACM, 2013, pp. 439–450.

[24] C.-C. Liu, A. Stefanov, J. Hong, and P. Panciatici, "Intruders in the grid," *Power and Energy Magazine, IEEE*, vol. 10, no. 1, pp. 58–66, Jan 2012.

[25] R. Berthier, W. Sanders, and H. Khurana, "Intrusion detection for advanced metering infrastructures: Requirements and architectural directions," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, Oct 2010, pp. 350–355.

[26] N. Beigi Mohammadi, J. Misic, V. B. Misic, and H. Khazaei, "A framework for intrusion detection system in advanced metering infrastructure," *Security and Communication Networks*, vol. 7, no. 1, pp. 195–205, 2014. [Online]. Available: http://dx.doi.org/10.1002/sec.690

[27] Y. Zhang, L. Wang, W. Sun, R. Green, and M. Alam, "Distributed intrusion detection system in a multi-layer network architecture of smart grids," *Smart Grid, IEEE Transactions on*, vol. 2, no. 4, pp. 796–808, Dec 2011.

[28] S. Borenstein, M. Jaske, and A. Ros, "Dynamic pricing, advanced metering, and demand response in electricity markets," pp. 4136–45, March 2002. [Online]. Available: http://repositories.cdlib.org/ucei/csem/CSEMWP-105/

[29] F. Saghezchi, F. Saghezchi, A. Nascimento, and J. Rodriguez, "Game theory and pricing strategies for demand-side management in the smart grid," in *Communication Systems, Networks Digital Signal Processing (CSNDSP), 2014 9th International Symposium on*, July 2014, pp. 883–887.

[30] S. Amin and B. Wollenberg, "Toward a smart grid: power delivery for the 21st century," *Power and Energy Magazine, IEEE*, vol. 3, no. 5, pp. 34–41, Sept 2005.

[31] D. Niyato, L. Xiao, and P. Wang, "Machine-to-machine communications for home energy management system in smart grid," *Communications Magazine, IEEE*, vol. 49, no. 4, pp. 53–59, April 2011.

[32] A.-H. Mohsenian-Rad and A. Leon-Garcia, "Optimal residential load control with price prediction in real-time electricity pricing environments," *Smart Grid, IEEE Transactions on*, vol. 1, no. 2, pp. 120–133, Sept 2010.

[33] F. Bouhafs, M. Mackay, and M. Merabti, "Links to the future: Communication requirements and challenges in the smart grid," *Power and Energy Magazine, IEEE*, vol. 10, no. 1, pp. 24–32, Jan 2012.

[34] I. Atzeni, L. Ordonez, G. Scutari, D. Palomar, and J. Fonollosa, "Demand-side management via distributed energy generation and storage optimization," *Smart Grid, IEEE Transactions on*, vol. 4, no. 2, pp. 866–876, June 2013.

[35] J. Lopes, F. Soares, and P. Almeida, "Integration of electric vehicles in the electric power system," *Proceedings of the IEEE*, vol. 99, no. 1, pp. 168–183, Jan 2011.

[36] Z. Fan, "A distributed demand response algorithm and its application to phev charging in smart grids," *Smart Grid, IEEE Transactions on*, vol. 3, no. 3, pp. 1280–1290, Sept 2012.

[37] W. Kempton and J. Tomić, "Vehicle-to-grid power fundamentals: Calculating capacity and net revenue," *Journal of Power Sources*, vol. 144, no. 1, pp. 268 – 279, 2005. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0378775305000352

[38] A. Roscoe and G. Ault, "Supporting high penetrations of renewable generation via implementation of real-time electricity pricing and demand response," *Renewable Power Generation, IET*, vol. 4, no. 4, pp. 369–382, July 2010.