Cybersecurity of Electric Vehicle Smart Charging Management Systems

Narayan Bhusal, *Student Member, IEEE*, Mukesh Gautam, *Student Member, IEEE*,
and Mohammed Benidris, *Member, IEEE*
Department of Electrical & Biomedical Engineering, University of Nevada, Reno, NV
(emails: {bhusalnarayan62, mukesh.gautam}@nevada.unr.edu, and mbenidris@unr.edu)

2020 52nd North American Power Symposium (NAPS) | 978-1-7281-8192-9/21/$31.00 ©2021 IEEE | DOI: 10.1109/NAPS50074.2021.9449758

***Abstract*—In concept, a smart charging management system (SCMS) optimizes the charging of plug-in vehicles (PEVs) and provides various grid services including voltage control, frequency regulation, peak shaving, renewable energy integration support, spinning reserve, and emergency demand response. These functionalities largely depend upon data collected from various entities such as PEVs, electric vehicle supply equipment (EVSE), service providers, and utilities. SCMS can be susceptible to both cyber and physical threats (e.g. man-in-the-middle attack, data intrigued attack, denial of charging, physical-attack) due to interactions of and interdependencies between cyber and physical components. Cyber-physical threats through highly connected malware vectors raise various concerns including public safety hazards to vehicle operators and those in the immediate vicinity as well as disruptions to electric grid operations. This paper describes the concept of SCMS and provides a comprehensive review of cybersecurity aspects of EVSEs and SCMSs with their possible impacts on the power grid and society. It also contributes to the development of cybersecurity measures to the SCMSs. Various functions of SCMS are reviewed in detail including peak shaving, demand charge reduction, frequency regulation, spinning reserve, renewable integration support, distribution congestion management, reactive power compensation, and emergency demand response with unidirectional PEVs charging. Also, a critical literature survey on current practices of SCMS cybersecurity is provided to explore major impacts and challenges of cyber-physical attacks and to identify research gaps and vulneraibilities in currently available SCMSs technologies.**

***Index Terms*—Cybersecurity, cyber-physical threats, PEV and grid service, and smart charging management systems.**

I. INTRODUCTION

Penetration of plug-in electric vehicles (PEVs) into power grid is proliferating worldwide. With this increased penetration, optimum management of PEV charging is becoming an important factor for PEV owners, service providers, utilities, and power system operation. For proper management of PEV loads, a smart charging management system (SCMS) that is capable to optimize charging of PEVs at both public charging and residential charging stations is necessary. Apart from shifting loads to more desirable times for the grid, the SCMS can contribute in grid services such as voltage and frequency support and seamless integration of renewable energy sources. To provide multiple services, SCMS should properly monitor and control PEVs that are connected to electric vehicle supply equipments (EVSEs) at both individual charging locations and congregated charging stations. In this context, monitoring and control of PEVs and EVSEs necessitate the real-time data communication with SCMS and the grid. Consequently, SCMS can be susceptible to several cyber-physical attack vectors. Therefore, the cyber-physical security of SCMS should be properly addressed to ensure that the system is hardened against attacks and be able to detect and mitigate attacks on the grid, charging networks, and customers in real-time.

Numerous studies have focused on the technical aspects of PEV integration and their impacts on the smart grid. Several technical aspects have been studied in [1]–[5] including charging strategies, energy management, power losses, grid interface technologies, renewable energy integration support, power system reliability, voltage and frequency regulation, and regulation of PEVs in electricity markets.

Although cybersecurity of the smart grid has been amply addressed in the literature, cybersecurity aspects of PEVs, EVSEs, and SCMS have not been fully addressed. In [6], a comprehensive review of the detection algorithm for false data injection attacks (FDIAs) in smart grids has been provided. FDIA detection algorithm has been divided into model-based (based on the dynamic models of systems) approach and data-driven (based on the utilization of available smart grid data) approaches. State-of-the-art approaches for FDIA against smart grids from different perspectives have been provided in [7]. Also, [7] explores the theoretical basis of FDIA, the physical and economic impacts of FDIA, basic defense strategies, and future research directions. Both [6] and [7] provide a rich source of references for further exploration of the cybersecurity of smart grids. Although the cybersecurity of SCMS possesses some similarities with that of smart grids, there are some fundamental differences. More research attention is needed to identify these differences and to develop cybersecurity measures for SCMS.

Due to interactions of and interdependencies between cyber and physical components of SCMSs, they can be susceptible to cyber-physical threats. Therefore, as a stepping stone toward the development of cybersecurity measures to SCMS, this paper describes the concept of SCMS and provides a comprehensive review of cybersecurity concerns of EVSE and SCMS along with possible mitigation measures. Various functions of SCMS are described in detail including peak shaving, demand charge reduction, frequency regulation, spinning reserve, renewable integration support, distribution congestion management, reactive power compensation, and emergency demand response. A survey of the existing literature on cyber-

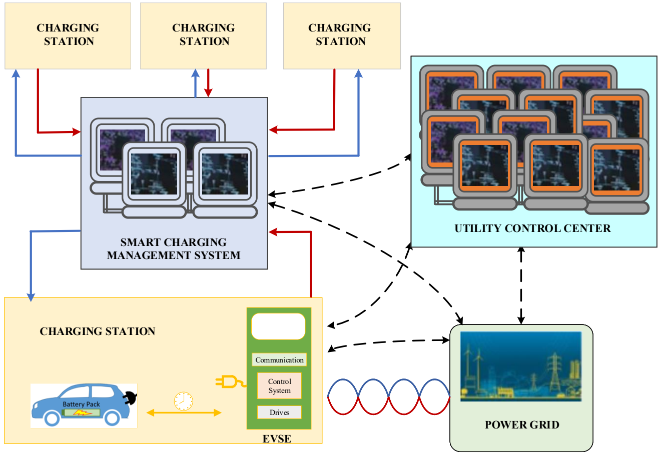

Fig. 1. Architecture of Smart Charging Management System

security of SCMS is also provided. Furthermore, major cyber-physical attacks, impact of these attacks on SCMS, and major challenges to deal with these attacks are identified. Research gaps and vulnerabilities associated with current commercially available SCMS technologies are also highlighted.

The rest of the paper is organized as follows. Section II explains the concept and architecture of SCMS. Section III explores potential grid services that PEVs can provide via SCMS. Section IV reviews existing literature on cybersecurity of PEVs, EVSEs, and SCMSs. Section V discusses the major cyber-physical threats in SCMS. Section VI presents the research gaps and vulnerabilities associated with commercially available SCMS technologies. Finally section VII provides concluding remarks.

II. Concept and Architecture of Smart Charging Management System

SCMS is a system that provides various benefits to PEV owners, charging network operators, energy service providers, and flexibility to the electric grid operators through the utilization of flexible PEV loads. Apart from optimizing the charging of PEV loads, SCMS also provides various grid services such as peak shaving, voltage control, frequency regulation, renewable integration support, demand-side management, demand charge reduction, loss reduction, and emergency demand response, to name a few. Fig. 1 provides a typical architecture for SCMS to describe its concept of operation [1], [3].

We can see from Fig. 1 that SCMS communicates with charging stations and its EVSEs, electric power grid, and electric utility to manage the charging of PEVs and to provide various grid services. The charging stations in the figure could be individual charging station or congregated charging stations at workplace, multi-unit dwelling, and retail-establishment. Each charging station is equipped with one or more EVSEs that can communicate with SCMS and the power grid for controlling the charging process and to provide various real-time measurements. SCMS receives charging requests from PEVs and EVSEs and electricity price signals and various grid service requests from utility control centers. The real-time and historical data from EVSE are processed and analyzed at SCMS and utilized to make demand forecast, planning, and investment decisions. Section III provides a brief description of potential grid services that PEVs can provide via SCMS. Also, providing cyber-physical security measures to detect, identify, control, and mitigate these threats is an important part of SCMSs.

III. Potential Grid Services Provided by PEVs via SCMS

There are several challenges and complications associated with vehicle to grid (V2G) integration [4]. Apart from that, there is still a big question on the economic feasibility of V2G integration [8]–[10]. In other words, V2G technology is not something that will come into practice anytime soon. Therefore, in this paper, only grid services that are possible from the flexibility of charging PEV loads at different times and rates are considered. In other words, this paper describes how PEV loads can be utilized to provide peak shaving, reactive power compensation, frequency regulation, renewable energy integration support, etc. through controlling charging time and rates without the use of V2G service. This section describes in detail the grid services provided by SCMS utilizing PEV loads.

A. Peak Shaving

Peak shaving refers to the reduction of peak power demand of the power grid. Peak shaving can be achieved by controlled charging through adjusting PEV charging times and rates. Very few or no PEVs are charged (or charged at a very low rate) during the time of peak power demand—charging of low-priority PEVs can be shifted to off-peak hours. Peak shaving can be implemented using SCMS algorithms. SCMS uses different pricing schemes for different times of the day (imposing high prices to charge the PEVs during the period of high power demand and imposing low prices during the period of low power demand). Numerous literature have studied the peak shaving scheme using PEVs [4], [11]–[14].

B. Ancillary Service

Frequency regulation: frequency drop usually occurs when the generation deficit occurs in the power system. Electric utilities constantly balance the supply and demand to keep system frequency at its nominal value. When a large number of PEVs are charged in an uncoordinated manner, it can disrupt the balance between generation and consumption resulting in disruption in system frequency. Therefore, providing the balance between power consumption and generation through flexible loads is critical if the generation cannot ramp up/down within a short period of time. The direct real-time control of the charging of PEVs can provide the power balance and support to regulate the frequency. The charging rate of PEVs is regulated up and down to meet the preference operation point to keep the frequency within the desired range [15].

Spinning reserve: this service can be achieved using PEVs by lowering the charging rate during the time of higher power demand [16]. A proper compensation scheme should be provided to PEVs for being agreed to provide these services.

C. Support Renewable Energy Integration

The ability to support renewable energy integration into the electric power grid is one of important transformative impacts of PEVs. Charging PEVs at higher power production mitigates the problem of photovoltaic/wind generator over-generation. The SCMS performs this by managing to charge a large number of PEV loads when there is peak power production from renewable energy sources (e.g. photovoltaic and wind). The integration of renewable sources can be achieved via real-time electricity pricing and demand response programs [17]. Because of the coordination between charging of PEVs and renewable generation, charging of PEVs and the excess generation of renewable sources do not need to be curtailed. Several approaches have been presented to demonstrate the ways of supporting renewable integration via PEVs [18]–[20].

D. Reactive Power Compensation

It is highly essential to understand the reactive power behavior and capability of PEVs for reactive power compensation. The reactive power behavior of PEVs has been studied in [21] which has shown that all of the studied PEVs have a power factor above 0.99. This indicates that the reactive power support can be provided by injecting reactive power during the time of charging (i.e. setting PEV's charger to provide capacitive power factor) [22], [23]. However, this comes with the cost of increased apparent power rating resulting in more active power consumption. For example, to obtain 0.95 capacitive power factor, the apparent power rating of a PEV becomes $105.3\%(1/0.95)$. This 5.3% increase in PEV charger can cause up to $\sqrt{1.053^2 - 1} = 32.9\%$ increase in active power consumption. For more work on reactive power supporting capability of PEVs, refer [22]–[25].

E. Emergency Demand Response

Emergency demand response is implemented in the utility control center during unexpected contingencies. These contingencies may disrupt the balance between generation and consumption. As PEVs are flexible loads, based on the command signal from the control center, they can be stopped from charging in response to emergency demand response [26], [27].

IV. Literature Survey on Cybersecurity of SCMS

Cyber-physical threats such as man-in-the-middle attack, data integrity attack, payment fraud, privacy/tracking concerns, intentional charging or discharging, denial of service attack, malware injection with the help of PEVs, and rapid cycling of a large number of PEVs are potential attacks on SCMS and its integrated components [28]. These cyber-physical threats result in various consequences: public safety hazard to the vehicle operators and those in the immediate vicinity and initiating and exacerbating electric grid disruption. Although a considerable amount of work has been proposed for the cybersecurity of the smart grid, cybersecurity of SCMS has received very little attention. Some of the literature that make an important contribution toward the cybersecurity of PEVs are as follows.

Authors of [29] have proposed a control-oriented approach to detect cyber-attacks that can affect PEV batteries during charging. Two algorithms have been proposed to detect cyber-attacks during the charging as follows: (a) static detector utilizing measured variables and (b) dynamic detector which utilizes the dynamics as well as the measurement variables. The results demonstrated in this study show that the performance of the dynamic detector is better than the static detector.

Authors of [30] have explored the cybersecurity measures of PEVs in the smart grid with a review on some of the state-of-the-art algorithms that have been used to detect cyber-attacks. The impact on operational cost, net power demand, and charging/discharging algorithms of data attacks on a PEV smart parking lot has been studied. Two intrusion detection approaches (model-based and signal-based with specific application to PEV data attack) have also been examined in [30].

In [31], vulnerability analysis and risk assessment of cyber-physical attacks on PEVs charging networks have been described. In [32], a cyber-physical interaction of various components of EVSE is provided with the classification of associated vulnerabilities and cyber-physical threats. Cybersecurity of the battery management system of PEVs has been considered in [33] through a neural network-based approach that estimates state of charge (SOC) of a battery under cyber-attacks. However, the work in [33] does not address the cybersecurity concern from the perspective of the charging management system. Although the aforementioned literature studied some insights into the cybersecurity-related concerns, there are still several areas of charging management systems that are unexplored; therefore, further research is needed.

V. Major Cyber-physical Attacks in SCMS

SCMSs and EVSEs are connected to PEVs, building energy management systems, electricity grid, telecommunication networks, billing systems, and utility control centers. These can cause disruption of electricity load management for buildings or the electric grid or damage to PEV batteries. The accessibility and power consumption of an EVSE system is a potential mechanism for disrupting the power of a building or distributing electricity to a specific area. In addition, if a hacker installs persistent malware in EVSE and propagates it to SCMS and power grid, it will exacerbate the disruption even further. In this context, SCMS and its integrated network will not be able to meet confidentiality, integrity, and availability (CIA) requirement. The major cyber-physical attacks in SCMS and its associated network are described as follows.

A. False Data Injection Attack

PEV charging/discharging data throughout the grid are collected with the help of smart measuring devices connected to the EVSEs, installed at charging stations. All of these grid services that SCMS provides depend upon the charging/discharging request received from PEVs and measurements provided by EVSEs. Data collected from SCMS and its integrated system are analyzed by utilities to determine the optimal dispatch of generators, demand-side management, demand forecast, and reliability and stability analysis of the system, to name a few. As PEV charging/discharging data have large use, their accurate measurement, processing, and analysis are very important. FDIA is one of the crucial attacks that can cause several damages to the PEVs, EVSE, SCMS, and even to the grid. FDIA aims at manipulating SCMS and its integrated system-related various data such as [30]: (a) energy request, (b) energy usage, (c) price signal from a utility, (d) demand response bidding from EVSE, (e) demand response needs from the utility, (f) event messages, (g) PEV ID, (h) premise location ID, (i) utility ID, and (j) customer ID, communicated between PEVs, EVSE, and SCMS. FDIA can cause overcharging to batteries and several damages to PEVs and the grid.

Although little attention has been given to detect data attacks on SCMS, the various techniques that have been applied to identify FDIA in power systems could motivate the research on detection of FDIA in SCMS. Authors of [6], [7] have provided a comprehensive review of FDIA and their detection from various perspectives for the smart grid. Both [6] and [7] provide a rich source of references for further exploration of the cybersecurity of smart grids. References [34]–[39] provide resources to develop appropriate cybersecurity measures for SCMS.

B. *Man-in-the-Middle Attack*

In Man-in-the-Middle (MITM) attack, an attacker intercepts and manipulates data that are communicated between various parties [40]. Fig. 2 shows a basic block diagram of MITM attack. In the context of SCMS, an attacker can intercept communication between PEVs, EVSEs, and SCMS and modify, drop, and falsify data transmission. When attackers insert between PEVs, EVSEs, and SCMSs, they can create tracking issues, payment fraud (e.g. the charging cycle does not last full amount of time paid for, the charger is spoofed into providing free service), and violate other personal privacy [28]. Through MITM, an attacker can also cause intentional overcharging/discharging of PEV batteries causing damage to PEV and its batteries and taking the PEVs out of service or degrading range. MITM attacks can also overload distribution transformers and sometime power grid frequency and voltage stability disturbances leading to power grid failure via rapid cycling of a large number of PEV loads [41]. Apart from that, compromised EVSEs and PEVs can cause several personal safety concerns.

Authors of [29] have provided some studies on impacts of overcharging attacks on PEV batteries; however, there is still a huge research gap for MITM attacks in SCMSs. Work proposed in [42]–[48] could be adopted to develop detection, identification, defense, and mitigation measures for MITM attacks in SCMSs.

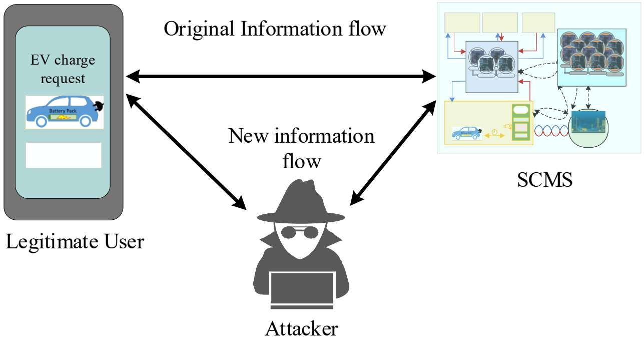

Fig. 2. Basic structure of Man in the middle attack

C. *Denial-of-Service Attack*

A denial-of-service attack causes the unavailability of network service to intended users as a result of an attacker's action to jam and overload the network [49]. In the case of SCMS and its entities, attackers can attack servers and block valid requests from PEVs resulting in rejecting requests from legitimate PEV users. Due to denial-of-charge (a type of DoS in SCMSs), important emergency vehicles (e.g., ambulance, firetrucks, and security vehicles) may be denied from charging resulting in the detrimental effects on the various emergency services and society.

Although very few works have been proposed for DoS attack in SCMS, authors of [29] have provided some insightful studies on the denial-of-charging attacks in which measurements based static attack detection and measurements and system dynamics based dynamic attack detection algorithms have been proposed. The work proposed in [50]–[52] could be used as a basis to develop DoS detection, defense, and mitigation system for SCMSs.

D. *Malware Injection via EVSEs*

Due to the publicly available nature of EVSEs, especially, at public charging stations, EVSEs are susceptible to malware injections. The malware injected EVSEs can cause theft of several sensitive information such as payment information (debit/credit card information), personal information, charging time, payment amounts, etc. [41]. The malware injected EVSE not only affects individual EVSEs, but it also has a probability to propagate to a network of EVSEs. The malware injected in EVSEs can also pass to PEVs, SCMS, and the power grids resulting in detrimental effect to all the stakeholders [28]. The best way to deal with these attacks is to provide cybersecurity-related testing and assessment while installing EVSEs.

E. *Physical Attack*

Physical attacks to EVSEs or PEVs can compromise the service provided by EVSEs and PEVs. A compromised PEV or EVSE is a potential personal safety concern and grid network concern. The coordinated charging events could cause widespread disruption of the power grid [41].

VI. Research Gaps and Associated Vulnerabilities of Commercially Available SCMS Technologies

This section describes the research gaps and associated vulnerabilities of currently available technologies of various entities of SCMSs such as PEVs, EVSEs, and smart meters. The research gaps and vulnerabilities identified by DOE/DHS/DOT technical meeting on electric vehicle and charging station cybersecurity are listed as follows [28].

- Currently available PEV and EVSE charging infrastructures are immature for cybersecurity best practices. Most of the PEV industries do not have security software and development methodologies and guidelines. Also, buyers of PEVs and EVSEs do not typically specify the cybersecurity-related protection requirements because of limited knowledge.
- The trust model for end-to-end communication is in an early stage of development. Also, the standards for end-to-end communications between PEVs, EVSEs, and the power grid are still in the development phase.
- Cybersecurity-related testing and assessment are not accessible to most of the PEVs and charging infrastructure industries. Further research in this field is inevitable.
- The guidelines and guidance on cybersecurity requirements for wireless charging infrastructures for light passenger PEVs, electric buses, and electric trucks are still in the testing and demonstration phase.
- Currently available PEV infrastructures such as EVSEs, smart meters, advanced metering infrastructure, and demand response equipment are yet to be matured with up-to-date technologies.
- Commonly available EVSEs are still struggling with proper physical security guidelines and guidance. Unavailability of such guidelines has adversely affected the consumer's confidence in PEVs.

VII. Conclusion

This paper has described the concept of SCMS and the potential grid services that can be provided by unidirectional PEVs (without the use of V2G technology) charging. The various grid services provided by SCMS such as peak shaving, demand charge reduction, frequency regulation, spinning reserve, renewable energy integration support, distributed congestion management, reactive power compensation, and emergency demand response were discussed in detail. This paper also provided a literature survey on existing work on cybersecurity of SCMS, the major cyber-physical attacks in SCMS with their various impacts, and the major challenges of dealing with these attacks were explored. Moreover, research gaps and associated vulnerabilities of commercially available SCMSs technologies were also discussed.

The goal of SCMS is not only to optimize the coordinated charging of a large number of PEVs but also provide numerous grid services. Therefore, proper algorithms should be developed through more research and development in SCMSs. Due to the involvement of various cyber-physical components during the implementation of SCMS, it possesses various serious cyber-physical threats. Therefore, proper detection, identification, defense, and mitigation measures are required to provide cybersecurity of SCMS. Moreover, current commercially available SCMS technologies are struggling with unique cybersecurity-related threats, therefore, further research and development, and various guidelines and security need to be developed.

Acknowledgement

This work was supported by the U.S. National Science Foundation (NSF) under Grant NSF 1847578.

References

[1] D. Wu, N. Radhakrishnan, X.Ke, S. Huang, A. Reiman, and K. Kalsi, "Coordinated pev charging for distribution system management," PNNL, Tech. Rep. PNNL-27710, July 2019.

[2] M. Kamruzzaman, N. Bhusal, and M. Benidris, "Determining maximum hosting capacity of electric distribution systems to electric vehicles," in *2019 IEEE Industry Applications Society Annual Meeting*, Baltimore, MD, USA, USA, 2019, pp. 1–7.

[3] J. García-Villalobos, I. Zamora, J. San Martín, F. Asensio, and V. Aperribay, "Plug-in electric vehicles in electric distribution networks: A review of smart charging approaches," *Renewable and Sustainable Energy Reviews*, vol. 38, pp. 717 – 731, 2014.

[4] K. M. Tan, V. K. Ramachandaramurthy, and J. Y. Yong, "Integration of electric vehicles in smart grid: A review on vehicle to grid technologies and optimization techniques," *Renewable and Sustainable Energy Reviews*, vol. 53, pp. 720 – 732, 2016.

[5] M. Kamruzzaman and M. Benidris, "Reliability-based metrics to quantify the maximum permissible load demand of electric vehicles," *IEEE Transactions on Industry Applications*, vol. 55, no. 4, pp. 3365–3375, 2019.

[6] A. S. Musleh, G. Chen, and Z. Y. Dong, "A survey on the detection algorithms for false data injection attacks in smart grids," *IEEE Transactions on Smart Grid*, doi:10.1109/TSG.2019.2949998, 2019.

[7] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1630–1638, 2017.

[8] J.Deign. (2018, March) Why is vehicle-to-grid taking so long to happen? [Online]. Available: https://www.greentechmedia.com/articles/read/why-is-vehicle-to-grid-taking-so-long-to-happen

[9] R. Gough, C. Dickerson, P. Rowley, and C. Walsh, "Vehicle-to-grid feasibility: A techno-economic analysis of ev-based energy storage," *Applied Energy*, vol. 192, pp. 12 – 23, 2017.

[10] A. Briones, J. Francfort, P. Heitmann, M. Schey, S. Schey, and J. Smart, "Vehicle-to-grid (V2G) power flow regulations and building codes review by the AVTA," INL, Tech. Rep. INL/EXT-12-26853, September 2012.

[11] C. S. Ioakimidis, D. Thomas, P. Rycerski, and K. N. Genikomsakis, "Peak shaving and valley filling of power consumption profile in non-residential buildings using an electric vehicle parking lot," *Energy*, vol. 148, pp. 148 – 158, 2018.

[12] C. G. Tse, B. A. Maples, and F. Kreith, "The Use of Plug-In Hybrid Electric Vehicles for Peak Shaving," *Journal of Energy Resources Technology*, vol. 138, no. 1, 09 2015.

[13] N. Leemput, F. Geth, B. Claessens, J. Van Roy, R. Ponnette, and J. Driesen, "A case study of coordinated electric vehicle charging for peak shaving on a low voltage grid," in *2012 3rd IEEE PES Innovative Smart Grid Technologies Europe (ISGT Europe)*, Berlin, Germany,, 2012, pp. 1–7.

[14] A. S. Masoum, S. Deilami, P. S. Moses, M. A. S. Masoum, and A. Abu-Siada, "Smart load management of plug-in electric vehicles in distribution and residential networks with charging stations for peak shaving and loss minimisation considering voltage regulation," *IET Generation, Transmission Distribution*, vol. 5, no. 8, pp. 877–888, 2011.

[15] M. López, S. [de la Torre], S. Martín, and J. Aguado, "Demand-side management in smart grid operation considering electric vehicles load shifting and vehicle-to-grid support," *International Journal of Electrical Power & Energy Systems*, vol. 64, pp. 689 – 698, 2015.

[16] E. Sortomme and M. A. El-Sharkawi, "Optimal combined bidding of vehicle-to-grid ancillary services," *IEEE Transactions on Smart Grid*, vol. 3, no. 1, pp. 70–79, 2012.

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

[18] M. Caramanis and J. M. Foster, "Management of electric vehicle charging to mitigate renewable generation intermittency and distribution network congestion," in *Proceedings of the 48h IEEE Conference on Decision and Control (CDC) held jointly with 2009 28th Chinese Control Conference*, Shanghai, China, 2009, pp. 4717–4722.

[19] F. Mwasilu, J. J. Justo, E.-K. Kim, T. D. Do, and J.-W. Jung, "Electric vehicles and smart grid interaction: A review on vehicle to grid and renewable energy sources integration," *Renewable and Sustainable Energy Reviews*, vol. 34, pp. 501 – 516, 2014.

[20] D. B. Richardson, "Electric vehicles and the electric grid: A review of modeling approaches, impacts, and renewable energy integration," *Renewable and Sustainable Energy Reviews*, vol. 19, pp. 247 – 254, 2013.

[21] E. Sortomme, A. I. Negash, S. S. Venkata, and D. S. Kirschen, "Voltage dependent load models of charging electric vehicles," in *2013 IEEE Power Energy Society General Meeting*, Vancouver, BC, Canada, 2013, pp. 1–5.

[22] N. Leemput, F. Geth, J. Van Roy, J. Büscher, and J. Driesen, "Reactive power support in residential lv distribution grids through electric vehicle charging," *Sustainable Energy, Grids and Networks*, vol. 3, pp. 24 – 35, 2015.

[23] M. Nikkhah Mojdehi and P. Ghosh, "An on-demand compensation function for an ev as a reactive power service provider," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 6, pp. 4572–4583, 2016.

[24] S. Paudyal, O. Ceylan, B. P. Bhattarai, and K. S. Myers, "Optimal coordinated ev charging with reactive power support in constrained distribution grids," in *2017 IEEE Power Energy Society General Meeting*, Chicago, IL, USA, 2017, pp. 1–5.

[25] M. Kesler, M. C. Kisacikoglu, and L. M. Tolbert, "Vehicle-to-grid reactive power operation using plug-in electric vehicle bidirectional offboard charger," *IEEE Transactions on Industrial Electronics*, vol. 61, no. 12, pp. 6778–6784, 2014.

[26] R. Gadh, "Demonstrating plug-in electrical vehicles smart charging and storage supporting the grid," UCLA Smart Grid Energy Research Center (SMERC), Tech. Rep. CEC-500-2018-020, August 2018.

[27] M. Mallette and G. Venkataramanan, "The role of plug-in hybrid electric vehicles in demand response and beyond," in *IEEE PES T D 2010*, New Orleans, LA, USA, 2010, pp. 1–7.

[28] K. Harnett, B. Harris, D. Chin, and G. Watson, "DOE/DHS/DOT volpe technical meeting on electric vehicle and charging station cybersecurity," U.S. Department of Transportation, Tech. Rep. DOTVNTSC-DOE-18-01, March 2018.

[29] S. Dey and M. Khanra, "Cybersecurity of plug-in electric vehicles: Cyber attack detection during charging," *IEEE Transactions on Industrial Electronics*, doi: 10.1109/TIE.2020.2965497, 2020.

[30] S. Abedi, A. Arvani, and R. Jamalzadeh, *Cyber Security of Plug-in Electric Vehicles in Smart Grids: Application of Intrusion Detection Methods*. Singapore: Springer Singapore, 2015, pp. 129–147.

[31] D. Reeh, F. Cruz Tapia, Y. Chung, B. Khaki, C. Chu, and R. Gadh, "Vulnerability analysis and risk assessment of EV charging system under cyber-physical threats," in *2019 IEEE Transportation Electrification Conference and Expo (ITEC)*, Detroit, MI, USA, USA, 2019, pp. 1–6.

[32] R. Gottumukkala, R. Merchant, A. Tauzin, K. Leon, A. Roche, and P. Darby, "Cyber-physical system security of vehicle charging stations," in *2019 IEEE Green Technologies Conference(GreenTech)*, Lafayette, LA, USA, USA, 2019, pp. 1–5.

[34] K. Manandhar, X. Cao, F. Hu, and Y. Liu, "Detection of faults and attacks including false data injection attack in smart grid using kalman

[33] S. Rahman, H. Aburub, Y. Mekonnen, and A. I. Sarwat, "A study of EV BMS cyber security based on neural network soc prediction," in *2018 IEEE/PES Transmission and Distribution Conference and Exposition (T D)*, Denver, CO, USA, 2018, pp. 1–5.

filter," *IEEE Transactions on Control of Network Systems*, vol. 1, no. 4, pp. 370–379, 2014.

[35] S. Li, Y. Yılmaz, and X. Wang, "Quickest detection of false data injection attack in wide-area smart grids," *IEEE Transactions on Smart Grid*, vol. 6, no. 6, pp. 2725–2735, 2015.

[36] M. A. Rahman and H. Mohsenian-Rad, "False data injection attacks with incomplete information against smart power grids," in *2012 IEEE Global Communications Conference (GLOBECOM)*, 2012, pp. 3153–3158.

[37] X. Wang, X. Luo, M. Zhang, and X. Guan, "Distributed detection and isolation of false data injection attacks in smart grids via nonlinear unknown input observers," *International Journal of Electrical Power & Energy Systems*, vol. 110, pp. 208 – 222, 2019.

[38] Y. He, G. J. Mendis, and J. Wei, "Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2505–2516, 2017.

[39] R. M. Shukla and S. Sengupta, "Scalable and robust outlier detector using hierarchical clustering and long short-term memory (lstm) neural network for the internet of things," *Internet of Things*, vol. 9, p. 100167, 2020.

[40] C. Carter, I. Onunkwo, P. Cordeiro, and J. Johnson, "Cyber security assessment of distributed energy resources," in *2017 IEEE 44th Photovoltaic Specialist Conference (PVSC)*, Washington, DC, USA, 2017, pp. 2135–2140.

[41] Cyber Security Research and Development, "Cyber Assessment Report of Level 2 AC Powered Electric Vehicle Supply Equipment," INL, Tech. Rep. INL/MIS-18-45521, May 2018.

[42] U. Meyer and S. Wetzel, "A man-in-the-middle attack on umts," in *Proceedings of the 3rd ACM Workshop on Wireless Security*. New York, NY, USA: Association for Computing Machinery, 2004, pp. 90—97. [Online]. Available: https://doi.org/10.1145/1023646.1023662

[43] L. Su and D. Ye, "A cooperative detection and compensation mechanism against denial-of-service attack for cyber-physical systems," *Information Sciences*, vol. 444, pp. 122 – 134, 2018.

[44] T. Mahjabin, Y. Xiao, G. Sun, and W. Jiang, "A survey of distributed denial-of-service attack, prevention, and mitigation techniques," *International Journal of Distributed Sensor Networks*, vol. 13, no. 12, p. 1550147717741463, 2017.

[45] F. Callegati, W. Cerroni, and M. Ramilli, "Man-in-the-middle attack to the https protocol," *IEEE Security Privacy*, vol. 7, no. 1, pp. 78–81, 2009.

[46] B. Bhushan, G. Sahoo, and A. K. Rai, "Man-in-the-middle attack in wireless and computer networking — a review," in *2017 3rd International Conference on Advances in Computing,Communication Automation (ICACCA) (Fall)*, 2017, pp. 1–6.

[47] K. Ouafi, R. Overbeck, and S. Vaudenay, "On the security of hb# against a man-in-the-middle attack," in *Advances in Cryptology - ASIACRYPT 2008*, J. Pieprzyk, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 108–124.

[48] Z. Xu, R. A. Sowah, K. B. Ofori-Amanfo, G. A. Mills, and K. M. Koumadi, "Detection and prevention of man-in-the-middle spoofing attacks in manets using predictive techniques in artificial neural networks (ann)," *Journal of Computer Networks and Communications*, 2019.

[49] J. Qin, M. Li, L. Shi, and X. Yu, "Optimal denial-of-service attack scheduling with energy constraint over packet-dropping networks," *IEEE Transactions on Automatic Control*, vol. 63, no. 6, pp. 1648–1663, 2018.

[50] T. V. Phan and M. Park, "Efficient distributed denial-of-service attack defense in sdn-based cloud," *IEEE Access*, vol. 7, pp. 18 701–18 714, 2019.

[51] B. A. Khalaf, S. A. Mostafa, A. Mustapha, M. A. Mohammed, and W. M. Abduallah, "Comprehensive review of artificial intelligence and statistical approaches in distributed denial of service attack and defense methods," *IEEE Access*, vol. 7, pp. 51 691–51 713, 2019.

[52] T. Jamal, Z. Haider, S. A. Butt, and A. Chohan, "Denial of service attack in cooperative network," *arXiv:1810.11070v1*, 2018.