Coordinated EV Charging Attacks to Cause Transmission Line Overloads

Mahdi Bahrami
Montefiore Institute, Department of EE&CS
University of Liège
Liège, Belgium
mahdi.bahrami@uliege.be

Louis Wehenkel
Montefiore Institute, Department of EE&CS
University of Liège
Liège, Belgium
l.wehenkel@uliege.be

***Abstract*— This paper proposes a model for one of the most important cyber-attacks against an electric vehicle (EV) ecosystem. In the considered attack, the aim is to disrupt the normal operation of the transmission system (TS) by causing a spike in EV load demand in order to induce multiple branch overloads in the TS. We thus formulate a decision-making problem aiming at inducing line overloads by manipulating EV charging prices in different regions, while considering limited resources of the cyber-attacker and a simplified model of the TS. This problem is expressed from the attackers' perspective as a mixed-integer linear programming (MILP) problem of maximizing the total magnitude of branch overloads. To illustrate the proposed model, it is applied to the Roy Billinton Test System. The simulation results show that this attack strategy could cause some problems in the TS.**

***Keywords*— *Charging prices, cyber-attacks, electric vehicles, line overloads, transmission systems*[1]**

Indices and Sets

σ, Ω_σ	Index and set of regions.
d, Ω_d^σ	Index and set of DSs in region σ.
ij, Ω_{ij}	Index and set of transmission lines.
i, Ω_i	Index and set of transmission nodes.
g, Ω_g	Index and set of generating units.

Parameters and Constants

ε_σ	The resources required to compromise all EVCS servers in region σ.
$\Upsilon_\sigma^{\max}$	The maximum EV load demand that can be created by attackers in region σ.
N_σ^{ser}	Number of EVCS servers in region σ.
κ	Attackers' available resources in total.
P_g°	Economic base point of unit g before attack occurrence.
$P_g^{\Delta}, P_g^{\nabla}$	Upward and downward reserve of unit g.
pf_g	Participation factor of generation unit g.
$[B]$	Susceptance matrix.
X_{ij}	Reactance of line ij.
M	A large positive number.
$\bar{f}_{ij}$	Transmission line capacity.
P_i^{dem}	Non-EV load demand at node i.
P_i^{ev}	EV load at node i just before cyber attacks.

Variables

Γ_σ^{ev}	EV load demand induced by cyber attackers in region σ.
η_σ^{ser}	A non-negative integer variable representing the number of compromised EVCS servers in region σ.
$\bar{\Psi}_{ij}, \underline{\Psi}_{ij}$	Non-negative continuous variable representing the magnitude of branch overloads caused by the cyber attacks for positive and negative flow direction, respectively.
$\bar{\eta}_{ij}, \underline{\eta}_{ij}$	Binary variable representing whether transmission line ij has been respectively overloaded in positive or negative flow direction or not.
P_g^{gen}	Output power of unit g.
θ_i	Node phase angel (in radians).
f_{ij}^{line}	Power flow on transmission line ij.

Symbols and Acronyms

TS, DS	Transmission system and distribution system, respectively.

I. Introduction

In line with the de-carbonization of transportation systems, a rapid transition from internal-combustion-engine (ICE) vehicles to electric vehicles (EVs) is being made. As a result, the number of EVs is increasing rapidly. EVs are considered as a high-wattage demand-side appliance [1]. EVs are controllable

[1] This work has been prepared with the support of the Belgian Energy Transition Fund, project CYPRESS (https://cypress-project.be/).

loads to some extent as well [2]. Thus, EV users can participate in vehicle-to-grid (V2G) or grid-to-vehicle (G2V) programs through managing the charging/discharging process of their EVs. Based on the travel needs of EV users, the V2G/G2V programs are implemented in such a way that EV owners are encouraged to charge their EVs in valley period of grid load and discharge the stored energy in EV batteries in peak periods [3]. In this context, EVs can be viewed as DERs [4]. In addition, the cyber space of the EV ecosystem is complex and consists of multiple entities which interact with each other through physical and/or cyber connections [5]. Furthermore, EVs typically have interfaces with communication and control networks. Consequently, the EVs can be considered as a cyber-attack vector [6].

However, EV users may themselves respond to changes in prices by modifying their charging behavior [7]. Indeed, EV users are willing to charge their EVs with low electricity prices during low-price periods. In this regard, cyber attackers may find the EV load profile ideal to disrupt power grids. Indeed, the distinguishing feature of EVs, high-wattage demand, could be exploited by cyber attackers to disrupt normal operation of transmission systems. To this end, the attackers could manipulate EV charging prices to encourage EV users to charge their EVs during high-demand periods. Actually, the EV users would benefit from low charging cost in this situation. When a large number of EVs are charged in an uncoordinated way, the imbalance between generation and demand can cause several problems, including overloads and frequency drop [5].

In the literature, there are a few studies focused on the possible impacts caused by cyber-attacks against EVs on power systems. Most of these studies analyze the possible impacts on DSs. In contrast, the research works concerned with analyzing their impacts on TSs are scarce in the literature. In [8], the effect of cyber-attacks against EVs on the TS operation is studied. It is concluded that such attacks could cause line congestion in TSs, and the attack could even cause line tripping by triggering the protection system, if the increase in load is significant. The authors in [6] implied that a frequency drop can be caused by a surge in EV user demand. This might create subsequent impacts such as generation unit disconnection. This condition might lead to voltage collapse or even frequency instability. Although these studies provide valuable results, they do not incorporate the attackers' perspective into the model for measuring the overloads induced by cyber-attacks on EV charging process. In other words, they consider the cyber-attacks aiming to increase EV load demand as a specific increase in loads, and then power flow analysis is deployed to measure the magnitude of overloads.

On the above premises, this paper proposes a novel formulation that models the cyber-attackers' decision-making problem of overloading transmission lines through manipulating EV charging prices. In this paper, the attackers conduct the cyber-attack during power-grid peak-load hours. In doing so, EV peak load would overlap with power system peak load, and additional stress is put on the system. The problem is formulated as a mixed-integer linear programming (MILP) optimization model. The model is presented from the attackers' viewpoint. The cyber attackers control some decision variables, including the regions to be attacked and the resources to be allocated to targeted regions. These decisions are made by the attackers in such a way that the amount of transmission line overloads is maximized. In this regard, the main contributions of this paper are as follows:

- Proposing a novel formulation for modeling the cyber-attacker decision-making problem of causing overloads in TS through launching cyber-attacks against EV charging prices.
- Modeling the problem as a MILP optimization model, while considering attack resources for compromising EVCS servers.

The remainder of this paper is organized as follows: First, the problem under study and the hypothesized cyber-attack scenario are introduced in Section II. The rest of this section is devoted to DS modeling and the decision variables of cyber attackers. Section III formulates the problem as a MILP optimization model. The simulation results are presented and discussed in Section IV. Finally, Section V concludes the paper.

II. Coordinated Charging Attack on Transmission Networks

A. *Problem Definition*

Cyber attackers might target the EV charging process to impact TSs. To this end, the attackers could try to abruptly increase the load demanded by EV users through launching cyber-attacks against charging prices. In doing so, the transmission system is indirectly impacted, and significant stress may be put by cyber attackers on the transmission system. They may make the attack more impactful by launching the attack during on-peak periods. This type of cyber-attacks could lead to multiple transmission line overloads. In this regard, although the cyber-attacks are launched at distribution levels, they could impact both DS and TS.

In this study, the problem is presented from the viewpoint of cyber attackers. In addition, the impact assessment is done at transmission levels. In this problem, the cyber attackers aim to launch cyber-attacks from DSs in a coordinated way to target TS lines. Using this strategy, they aim at causing overloads. In other words, the attackers' goal is to overload some transmission lines during attack time. However, the resources used by the cyber attackers to target EV users in different regions are limited by a prespecified budget. Therefore, they could not target all regions simultaneously, and they should decide how to use the available attack resources. This decision-making process is modeled as a MILP optimization problem. In this regard, the problem can be translated as locating and allocating the attack resources to the regions where the impacts of such attacks are amplified. It should be mentioned that each transmission node and its associated loads construct a region.

In this sense, transmission nodes and regions are used interchangeably in the text.

B. *Hypothesized Cyber Attack Scenario*

Cyber attackers manipulate EV charging prices such that EV users show desire to charge their EVs. However, the EV ecosystem consists of multiple entities communicating with one another. In this study, cyber attackers target EV Charging Station (EVCS) servers to change EV charging prices. As can be traced in Fig. 1, EV users interact with EVCS servers via EV charging Apps, such as ChargePoint [1]. After successful intrusion into EVCS servers, the cyber attackers maliciously change EV charging prices for the attack interval. Thus, EV users see the manipulated prices on EV charging Apps [9].

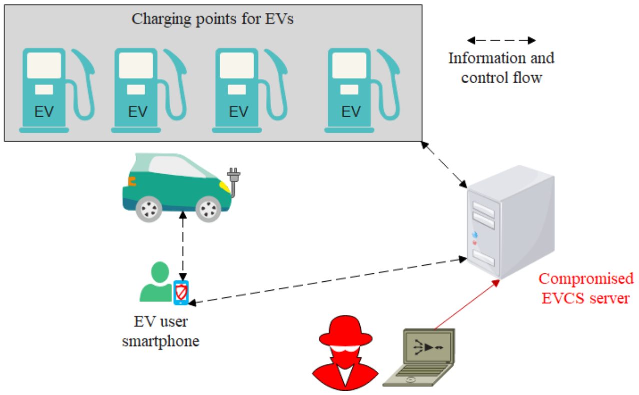

Fig. 1. Schematic view of the cyber-attack scenario.

It is assumed that time of use (ToU) price structure is deployed by EV charging providers. Under ToU pricing, three different charging prices are usually offered. In addition, based on the day and time, charging prices are given for on-peak, off-peak, and early bird hours [10]. In this paper, it is assumed that on the attack day, the charging price ranges for the different periods and different locations, which are given Table I. It is worth mentioning that these prices are derived from the ‘‘EVgo’’ company’s website [11].

TABLE I
True ToU Prices for EV charging on the Attack Day

	Early bird	Off-peak	On-peak
Hours	12am-8am	8am-4pm, 9pm-12am	4pm-9pm
Price ($/kWh)	0.36 to 0.49	0.41 to 0.56	0.46 to 0.63

In the hypothesized cyber-attack scenario, cyber attackers manipulate EV charging prices during peak-EV-load period. In doing so, it overlaps with the power grid peak-load period. In addition, the manipulated prices are set to 0.36 $/kWh. Thus, it cannot easily be detected, and EV users get it as a special offer. In addition, the targeted EV users are encouraged to charge their EVs. Furthermore, it is assumed that the number of responsive EV users receiving the offer in compromised regions is higher than that of charging outlets. So, all charging points are occupied by EV users.

C. *DS Modeling*

For analyzing the impacts of the cyber-attacks against EV charging prices, both the DS and the TS should be analyzed at once. In other words, a co-simulation framework is required. However, this could make the problem very complex. To tackle this issue, some simplifications can be made. For instance, each distribution system is modeled as lumped loads in the transmission system. In this study, each load point in TS consists of two main loads, namely non-EV loads and EV loads. However, the EV load at each transmission load point is considered as a variable. In other words, based on how cyber attackers allocate the attack resources to different regions, the amount of it can be changed.

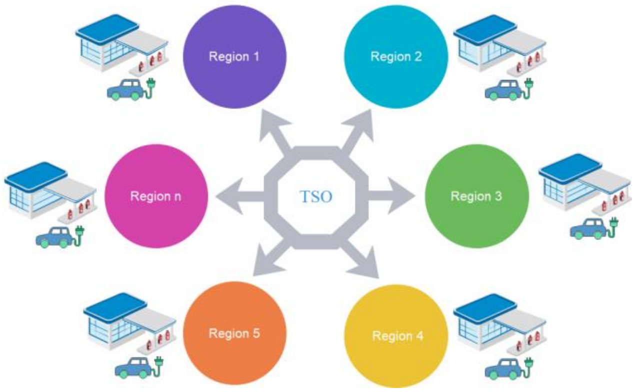

Fig. 2. A power grid with a TSO and *n* regions hosting EVCSs.

D. *Attackers’ Decision Variables*

As shown in Fig. 2, the transmission grid is connected to *n* regions. Each region can host EV charging points. In this regard, the cyber attackers should answer this question:

- Which EV-hosting regions should be compromised to maximize the total magnitude of overloads in the TS?
- How many EVCS servers should be compromised in each region?
- How available resources should be allocated to each region?

Considering the above questions, cyber attackers have control of the independent decision variable η_{σ}^{ser} representing the number of compromised EVCS servers in each region. Additionally, there are two other dependent variables that are controlled by the attackers, namely attacker-induced EV demand and allocated resources to each region.

III. Problem Formulation

In this section, the proposed formulation is presented. It is worth mentioning that the formulation models attackers’ decision-making problem. In addition, an approximation of DC-power flow is deployed by attackers to analyze the behavior of the targeted TS immediately after cyber-attacks. Thus, only the automatic response of generating units is taken into account. In other words, the response of transmission system operator (TSO) to the attacks is not incorporated into the model, and it is outside the scope of this paper.

A. *Attackers' Objective*

The attackers' objective is to maximize the total magnitude of transmission-line overloads caused by the cyber-attacks. Therefore, the objective function is expressed as follows:

$$\max \sum_{\forall ij} (\bar{\Psi}_{ij} + \underline{\Psi}_{ij}) \tag{1}$$

Two non-negative variables $\bar{\Psi}_{ij}$ and $\underline{\Psi}_{ij}$ represent the magnitude of overloads in positive and negative flow directions, respectively.

B. *Constraints*

This optimization problem has several equality and inequality constraints, which are given in (2)-(4j):

$$\sum_{\sigma} (\varepsilon_{\sigma} . \frac{\eta_{\sigma}^{ser}}{N_{\sigma}^{ser}}) \le \kappa \tag{2}$$

The budget for performing the cyber-attacks against EVs is limited by κ . This is imposed by constraint (2). As an approximation, it is assumed that the EV load induced by the cyber-attacks is proportional to the number of compromised EVCS servers in the region. This is given by (3).

$$\Gamma_{\sigma}^{ev} = \frac{\eta_{\sigma}^{ser}}{N_{\sigma}^{ser}} . \Upsilon_{\sigma}^{\max} \quad \forall \sigma \tag{3}$$

The extra EV load demand triggered by the cyber-attacks is upper bounded in each region by $\Upsilon_{\sigma}^{\max}$. This value depends on the number of charging points as well as the charging levels of charging outlets. When the cyber attackers do not target the EVs of a region, the EV demand induced by the cyber-attacks must be equal to zero.

$$[B]\theta = P^{gen} - P^{dem} - P^{ev} - \Gamma^{ev} \tag{4a}$$

$$P_{g}^{gen} = P_{g}^{\circ} + pf_{g}\, \Delta P_{tot}^{d} \quad \forall g \in \Omega_{g} \tag{4b}$$

$$0 \le \bar{\Psi}_{ij} \, , \underline{\Psi}_{ij} \quad \forall ij \in \Omega_{ij} \tag{4c}$$

$$(f_{ij}^{line} - \bar{f}_{ij}) - M(1-\bar{\eta}_{ij}) \le \\ \bar{\Psi}_{ij} \le (f_{ij}^{line} - \bar{f}_{ij}) + M(1-\bar{\eta}_{ij}) \quad \forall ij \in \Omega_{ij} \tag{4d}$$

$$-\bar{f}_{ij} - f_{ij}^{line} - M(1-\underline{\eta}_{ij}) \le \\ \underline{\Psi}_{ij} \le -\bar{f}_{ij} - f_{ij}^{line} + M(1-\underline{\eta}_{ij}) \quad \forall ij \in \Omega_{ij} \tag{4e}$$

$$\bar{\Psi}_{ij} \le \bar{\eta}_{ij} . M \quad \forall ij \in \Omega_{ij} \tag{4f}$$

$$\underline{\Psi}_{ij} \le \underline{\eta}_{ij} . M \quad \forall ij \in \Omega_{ij} \tag{4g}$$

$$f_{ij}^{line} = \frac{\theta_i - \theta_j}{X_{ij}} \quad \forall ij \in \Omega_{ij} \tag{4h}$$

$$\theta_1 = 0 \tag{4i}$$

$$-\pi \le \theta_i \le \pi \quad \forall i \in \Omega_N \, , i \ne 1 \tag{4j}$$

Equation (4a) stands for the general representation of power balance at nodes. At each node, the load demand is split into non-EV loads (P_i^{dem}) and EV loads. In addition, EV load demand consists of two terms: EV load demand in normal non-attack condition (P_i^{ev}) and the EV load demand induced by cyber attackers (Γ^{ev}). The former is taken as a parameter, while the latter is a variable in this model and depends on how cyber attackers use their resources. However, the generation units respond to changes in total system demand based on their participation factors, which is shown in (4b). Thus, the new value of generation for each unit is given by (4b). In this equation, P_g° is the initial generation of unit *g*. It is calculated by solving the DC optimal power flow (OPF) problem [12]. In (4b), ΔP_{tot}^{d} represents the change in total system demand after the occurrence of the cyber-attacks. It is a variable in the proposed formulation. Additionally, its value is equal to the total EV load demand induced by the cyber-attacks in regions.

In order to measure the magnitude of transmission line overloads, a set of constraints is proposed, which are given by (4c)-(4g) [13]. Two non-negative variables are defined for measuring the overloads for both power-flow directions. $\bar{\Psi}_{ij}$ represents the overloads for positive power flow, while $\underline{\Psi}_{ij}$ stands for the amount of line overloads in the negative flow direction. However, when the amount of power flow is within the bounds, both $\bar{\Psi}_{ij}$ and $\underline{\Psi}_{ij}$ must be equal to zero. If the power flow on transmission line *ij* hits its limit either in positive or in negative direction, $\bar{\Psi}_{ij}$ or $\underline{\Psi}_{ij}$ gets a positive value, respectively. This is ensured by (4d) and (4e). To this end, two binary variables are defined for each transmission line, namely $\bar{\eta}_{ij}$ and $\underline{\eta}_{ij}$. These variables flag overloaded lines in positive and negative follow direction, respectively. In addition, the amount of overloading in positive or negative flow direction is equal to the difference between power flow and line capacity.

On this basis, the big-M method is utilized in (4d) and (4e) to ensure the abovementioned requirements.

Constraints (4f) and (4g) ensure that when a line is overloaded, it is flagged as an overloaded line. Equation (4h) represents the relationship between the power flow on a transmission line and its both ending voltage angles. Voltage angle limits are imposed by constraints (4i) and (4j).

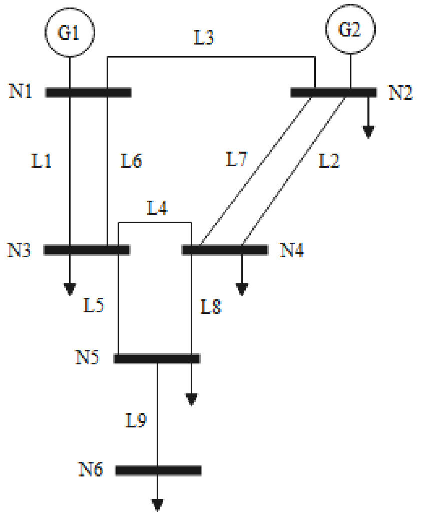

Fig. 3. Single-line diagram of the RBTS.

IV. Simulation Results

In this section, a modified version of the Roy Billinton Test System (RBTS) is utilized as the test system [14]. The single-line diagram of this test network is shown in Fig. 3. The proposed MILP model was implemented and solved in the GAMS environment.

A. *Main Assumptions*

There are charging levels 2 and 3 in the regions. Detailed information about them in terms of charging power and total number of charging outlets in each region is given in Tables II and III, respectively.

TABLE II
Charging Power of Charging Outlets [15]

	Level 2	**Level 3**
Charging power (kW)	11 to 24	50 to 360

TABLE III
Total Number of Charging Outlets and the Total EV Load under Simultaneous Charging in the Regions

Region #	**Level 2**	**Level 3**	**Total Capacity (MW)**
N1	0	0	0
N2	200	50	7
N3	300	250	24
N4	250	130	14
N5	200	50	7
N6	200	50	7

Table IV lists the number of EVCS servers and the resources required for compromising them in each region. In addition, it represents the maximum EV load demand induced by the cyber-attacks ($\Upsilon_\sigma^{\max}$) as well as the EV load demand in each region just before the cyber-attack occurrence (P_i^{ev}).

TABLE IV
Total Number of EVCS Servers, the Maximum Attack-Created EV Load Demand, and EV Load Before the Attacks in the Regions

Region #	N_σ^{ser}	ε_σ	$\Upsilon_\sigma^{\max}$ **(MW)**	P_i^{ev} **(MW)**
N1	0	0	0	0
N2	2	2	6	1
N3	5	5	20	4
N4	3	3	12	2
N5	2	2	6	1
N6	2	2	6	1

As can be traced in Table IV, the simultaneous charging of all charging points requires the power of 59 MW, while the total amount of non-EV peak load is 176 MW. It is assumed that an EV load of 9 MW was already at EV charging stations once the attack interval starts. In the simulations, the amount of attackers' resources for targeting EVCS servers is set to 7. In the simulations, a unit of attack resources refers to a specific amount of money that cyber-attackers need to spend on the cyber-attack implementation. As realistic data on them are not publicly available, the resources are considered in this way.

To simulate a stressed operational condition, the capacities of the transmission lines are changed, which are listed in Table V. In addition, it is assumed that the system is on-peak hours at the cyber-attack onset. In addition, the load demand connected to each transmission node in Fig. 3 consists of both non-EV load and EV load in attack time. Furthermore, the upward capacity of generation units 1 and 2 is assumed to be 15 percent of its generation capacity. The generation capacity of units 1 and 2 is respectively 110 MW and 130 MW. Considering the upward reserve of generation units 1 and 2, the participation factors of units 1 and 2 are respectively equal to 0.458 and 0.542.

TABLE V
Power Flow on Lines in Pre- and Post-Attack Conditions and Their Corresponding Overloads after the Occurrence of the Cyber Attacks

Lines	**Capacity (MW)**	**Initial Power Flow (MW)**	**Power Flow (MW)**	**Overload (%)**
1-3, L1	50	45.94	**53.47**	6.94
2-4, L2	40	36.56	**43.03**	7.58
1-2, L3	30	0.62	-1.616	0
3-4, L4	20	-8.75	-12.05	0
3-5, L5	30	15.62	13.98	0
1-3, L6	50	45.94	**53.47**	6.94
2-4, L7	40	36.56	**43.03**	7.58
4-5, L8	30	24.37	26.02	0
5-6, L9	25	20	20	0

B. *Results*

Under the assumed conditions, the cyber attackers would be able to cause four simultaneous line overloads. The power flows before and after the occurrence of the attacks are reported in Table V. In addition, the magnitude of each overloaded line is presented in this table. As can be traced in this table, line L2 and L7 become overloaded by more than 7.5 percent of their capacity. The total amount of line overloads is 13 MW as well.

However, to induce the four overloads, cyber attackers target two regions. Table VI lists the attacked region and the number of compromised EVCS servers in the regions. Additionally, it shows how they use the available resources to maximize the total magnitude of overloads. In this sense, the DSs connected to nodes 3 and 4 are selected as the target of the cyber-attacks. The attackers allocate five units of the available resources to N3. As a consequence, an EV load of 20MW is induced by the attackers in region N3. However, two units of the resources used for attacking region N4, thereby inducing the EV load demand of 8 MW.

TABLE VI
Cyber-Attack Resource Allocation to the Regions

Region #	Γ_{σ}^{ev} **(MW)**	η_{σ}^{ser}	**Deployed Resources**
N1	0	0	0
N2	0	0	0
N3	20	5	5
N4	8	2	2
N5	0	0	0
N6	0	0	0

Pursuing the analysis from generation unit perspective, Table VII lists the output power of the generation units in two conditions: Before the start of the cyber-attacks and immediately after the attack onset. Before the occurrence of the cyber-attacks, the system is in normal condition. Therefore, the initial unit generations are obtained by solving the DC-OPF problem for the modified version of the RBTS. Immediately after the attacks, the total load is increased by 28 MW. Accordingly, the total generation is increased. However, the total change in generation is divided between the units based on the participation factors.

TABLE VII
Generation Dispatch before and after the Cyber Attacks

Generation	**Before Attacks**	**After Attacks**
P_1^{gen}	92.49	105.31
P_2^{gen}	92.51	107.69

V. Conclusion and Summary

In this paper, we have modeled the cyber-attacker decision-making problem for inducing overloads in transmission systems. They launch coordinated cyber-attacks against EV charging prices in different regions to encourage EV users to charge their EVs during the attack interval. However, as their resources are limited, they should decide how to use their available resources to maximize the amount of transmission line overloads.

The proposed model was implemented in a modified version of RBTS. The results illustrate that such attacks could put significant stress on transmission lines and generation systems. The reason behind this lies in the fact that EVs are high-wattage assets. More specifically, the simulation results showed that the attacks that are launched during system peak times and on impactful targets can induce four branch overloads in the test system. Thus, this paper aims at not only proposing a new MILP optimization model for the problem, but also raising awareness about the impacts that can be caused by such attacks.

References

[1] S. Acharya, Y. Dvorkin and R. Karri, "Public Plug-in Electric Vehicles + Grid Data: Is a New Cyberattack Vector Viable?," in *IEEE Trans. Smart Grid*, vol. 11, no. 6, pp. 5099-5113, Nov. 2020, doi: 10.1109/TSG.2020.2994177.

[2] Y. Du, T. Li, M. Li and Y. Sun, "V2G Multi-Objective Optimization Considering Data-Driven User's Demand Response," *2022 IEEE/IAS Industrial and Commercial Power System Asia (I&CPS Asia)*, Shanghai, China, 2022, pp. 1002-1008, doi: 10.1109/ICPSAsia55496.2022.9949925.

[3] H. Saber, H. Ranjbar, S. Fattaheian-Dehkordi, M. Moeini-Aghtaie, M. Ehsan and M. Shahidehpour, "Transactive Energy Management of V2G-Capable Electric Vehicles in Residential Buildings: An MILP Approach," in *IEEE Trans. Sustain. Energy*, vol. 13, no. 3, pp. 1734-1743, July 2022, doi: 10.1109/TSTE.2022.3173943.

[4] B. Wang, P. Dehghanian, S. Wang and M. Mitolo, "Electrical Safety Considerations in Large-Scale Electric Vehicle Charging Stations," in *IEEE Trans. Ind. Appl.*, vol. 55, no. 6, pp. 6603-6612, Nov.-Dec. 2019, doi: 10.1109/TIA.2019.2936474.

[5] N. Bhusal, M. Gautam and M. Benidris, "Cybersecurity of Electric Vehicle Smart Charging Management Systems," *2020 52nd North American Power Symposium (NAPS)*, Tempe, AZ, USA, 2021, pp. 1-6, doi: 10.1109/NAPS50074.2021.9449758.

[6] M. A. Sayed, R. Atallah, C. Assi, and M. Debbabi, “Electric vehicle attack impact on power grid operation,” *Int. J. Electr. Power Energy Syst*., vol. 137, May 2022, Art. no. 107784.

[7] H. S. Karimi, K. Jhala and B. Natarajan, "Impact of Real-Time Pricing Attack on Demand Dynamics in Smart Distribution Systems," *2018 North American Power Symposium (NAPS)*, Fargo, ND, USA, 2018, pp. 1-6, doi: 10.1109/NAPS.2018.8600625.

[8] O. G. M. Khan, E. El-Saadany, A. Youssef and M. Shaaban, "Impact of Electric Vehicles Botnets on the Power Grid," *2019 IEEE Electrical Power and Energy Conference (EPEC)*, Montreal, QC, Canada, 2019, pp. 1-5, doi: 10.1109/EPEC47565.2019.9074822.

[9] A. Akbarian, M. Bahrami, M. Vakilian and M. Lehtonen, "Vulnerability of EV Charging Stations to Cyber Attacks Manipulating Prices," *2023 International Conference on Future Energy Solutions (FES)*, Vaasa, Finland, 2023, pp. 1-6, doi: 10.1109/FES57669.2023.10183070.

[10] B. M. Davis and T. H. Bradley, "The Efficacy of Electric Vehicle Time-of-Use Rates in Guiding Plug-in Hybrid Electric Vehicle Charging Behavior," in *IEEE Trans. Smart Grid*, vol. 3, no. 4, pp. 1679-1686, Dec. 2012, doi: 10.1109/TSG.2012.2205951.

[11] [Online]. Available: https://www.evgo.com/

[12] Allen J. Wood, et al. Power Generation, Operation and Control, 3rd ed. John Wiley & Sons, Inc, Hoboken, New Jersey, 2013.

[13] E. Karangelos and L. Wehenkel, “Cyber-physical risk modeling with imperfect cyber-attackers,” in *Electr. Power Syst. Research*, vol. 211, p. 108437, 2022.

[14] R. Billinton and S. Jonnavithula, "A test system for teaching overall power system reliability assessment," in *IEEE Trans. Power Syst.*, vol. 11, no. 4, pp. 1670-1676, Nov. 1996, doi: 10.1109/59.544626.

[15] [Online]. Available: https://new.abb.com/ev-charging