23rd EURO Working Group on Transportation Meeting, EWGT 2020, 16-18 September 2020, Paphos, Cyprus

Impact of False Data Injection attacks on Decentralized Electric Vehicle Charging Protocols

Nikos Piperigkos[a,c,*], Aris S. Lalos[a,b]

[a] Industrial Systems Institute, ATHENA Research and Innovation Center, 265 04 Platani, Greece
[b] Department of Electrical and Computer Engineering, University of Patras, Patra, Greece
[c] Department of Computer Engineering and Informatics, University of Patras, Patra, Greece

Abstract

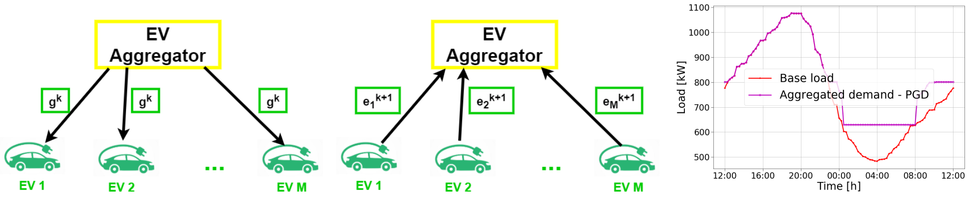
Electric vehicles (EVs) gain great attention nowadays since the electrification of private and public transport has a great potential to reduce greenhouse gas emissions and mitigate oil dependency. However, the influx of a large number of electrical loads without any coordination could have adverse affects to the electrical grid. More importantly, the complexity in the coordination of a large number of EVs, pose critical challenges in ensuring overall system integrity. A typical attack found in the controllers of connected EVs is false data injection (FDI), which can be utilized to distort real energy demand and supply figures. Energy distribution requests may therefore be erroneous. The lack of a proper coordination scheme, robust to such cyber attacks could cause voltage magnitude drops and unacceptable load peaks. In this work, we study the impact of FDI attacks, on various decentralized charging protocol with reduced computational requirements. The proposed decentralized EV charging algorithms only require from each EV to solve a local problem, hence the proposed implementation require low computational resources. An extensive evaluation study highlights the strengths and weaknesses of the presented solutions which are based on iterative convex optimization solvers .

Keywords: Electric Vehicles; Coordinated Charging; Decentralized Protocols; False Data Injection Attacks

Electric Vehicles (EVs) are gaining increasing interest, as a long-term vehicular technology facilitating the reduction of greenhouse gases. However, as EV penetration increases, uncoordinated charging affects may lead to unacceptable voltage variation, overloading the power grid. As a viable option, a “smart grid” solution could be also adopted, allowing EVs to communicate with an EV aggregator module, that in turn coordinates their charging. Furthermore, cyber-security has been become a crucial aspect of modern power systems, due to the emerging attackers capabilities. FDI attacks is a common threat in power grids and various detection and mitigation techniques have been developed (He et al. (2017), Liang et al. (2017)) so far. Therefore, since EVs must connect to the grid, they are also vulnerable during the charging period. The area of EV scheduling is a very active area of current research. The approaches

[*] Corresponding author.
E-mail address: piperigkos@ceid.upatras.gr

proposed can be categorized concerning the degree of the centralization of the scheduling control. Decentralized control strategies require less computational resources while they enhance user privacy. State of the art approaches on coordinated EV charging include Fan et al. (2012), Karfopoulos et al. (2013), Chen et al. (2014). To the best of our knowledge, this is the first work that studies the impact of FDI attacks in the robustness of low complexity charging schemes that successfully address the valley-filling task in attack free scenarios. The goal of valley-filling is to flatten the given load demand profile of the aggregator as much as possible, by filling the overnight valley in the load demand with the demand caused by the EVs, even in the presence of FDI attacks. The general architecture of decentralized charging protocols aiming to fulfil this task, is depicted on Fig. 1. During this iterative procedure, an EV aggregator distributes the current aggregated load demand $\boldsymbol{g^k}$ of all EVs and then, EVs update their charging profiles $\boldsymbol{e_m^{k+1}}$ accordingly and sent them back to the aggregator. Due to exactly this ”exchange” protocol, an attacker can modify what EVs sent back to the aggregator. In this paper, we evaluate the performance of three decentralized charging protocols under FDI attacks aiming to discharge the individuals EVs. Furthermore, each EV is equipped with a controller capable of: i) communicating with an aggregator and ii) performing tasks, like receiving information, updating the charging profile of EV and forwards it back to the aggregator. The three protocols under study, are based on: i) Frank-Wolfe (FW) (Zhang et al. (2017)), ii) Projected Gradient Descent (PGD) (Gan et al. (2013)) and iii) Alternating Direction Method of Multipliers (ADMM) (Rivera et al. (2017)) algorithms. Based on extensive experimental evaluation, both PGD and ADMM are less affected by the different attacks and significantly outperforms FW. In fact, both PGD (Fig. 1-(c)) and ADMM remain almost intact by the attack, while FW is actually unable to perform the coordinated EV charging.



(a) Aggregator sent $\boldsymbol{g^k}$ (b) EVs sent $\boldsymbol{e_m^{k+1}}$ (c) PGD

Fig. 1. Decentralized charging protocol and total load demand with PGD under attack.

Acknowledgements

This paper has received funding from the European Union’s H2020 research and innovation programme CARAMEL under grant agreement No 833611.

References

J. Rivera, C. Goebel and H. Jacobsen, ”Distributed Convex Optimization for Electric Vehicle Aggregators,” in IEEE Transactions on Smart Grid, vol. 8, no. 4, pp. 1852-1863, July 2017.

L. Zhang, V. Kekatos and G. B. Giannakis, ”Scalable Electric Vehicle Charging Protocols,” in IEEE Transactions on Power Systems, vol. 32, no. 2, pp. 1451-1462, March 2017.

L. Gan, U. Topcu and S. H. Low, ”Optimal decentralized protocol for electric vehicle charging,” in IEEE Transactions on Power Systems, vol. 28, no. 2, pp. 940-951, May 2013.

Z. Fan, “A distributed demand response algorithm and its application to PHEV charging in smart grids,” IEEE Trans. Smart Grid, vol. 3, no. 3, pp. 1280–1290, Sep. 2012.

E. L. Karfopoulos and N. D. Hatziargyriou, “A multi-agent system for controlled charging of a large population of electric vehicles,” IEEE Trans. Power Syst., vol. 28, no. 2, pp. 1196–1204, May 2013.

N. Chen, C. W. Tan, and T. Quek, “Electric vehicle charging in smart grid: Optimality and valley-filling algorithms,” IEEE J. Sel. Topics Signal Process., vol. 8, no. 6, pp. 1073–1083, Dec. 2014.

Y. He, G. J. Mendis and J. Wei, ”Real-Time Detection of FDI Attacks in Smart Grid: A Deep Learning-Based Intelligent Mechanism,” in IEEE Transactions on Smart Grid, vol. 8, no. 5, pp. 2505-2516, Sept. 2017.

G. Liang, S. R. Weller, J. Zhao, F. Luo and Z. Y. Dong, ”The 2015 Ukraine Blackout: Implications for FDI Attacks,” in IEEE Transactions on Power Systems, vol. 32, no. 4, pp. 3317-3318, July 2017.