Akbarian, Amirhossein; Bahrami, Mahdi; Vakilian, Mehdi; Lehtonen, Matti

Vulnerability of EV Charging Stations to Cyber Attacks Manipulating Prices

Published in:
2023 International Conference on Future Energy Solutions, FES 2023

DOI:
10.1109/FES57669.2023.10183070

Published: 01/01/2023

Document Version
Peer-reviewed accepted author manuscript, also known as Final accepted manuscript or Post-print

Vulnerability of EV Charging Stations to Cyber Attacks Manipulating Prices

Amirhossein Akbarian, Mahdi Bahrami,
Mehdi Vakilian, Senior Member, IEEE
Electrical Engineering Department and Center of Excellence in
Power System Management and Control
Sharif University of Technology
Tehran, Iran

Matti Lehtonen
Department of Electrical Engineering and Automation
Aalto University
Espoo, Finland

***Abstract*—Electric vehicles (EVs) have experienced an unprecedented increase in their penetration; in well developed countries; due to the advancement of battery technology and the need to make transportation more environmentally friendly. As a result of this trend, EVs have become an integral part of those countries power grid ecosystem, where they may be used as both a source, and a consumer of energy. However, cybersecurity risks associated with large fleets of EVs within the power grids can significantly impact the normal operation of distribution systems. This paper considers the cyber-attack consequences, from attackers' perspective. The cyber attackers under study target the charging price (CP) by increasing the CP in off-peak hours and accordingly subsiding it in on-peak hours. A two-stage optimization framework is proposed to identify the most important ultra-fast charging stations (XFCs) under the cyber-attack, meanwhile, the EV users' response to the compromised CP is considered. Then, the proposed model is implemented on a modified IEEE 123-bus distribution test system, and the effectiveness of the model is proved through some case studies. In particular, they demonstrated that the amount of load shedding is increased by 8.198 MW when the EV user response is taken into account.**

Keywords—Charging price, customer behavior, EV, FDIA, two-stage optimization, XFC.

I. INTRODUCTION

THE auto industry's transition to electric vehicles (EVs) is accelerating in the third decade of 21 century. The year 2026 has emerged as a tipping point for an acceleration in EV adoption that will drive automotive electrification trends ahead. By 2030, over one in four new passenger cars sold will be an electric vehicle. Many major vehicle manufacturers worldwide have signaled the end of an era of internal combustion engines (ICE) as the transition to zero emission vehicles (ZEV) is ramped up [1]. Since the penetration of EVs has increased, optimal management of the charging process has become an increasingly important factor for EVs owners (EVOs), service providers, utilities, and operators of power systems. In order to properly manage the charging of EVs, a smart charging management system is required that can optimize charging both at public charging stations and at residential charging stations. Accurately monitoring charging price (CP) rate is an important action to pave the above-mentioned aid. However, there is no doubt that the large adoption of EVs will present a significant challenge to the current electrical grid [2]. It is anticipated that unmanaged loads associated with the charging of EVs will have significant negative effects on grids, from degradation of power quality and overloading of transformers to frequency and voltage disturbances, leading to brownouts or even blackouts. Hence, it can threaten the security and stable operation of the power systems.

Cyber-attack against CP is one of the paramount intrusive actions, targeting the load and supply balance. Such attacks can be launched in both vehicle-to-grid (V2G) and grid-to-vehicle (G2V) states. It is possible to exchange bidirectional energy between EVs and grids with the help of V2G technology. Thus, surplus power can be stored during periods of low demand and can be fed back into grids during times of high demand (peak hours) [3]. By considering EV user response to the CP variations, cyber attackers can employ more efficient strategies. Thus, the adverse impacts of the attacks are intensified.

In the literature, numerous studies have examined the technical aspects of the integration of EVs and their possible impacts on the smart grid. A number of technical aspects have been examined in [4], including charging strategies, energy management, power losses, grid interface technologies, integrating renewable energy sources, ensuring power system reliability, regulating voltages and frequencies, and regulating EVs in electricity markets. In spite of the fact that cybersecurity has been extensively addressed in the literature, it has not been adequately addressed for EVs, electric vehicle charging stations (EVCSs), and smart charging management system (SCMS). To this end, an in-depth review of false data injection attacks (FDIAs) in smart grids is given in [5]. These existing works are mainly designed to detect any abnormality. However, the security assessment of EV infrastructure has remained as an important aspect of power delivery. In this regard, Tony et al. devise a system lookup and collection approach to obtain a representative sample of widely deployed EV charging station management systems (EVCSMS) so that derive comprehensive security and vulnerability analysis [6]. This work ignores attackers' perspective and more importantly the user response to the attack. However, by expressing the model from the attackers' perspective, the behavior of the cyber attackers can be analyzed in different conditions. The results of this analysis then enhance the operators' cyber-security situational awareness. Thus, they can efficiently respond to the cyber-security events.

In addition, some studies have focused on modeling the charging/discharging behavior of EV users in normal conditions (without cyberattacks) [7]. However, such studies do not consider FDIA. In response, this paper presents a novel optimization model so as to identify paramount EVCSs location to maximize load shedding amount, the model is presented from attackers' perspective and the relevant constraints are introduced. A coordinated cyberattack is launched to change the CP. The EV user response (EVUR) to this price changed is modeled and

subsequently the load profile changes will be accordingly demonstrated. As outlined above, the main contribution of this work encompasses:

1) Proposing a cyber vulnerability assessment method to determine the most important ultra-fast charge stations (XFCs) to be attacked, from the cyber attackers' viewpoint.
2) The proposed framework includes two optimization problems, and these two problems are linked together through location of most important XFCs.
3) The EV users' reaction in response to this change in CP rate toward their charging policy is modeled, and then these models are taken by the proposed framework to evaluate the possible impacts of such attacks.

The remainder of the paper is divided as follows; a concise introduction is mentioned at Section II so as to reveal the attackers' aims, then, an optimization is formulated to maximize the load shedding (LS), attackers' perspective is considered. The attack target is to change CP during peak hours so as to soar demand unexpectedly, Section III is devoted to modeling EVUR to this CP changed. At Section IV, the proposed model is simulated on the test system, and the results are discussed. Finally, Section V concludes the paper and highlights the objectives of it.

II. Proposed Framework Outline

In this section, the proposed framework is discussed, and then attack strategy under study is introduced.

A. Outline of the Proposed Framework

A framework of two-stage optimization utilized in this paper is illustrated in Fig. 1. At the first stage, the problem is formulated from attackers' viewpoints to maximize load shedding amount at the grid. To obtain this target, constraints, such as power flow, voltage, EVCS, and attackers' limitation are considered. Attackers can easily take advantage of this information so as to increase the severity of the attack. The mathematically EVUR is revealed, at the second stage optimization. The detected XFCs are selected to model EVUR, in a way that, a satisfaction function is introduced to show customer behavior changing after the coordinated cyber-attack and obtain the compromised load curve.

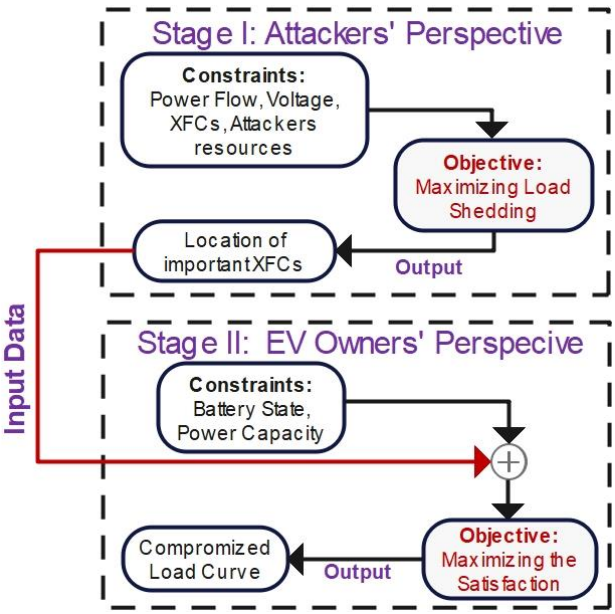

Fig. 1. The proposed two-stage optimization framework

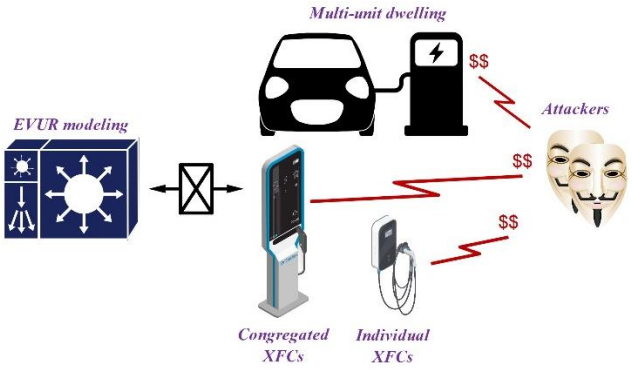

Fig. 2. Attackers' target and electric vehicles owner response relationship

B. Attack Motivation and Strategy

An important consideration for the distribution system operators (DSOs) is that how to minimize the passive impacts of public charging stations, including individual or congregated charging stations at workplace, multi-unit dwelling, and retail-establishment, on power systems and the operating costs of the station, leading to determining the CPs. A proper CP mechanism is of the utmost importance to improve public satisfaction. According to Fig. 2, the attackers' target is to change CP rates through FDIA so as to increase the rates during off-peaks and subside them in on-peaks. The attack will be intensified in case of aiming XFCs due to the higher accessibility and a large amount of the power flow to EVs. Having said that, though, the attackers are looking for more crucial tasks to increase the severity of their attacks. To this end, analyzing customers' behavior in reaction toward CP changes can be considered paramount for the cyber attackers targeting CP rate.

III. Mathematical Formulation for the First Stage of Optimization(Attackers' Perspective)

In this section, a mathematical formulation is presented. By its application, the most important charging stations are evaluated. The result is expressed in terms of the cyber attackers' perspective who are targeting the CP rate.

A. Objective Function

Any change in EVO's behavior (due to CP rate change) will arise operational and economic concerns, in such a way that during peak hours the power operators will face such an overload that can't manage the operation by employing the reserved resources, e.g. distributed generators (DGs). A coordinated attack, in particular against XFCs, provokes the case, leading to cascading blackouts in grid. To this end, attackers' objective function is defined in (1):

$$\max\{ALS_{\tau,k,t}\} \quad ; \forall \tau \epsilon \vartheta_{EVCS} \text{ and } t \in T \text{ and } k \epsilon \varphi_s; \tag{1}$$

Where, *ALS* represents active LS in MW. In addition, τ is an EVCS from the whole set of EVCSs (ϑ_{EVCS}). In this study, it is assumed that there are 20 EVCSs in 20 dedicated zones. In (1), *t* shows time interval within a duration of T=24 hours, and *k* stands for the attack scenarios. Thus, based on the number of EVCSs in the grid, the total number of possible cyber-attacks is determined. In the case study of this work where there are 20 EVCSs in the distribution grid, the total number of possible attacks is equal to (2):

$$\binom{20}{1}+\binom{20}{2}+\binom{20}{3}+\cdots+\binom{20}{20}=2^{20}-1; \quad (2)$$

In other words, all possible simultaneous attacks against 20 EVCSs are calculated by (2). However, the attackers' resources limitation causes the actual number to be much lower than (2).

B. Constraints

1) Power Flow Constraints

A linear Distflow algorithm [8] is utilized in this study for power flow calculation. Equations (3) and (4) demonstrate the active and reactive power balance at each bus, respectively.

$$\sum_{j|\, ij \in \varphi_L} P_{k,t}^{ij} = \gamma^i PG_{k,t}^i + \aleph^i PDG_{k,t}^i + \omega^i PWT_{k,t}^i + \rho^i PPV_{k,t}^i - PD_t^i - \beth^i PEVCS_{k,t}^i + ALS_{i,k,t} \; ; \forall i \epsilon \varphi_B \; and \; t \epsilon T \; and \; k \epsilon \varphi_s; \quad (3)$$

$$\sum_{j|\, ij \in \varphi_L} Q_{k,t}^{ij} = \gamma^i QG_{k,t}^i + QDG_{k,t}^i - QD_t^i - QEVCS_{k,t}^i + RLS_{i,k,t} \; ; \forall i \epsilon \varphi_B \; and \; t \epsilon T \; and \; k \epsilon \varphi_s; \quad (4)$$

Where, P and Q represent active and reactive power flowing in line ij, respectively. PG and QG stand for active and reactive power supplied by diesel generators at the specific buses pinpointed via binary variable of γ, respectively. Also, the amount of supplied active/reactive power via DG units is shown by *PDG/QDG*. Regarding the fact that all buses may not have a DG, a binary variable of $\aleph$ is defined, $\aleph$ is equal to 1 in case of existing DG at bus i, otherwise, it is 0. In this work, it is assumed that there are photovoltaic (PVs) and wind turbine (WTs) units, among other classic electricity resources. Hence, *PWT and PPV* illustrate the power generated by these units, respectively. Whereas, $\omega \; and \; \rho$ are two binary variables showing whether there are WT and PV units. Also, *PD/QD* is the ratio of active/reactive load at each bus. PEVCS/QEVCS shows the active/reactive power consumed in each station. As before, whole buses are not equipped with EVCSs, so we define an auxiliary variable of $\beth$ to specify each deployed bus. In (3) and (4), *ALS/RLS* indicates active/reactive load shedding at each bus. Finally, φ_B shows all buses, φ_L represents all lines, and φ_s shows all possible scenarios.

$$PEVCS_{k,t}^{\tau} \le ALS_{\tau,k,t} \le PD_t^i \quad ; \forall \tau \epsilon \vartheta_{EVCS} \; , \forall t \in T \quad (5)$$

$$RLS_{\tau,k,t} = ALS_{\tau,k,t} tg(\cos^{-1}\varphi_i); \; \forall \tau \epsilon \vartheta_{EVCS} \; , \; \forall t \in T \quad (6)$$

$$PGMIN \le PG_{k,t}^h \le \text{PGMAX} \; ; \; \forall h \in \varphi_H \; , \forall t \in T \quad (7)$$

$$QGMIN \le QG_{k,t}^h \le QGMAX \; ; \; \forall h \in \varphi_H \; , \forall t \in T \quad (8)$$

$$0 \le PDG_{k,t}^q \le \text{PDGMAX} \; ; \; \forall q \in \varphi_Q \; , \forall t \in T \quad (9)$$

$$0 \le QDG_{k,t}^q \le \text{PDGMAX}; \; \forall q \in \varphi_Q, \forall t \in T \quad (10)$$

$$0 \le PWT_{k,t}^w \le \text{PWTMAX}; \; \forall w \in \varphi_W, \forall t \in T \quad (11)$$

$$0 \le PPV_{k,t}^p \le \text{PPVMAX}; \; \forall p \in \varphi_P, \forall t \in T \quad (12)$$

Load shedding cannot be exceeded the amount of demand at each bus, this constraint reveals in (5) and (6) within EVCS buses. Equations (7) and (8) examine the maximum and minimum amount of substation supplied power. Meanwhile, (9) and (10) cover maximum amount of each DG supplied power, if exists. Finally, PV and WT production must not be out of the defined limitation.

2) Voltage Constraints

$$\mathcal{V}_{min}^i \le |\mathcal{V}|_{k,t}^i \le \mathcal{V}_{max}^i \quad \forall i \in \varphi_B \; , \forall t \in T; \quad (13)$$

Equation (13) is contingent with voltage magnitude limits.

$$(-BN)(\delta_{k,t}^{ij})(\beta_{k,t}^{ij}) - (r_{ij}P_{k,t}^{ij} + x_{ij}Q_{k,t}^{ij}) \le \mathcal{V}_{k,t}^j - \mathcal{V}_{k,t}^i \le (+BN)(\delta_{k,t}^{ij})(\beta_{k,t}^{ij}) + (r_{ij}P_{k,t}^{ij} + x_{ij}Q_{k,t}^{ij}) \quad ; \forall ij \in \varphi_L \; , \forall t \in T \quad (14)$$

Equation (14) is concerned with adjacent voltage relationships, in which BN is a big number. In this constraint, δ is equal to 1 when there is a line between two buses (*i and j*). In addition, β is a binary variable equaling to 0 by default and altering to 1 in case there is an open switch between two buses. r_{ij}/x_{ij} is resistance/reactance amount of line *ij*.

Equations (15) - (17) stand for line flow constraints.

$$-\sqrt{2}(\delta_{k,t}^{ij})(\beta_{k,t}^{ij})\bar{S}_{ij} \le P_{k,t}^{ij} + Q_{k,t}^{ij} \le \sqrt{2}(\delta_{k,t}^{ij})(\beta_{k,t}^{ij})\bar{S}_{ij} \; ; \forall ij \in \varphi_L \; , \forall t \in T \quad (15)$$

$$-(\delta_{k,t}^{ij})(\beta_{k,t}^{ij})\bar{S}_{ij} \le P_{k,t}^{ij} \le (\delta_{k,t}^{ij})(\beta_{k,t}^{ij})\bar{S}_{ij} \quad ; \quad \forall ij \in \varphi_L \; , \forall t \in T \quad (16)$$

$$-(\delta_{k,t}^{ij})(\beta_{k,t}^{ij})\bar{S}_{ij} \le Q_{k,t}^{ij} \le (\delta_{k,t}^{ij})(\beta_{k,t}^{ij})\bar{S}_{ij} \quad ; \quad \forall ij \in \varphi_L \quad , \quad \forall t \in T \quad (17)$$

Where $\bar{S}_{ij} = \sqrt{(P_{k,t}^{ij})^2 + (Q_{k,t}^{ij})^2}$.

3) EVCS Constraints

There are several types of EVCSs. To cause the disturbing outcomes, attackers prefer to target XFCs [9]. Equation (18) implies this consideration. The attacker can access to EV charging power information via spoofing attack (SA) [10].

$$PEVCS_{\tau} \ge EVFCAPMIN \quad ; \forall \tau \epsilon \vartheta_{EVCS} \quad (18)$$

Where; $PEVCS_m$ is power of m-th charging station among all $\varphi_{EV}, and \; EVFCAPMIN$ is the capacity of an EVCS in kW.

4) Attackers' Resources Constraints

In this paper, the attack can be launched via a skilled attacker who knows the existing security topologies. There are security levels (SLs) for each EVCS. The stations with lower SL are more prone to the attack. Equation (19) comes to satisfy this restriction.

$$SL_{\tau} \le SLMAX \quad ; \forall \tau \epsilon \vartheta_{EVCS} \quad (19)$$

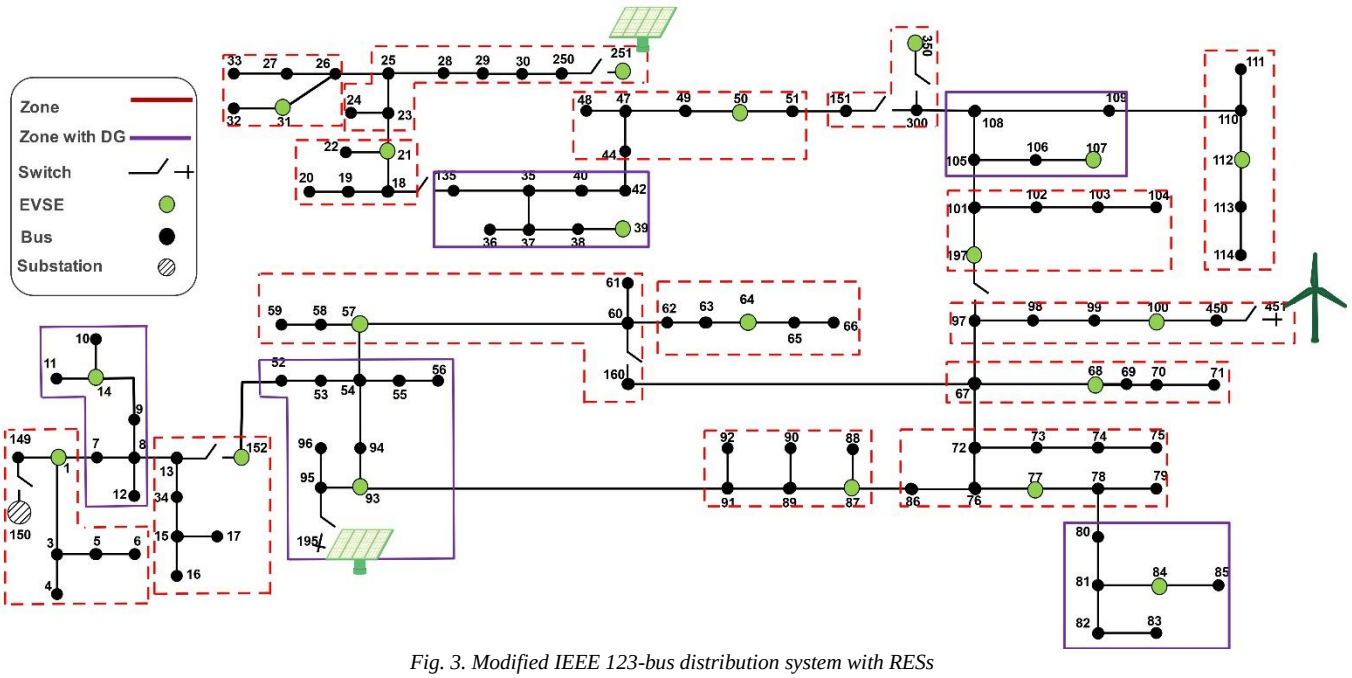

Fig. 3. Modified IEEE 123-bus distribution system with RESs

where, SL_r is equal to SL amount ranging between 0 and 1; and $SLMAX$ is a maximum desired SL from the attackers' perspective.

IV. Mathematical Formulation for the Second Stage of Optimization(User Response Modeling)

The EVUR behavior according to fluctuating electricity price is mostly reflected in the changes in the load demanded. On the side of EVOs, paying minimum CP is the most preferable objective. While type of travel, efficiency of battery, amount of state of charge (SoC) are among the most important factors affecting charging pattern, manipulating CP under some conditions may lead to load shifting. Thus, an objective function is introduced from EVO perspective so as to reach the maximum load in the peak hours. Which is the attackers' aim, as well.

A. Objective Function

After CP compromised, charging amount will increase during peak hours, the issue can be modeled from users' perspective as follows:

$$\max \Psi = 1 - \frac{\sum_t |P_{desired.t.n} - P_{\tau.t.n}|}{P_{desired.t.n}} \; ; t \epsilon T. n \epsilon \varphi_{EV} \, . and \; \tau \epsilon \; \overset{Chosen}{\vartheta}_{EVCS} \quad (20)$$

Obviously, EVOs prefer to defer their charging process during off-peaks when the CP is the lowest and avoid charging in peak hours, but the proposed attack scenario disturbs the latter behavior and shifts the demand onto peak hours. Thus, (20) is solved through (t=15 minutes) iterations and performed over peak hours. Where $P_{desired,t,n}$ is the desired targeted power from attackers' perspective, and $P_{\tau,t}$ stands for real power requested by EVOs which will be obtained through the optimization solving. $\overset{Chosen}{\vartheta}_{EVCS}$ is the whole sets of XFCs selected after optimization in Section III.

B. Constraints

EVOs are able to choose their charging time based on the instantaneous CP and the SoC of their vehicle batteries. The EV users with higher SoC level prefer to charge at the time with lower price. When an attack is launched to change the time-of-use (ToU) pricing policy for EV charging, the power balance will be violated. Consequently, users adapt their policy to the new situation so as to obtain the highest benefit. In this regard, we focus on just EVs with a minimum amount of SoC so as to be able to change their charging session in accordance with CP. This issue determines below:

$$SoC_p \geq SoC_{min} \quad (21)$$

Constraint (21) determines the minimum amount of SoC for being allowed to defer the charging session.

$$PVmin \leq P_{\tau,t,n} \leq PVmax \quad (22)$$

The charging power of an EV is bounded by lower and upper limits, which is enforced by (22).

V. Simulation And Results

The IEEE 123-bus test network is shown in Fig. 3. In addition, this figure demonstrates the obtained results after the simulation. To implement the proposed framework, a computer with an Intel Core i7 processor and 8GB of memory was used. Further, a MILP model was solved by IBM ILOG CPLEX 12.8 in GAMS 25.1.3, with a mip gap of 0.2%.

A. Assumptions

We suppose, there are five diesel-powered DG units with capacity of 100 kW located at the determined buses according to Fig. 3 [11]. Whole network is fueled from the bus 150 with total capacity of 4000 MW and 3200 MVAR. There are one WT and two PV units in the test system. Each PV unit has the maximum capacity of 10 MW. In this paper, we consider maximum capacity of 5 MW for the WT [12]. Twenty XFCs are considered in this study, each XFC

has capacity ranging between 50 kW (PVmin) and 350 kW (PVmax) and 30 outlets [9], their locations are pinpointed on Fig. 3. $EVFCAPMIN$ is assumed to be 50 kW (minimum capacity of a XFC), which indirectly circumvents (18). Fig. 4 provides the value of the ToU pricing policy [13], and its corresponding historical load data [14] is illustrated in Fig. 5. There are 3×10^5 EVs in the territory, with SoC level complying with normal distribution with average 0.5 and variance 0.1, and the lithium-iron-phosphate battery used in Tesla model 3 (TM3) EVs is selected for analysis in this paper [15]. $P_{desired,t,n}$, shown in Fig. 5, is derived from the average load amount and minimum SoC is set to 15%. Day-ahead-load can easily be predicted via various ways, such as LSTM prediction [16] which is out of the paper's scope. Voltage magnitude of each bus can be set between 0.95 and 1.05 pu. There is a 24-hour simulation period and 15-minute intervals between each calculation. Also, all XFCs are not targeted by attackers, there is SL for each XFC, based on attackers' resources limitations *SLMAX* is set to 0.8. Attackers assumedly change CP during peak hours.

B. Results and Discussion

The most important buses are demonstrated in Table I. It is conspicuous that the reserved DGs are not able to compensate the power instability. This table provides accurate information about the most potentially attacked buses. Thus, XFCs located at buses ϒ={21, 39, 64, 68, 84, 87, 197, and 251} should be protected more. These XFCs are chosen to evaluate EVUR. However, there are 5 reserved DGs for compensating exceeded demand, these units are not able to cope with the malicious consequence of the proposed attacks. Table II indicates this issue.

Fig. 5 illustrates the results of the proposed model for maximization of EV user satisfaction, as well as the EV load curve obtained after optimization. Due to the fact that EV users charge their EVs according to their own preferences, load changes are generally concentrated during peak periods, and this results in an increase in the load demanded during peak periods. It can be seen that the load during peak hours has been increased by 92.156 MW.

TABLE I. LOAD SHEDDING AFTER THE PROPOSED ATTACK

# of attacked XFCs	List of attacked buses	ALS (MW)
7	39,50,57,64,87,107,112	41.21
10	1,21,39,57,64,84,87,100,197,251	58.564
12	1,14,21,31,39,50,57,68,77,84,87,107	70.845
13	14,21,39,64,68,77,84,87,110,152,197,251,350	76.125
14	14,21,31,39,50,64,68,84,100,107,112,152,197,251	81.196
15	21,31,39,64,68,77,84,87,100,107,112,152,197,251,350	82.451

TABLE II. LOAD SHEDDING AFTER THE PROPOSED ATTACK AND DG PLACEMENT

# of attacked XFCs	List of attacked buses	ALS (MW)
7	39,50,57,64,87,107,112	40.81
10	1,21,39,57,64,84,87,100,197,251	58.064
12	1,14,21,31,39,50,57,68,77,84,87,107	70.545
13	14,21,39,64,68,77,84,87,110,152,197,251,350	76.025
14	14,21,31,39,50,64,68,84,100,107,112,152,197,251	80.896
15	21,31,39,64,68,77,84,87,100,107,112,152,197,251,350	82.151

VI. SUMMARY AND CONCLUSION

This paper conducted research to enhance the power continuity security in a power grid. To secure the supply and demand balance, through study of EV owner response under the coordinated cyber-attack which resulted in change of the CP. Considering the attackers' perspective and their criteria to compromise an attack helps system operators and planners to improve the grid security. Thus, a two-stage optimization model was introduced. The first stage of this framework aimed at detecting the most potentially attacked EVCSs in the IEEE 123-bus distribution test system. In this work, the renewable energy sources, apart from the classic DG units and other traditional electricity supplies, were employed. To evaluate the worst-case situations, this paper has mainly focused on XFCs which are fast-developed types of chargers propagated throughout the world. It has been proved that, even with using DGs, the amount of load shedding has risen to 82.151 MW. In the second stage, the EV owner response

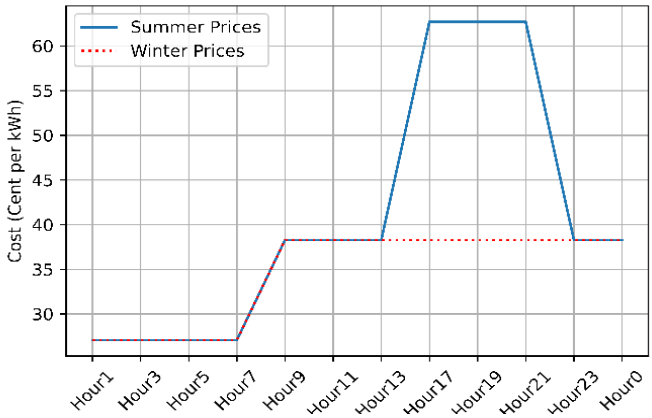

Fig. 4. Electricity price during Summer and Winter based on ToU bidding

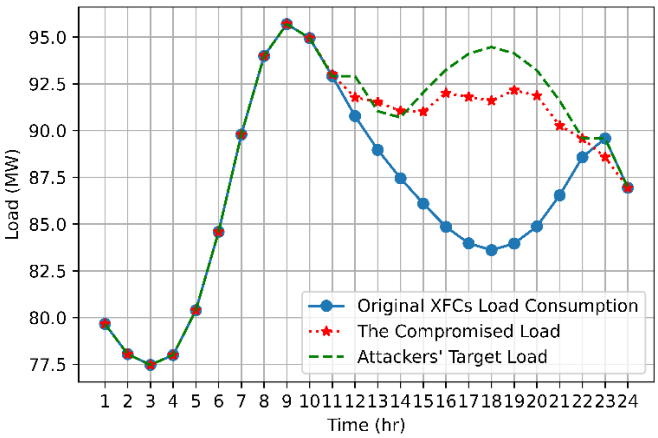

Fig. 5. Daily load curve before and after FDIA versus CP

to the changed CP due to the cyber attack was formulated. The results implied that after compromising the CPs during peak hours, the load demanded by EV users was increased to 92.156 MW. This huge consumption can cause voltage and a frequency instability.

REFERENCES

[1] S. Habib, M. M. Khan, F. Abbas, L. Sang, M. U. Shahid, and H. Tang, "A Comprehensive Study of Implemented International Standards, Technical Challenges, Impacts and Prospects for Electric Vehicles," *IEEE Access*, vol. 6, pp. 13866-13890, 2018, doi: 10.1109/ACCESS.2018.2812303.

[2] N. B. Arias, S. Hashemi, P. B. Andersen, C. Træholt, and R. Romero, "Distribution system services provided by electric vehicles: Recent status, challenges, and future prospects," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 12, pp. 4277-4296, 2019.

[3] E. Sortomme and M. A. El-Sharkawi, "Optimal charging strategies for unidirectional vehicle-to-grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 1, pp. 131-138, 2010.

[4] M. D. 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.

[5] 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*, vol. 11, no. 3, pp. 2218-2234, 2019.

[6] T. Nasr, S. Torabi, E. Bou-Harb, C. Fachkha, and C. Assi, "Power jacking your station: In-depth security analysis of electric vehicle charging station management systems," *Computers & Security*, vol. 112, p. 102511, 2022/01/01/ 2022, doi: https://doi.org/10.1016/j.cose.2021.102511.

[7] M. Kavianipour *et al.*, "Electric vehicle fast charging infrastructure planning in urban networks considering daily travel and charging behavior," *Transportation Research Part D: Transport and Environment*, vol. 93, p. 102769, 2021/04/01/ 2021, doi: https://doi.org/10.1016/j.trd.2021.102769.

[8] J. Xu, Z. Wu, X. Yu, S. Cheng, Q. Hu, and Q. Wu, "A Dynamic Robust Restoration Framework for Unbalanced Power Distribution Networks," *IEEE Trans. Ind. Informat.*, vol. 16, no. 10, pp. 6301-6312, Oct. 2020, doi: 10.1109/TII.2020.2964796.

[9] H. Tu, H. Feng, S. Srdic, and S. Lukic, "Extreme Fast Charging of Electric Vehicles: A Technology Overview," *IEEE Transactions on Transportation Electrification*, vol. 5, no. 4, pp. 861-878, 2019, doi: 10.1109/TTE.2019.2958709.

[10] D. Kosmanos *et al.*, "A novel Intrusion Detection System against spoofing attacks in connected Electric Vehicles," *Array*, vol. 5, p. 100013, 2020/03/01/ 2020, doi: https://doi.org/10.1016/j.array.2019.100013.

[11] A.-M. Hariri, M. A. Hejazi, and H. Hashemi-Dezaki, "Reliability optimization of smart grid based on optimal allocation of protective devices, distributed energy resources, and electric vehicle/plug-in hybrid electric vehicle charging stations," *Journal of Power Sources*, vol. 436, p. 226824, 2019/10/01/ 2019, doi: https://doi.org/10.1016/j.jpowsour.2019.226824.

[12] E. A. Pina, M. A. Lozano, and L. M. Serra, "Assessing the influence of legal constraints on the integration of renewable energy technologies in polygeneration systems for buildings," *Renewable and Sustainable Energy Reviews*, vol. 149, p. 111382, 2021/10/01/ 2021, doi: https://doi.org/10.1016/j.rser.2021.111382.

[13] L. Zhang, T. Brown, and S. Samuelsen, "Evaluation of charging infrastructure requirements and operating costs for plug-in electric vehicles," *Journal of Power Sources*, vol. 240, pp. 515-524, 2013/10/15/ 2013, doi: https://doi.org/10.1016/j.jpowsour.2013.04.048.

[14] P. ISO. *Markets & operations, energy markets. Dayahead energy market*. [Online]. Available: http://www.pjm.com/marke ts-and-operations /energ y/real-ti-me/hourl y-preli m-loads .aspx

[15] B. Xu and Z. Arjmandzadeh, "Parametric study on thermal management system for the range of full (Tesla Model S)/compact-size (Tesla Model 3) electric vehicles," *Energy Conversion and Management*, vol. 278, p. 116753, 2023.

[16] W. Kong, Z. Y. Dong, Y. Jia, D. J. Hill, Y. Xu, and Y. Zhang, "Short-term residential load forecasting based on LSTM recurrent neural network," *IEEE transactions on smart grid*, vol. 10, no. 1, pp. 841-851, 2017.