CLAC-SCO: Coordinated Load Alteration via Compromised Smart Charging Orchestrator

Koordineli Yük Değişikliği Saldırısı — Anomali Senaryosu ve Öneriler

1. Özet

Bu belge, akıllı şarj orkestratörlerinin veya aggregator yazılımlarının ele geçirilmesiyle gerçekleştirilebilecek yeni bir anomali/saldırı senaryosunu tanımlar: Coordinated Load Alteration via Compromised Smart Charging Orchestrator (CLAC-SCO). Saldırgan, ele geçirilen orkestratör vasıtasıyla çok sayıda şarj noktasına eşzamanlı olarak şarj profili değişikliği enjekte ederek dağıtım/iletim şebekesinde ani yük değişimleri oluşturur. Amaç finansal suistimal, piyasa manipülasyonu veya şebeke kararsızlığı üretmektir.

2. Saldırı Yüzeyleri (Attack Surface)

- Orkestratör / aggregator bulut hizmetleri, yönetim panelleri, API anahtarları.
- OCPP, Smart Charging API'leri ve market bidding API'leri gibi kontrol kanalları.
- Zayıf kimlik/erişim kontrolleri, CI/CD pipeline'da sızdırılmış secret'lar.
- Tedarik zinciri (third-party yazılım/agent) kompromisi.

3. Adım-Adım Saldırı Akışı

1. Keşif ve erişim kazanma: spear-phishing, credential stuffing veya CI secret leak ile orkestratöre erişim.
2. Agent dağıtımı/komutlanması: Orkestratör üzerinden toplu 'override' komutları gönderilmesi.
3. Koordineli zamanlama: Pik öncesi veya piyasa sinyallerine göre zamanlanmış toplu şarj profili değişiklikleri.
4. Maskelenme ve persistence: Telemetri manipülasyonu veya timing varyasyonları ile tespitten kaçınma.

4. Etki (Impact)

- Şebeke güvenliği: Ani yük artışları trafoları zorlayabilir, koruma cihazları tetiklenebilir, voltaj/akım dengesizliği oluşabilir.
- Ekonomik: Spot piyasa fiyatlarının manipülasyonu yoluyla finansal kazanç sağlanabilir.
- Hizmet kesintisi: Kritik bölgelerde şarj erişimi azalır, kullanıcı güveni sarsılır.
- Regülasyon ve itibar: Operatörler yaptırım ve itibar kaybı riskiyle karşılaşır.

5. Tespit Göstergeleri (Indicators)

- Aynı bölgedeki çok sayıda charger'da kısa zamana yayılmış benzer profil değişimleri (temporal correlation).
- Orkestratör API'lerinde sıra dışı override çağrıları, yeni token kullanımları, başarısız oturum denemeleri.
- Trafo/feeder telemetrilerinde beklenmeyen dalgalanmalar; market price feed ile uyumsuz hareketler.
- SIEM/EDR'de orkestratörden gelen anormal zamanlanmış taleplerin artışı.

6. Önerilen Önlemler (Mitigations)

Önlem	Açıklama

Least-privilege & secret hygiene	KMS kullanımı, secret rotation, CI/CD secret scanning, agent-başına sertifika ve mTLS.
Anomali tespiti — multi-source correlation	Charging logs + grid telemetry + market data'nın gerçek-zamanlı korelasyonu; sliding-window detection.
Rate limiting & scheduling guardrails	Toplu override'lara limit, phased rollout ve manuel onay eşiklerinin zorunlu kılınması.
Local fallback & graceful degrade	Charger'ların merkezi komutları reddeden veya doğrulayan yerel politikaları olması.
Threat intel & SOAR integration	Spot price anomaly'lerini ve orchestration kontrol sinyallerini SOAR ile otomatik yanıtlamak.

7. PoC / Laboratuvar Deneyi (Etik çerçeve)

Önerilen laboratuvar kurulumu: 50 sanal charger agent, bir orkestratör emülasyonu ve basit bir dağıtım feeder modeli (ör. GridLAB-D veya pandapower). Saldırı: Orkestratörden eşzamanlı 'increase charging power by X kW' komutu gönderilerek trafo akım/voltaj etkileri gözlenir. Tüm testler kapalı ortamda ve gerekli izinler alınarak gerçekleştirilmelidir.

8. Seçme Kaynaklar / Literatür (Destekleyici Makaleler)

1. Acharya et al., 'MaDEVIoT: Cyberattacks on EV Charging Can Disrupt Power Grids', arXiv 2023 — dağıtım seviyesinde coordinated saldırı riskleri.
2. Ghafouri et al., 'Coordinated Charging and Discharging of Electric Vehicles: A New Class of Switching Attacks', ACM 2022 — koordine switching saldırıları PoC.
3. Jahangir et al., 'Charge manipulation attacks against smart electric vehicle charging systems', WRAP 2024 — charge manipulation kavramı ve tespit önerileri.
4. Sayed et al., 'Uncertainty-conscious robust dynamic EV load-altering attacks', Applied Energy 2024 — dinamik saldırı modelleri.
5. Tanyıldız et al., 'Detection of cyber attacks in electric vehicle charging', Scientific Reports 2025 — attack detection yaklaşımları.

9. Hızlı Öneriler ve Sonraki Adımlar

1) Risk matrisini (olasılık × etki) çıkarın; yüksek öncelikli mitigasyonları uygulayın.
2) Orchestator erişimlerini KMS ve MFA ile güvene alın; CI/CD taramalarını aktif edin.
3) SIEM'de multi-source correlation kurun; anomali tespit modellerini lab ortamında eğitin ve test edin.
4) Orkestratörde bulk override için guardrail'lar ekleyin; phased rollout politikası uygulayın.

Hazırlayan: ChatGPT — Senaryo: CLAC-SCO. Hazırlayan kişi için: Şeref (Osama).

Ek: Kaynak Makale

Bu bölümde, CLAC-SCO anomali senaryosunu destekleyen akademik kaynak olarak Acharya ve arkadaşlarının hazırladığı “MaDEVIoT: Cyberattacks on EV Charging Can Disrupt Power Grid Operation” başlıklı makalenin tam metni sunulmaktadır. (arXiv:2311.06226, 2023)

Sayfa aşağısında makalenin orijinal içeriği başlar.

MaDEVIoT: Cyberattacks on EV Charging Can Disrupt Power Grid Operation

Samrat Acharya*, Hafiz Anwar Ullah Khan†, Ramesh Karri†, and Yury Dvorkin‡
* *Pacific Northwest National Laboratory, Richland, WA 99354, USA*
† *Department of Electrical and Computer Engineering, New York University, Brooklyn, NY 11201, USA*
‡ *Ralph O'Connor Sustainable Energy Institute, Department of Electrical and Computer Engineering, Department of Civil and Systems Engineering, Johns Hopkins University, Baltimore, MD 21218, USA*
{samrat.acharya}@pnnl.gov

***Abstract*—This paper examines the feasibility of demand-side cyberattacks on power grids launched via internet-connected high-power EV Charging Stations (EVCSs). By distorting power grid frequency and voltage, these attacks can trigger system-wide outages. Our case study focuses on Manhattan, New York, and reveals that such attacks will become feasible by 2030 with increased EV adoption. With a single EVCS company dominating Manhattan, compromising a single EVCS server raises serious power grid security concerns. These attacks can overload power lines and trip over-frequency (OF) protection relays, resulting in a power grid blackout. This study serves as a crucial resource for planning authorities and power grid operators involved in the EV charging infrastructure roll-out, highlighting potential cyberthreats to power grids stemming from high-power EVCSs.**

I. Introduction

The widespread adoption of Electric Vehicles (EVs) is crucial for global decarbonization, but it raises concerns about cybersecurity for the electric power infrastructure. Cyberattacks on power grids have increased globally, with 45 attacks since 2017 and 13 in 2022 [1]. Financial losses from cyber breaches in the energy sector have risen by 13% from 2019 to 2020. Such cybersecurity assessments focus on utility-side devices and networks, underestimating risks from high-wattage demand-side resources like IoT-enabled EV chargers. EV chargers are not typically monitored by grid operators, which exacerbates the poor security hygiene in their operation and complex supply chains [2], [3].

Studies have analyzed the impacts of demand-side cyberattacks on power grids, highlighting the vulnerabilities posed by Manipulation of Demand via IoT (MaDIoT) attacks on IoT-controlled HVAC loads [4], [5]. In contrast to previous studies, this paper focuses on *Manipulation of Demand via EV IoT (MaDEVIoT)* attacks launched by bots comprised of EV charging systems. These attacks involve coordinated Distributed Denial-of-Service (DDoS) attacks on EV charging stations (EVCSs) and servers, abruptly interrupting EV charging.

Recent studies have focused on the feasibility of *MaDEVIoT* attacks [6]–[10]. Remote attackers can destabilize urban power grids using publicly available power grid and EV charging data [6]. EV charging loads require lower capacity to destabilize power grids compared to conventional IoT-enabled residential loads due to higher reactive power of the former [7]. Coordinated charging/discharging power manipulation can further amplify the impact on power grid stability [9]. Coordinating EV charging demand manipulations with natural or technical disturbances requires fewer manipulations to destabilize the power grid [8]. Attacks on EV charging can result in both over-frequency and under-frequency events in power grids [10].

Literature on *MaDEVIoT* [7]–[10] highlights the distinct nature of EV loads in terms of attack severity and success, but relies on generic power system test beds and EV charging data. The study in [6] addresses some limitations but lacks detailed transient-state analysis and considers status-quo EV penetration. Moreover, the studies have demonstrated the feasibility of *MaDEVIoT* attacks on power grids assuming a massive hypothetical EV roll-out. In contrast to [6]–[10], this paper investigates when *MaDEVIoT* attacks become feasible based on transportation electrification plans. Additionally, it explores how an EVCS monopoly can be exploited by attackers. We use New York City's transportation electrification plans as a case study. Our contributions are threefold.

1) We investigate impacts of *MaDEVIoT* attacks on the Manhattan, New York power grid considering the city's transportation electrification policy and the market share of EV charging providers. Given the current EV adoption projections, we find that the EV roll-out can cause blackouts in the Manhattan power grid in 2030.
2) We perform transient-state analysis on frequency and voltage excursions caused by *MaDEVIoT* attacks using industry-standard software, PowerWorld.
3) We identify the vulnerability introduced by an EVCS monopoly and provide insights for the secure development and deployment of the IoT-enabled EV charging (e.g., National EV Infrastructure (NEVI) Program [11]).

II. The Growth of EV Charging

The global EV industry has grown rapidly, with an average annual increase of 60% between 2014 and 2019, led by China and the U.S. [12]. Despite the COVID-19 pandemic, EV sales rose by 43% from 2019 to 2020, reaching 16.5 million EVs in 2021. This growth will continue due to the following factors:

1) **Incentivizing clean fuel vehicles and decarbonization efforts:** Numerous countries, cities, and manufacturers, including Ford, Mercedes, Tesla, Volvo, and Mercedes-Benz, have committed to zero tailpipe emissions in new

cars and vans by 2040, with leading markets targeting 2035 at the 26th United Nation's Climate Change Conference (COP26) [13]. In the U.S., the Bipartisan Infrastructure Law allocates $7.5 billion for a nationwide network of 500,000 high-capacity EVCSs [14].

2) **Overcoming range anxiety for EV drivers:** Advances in battery and charging technologies have addressed range anxiety, and the deployment of publicly accessible EVCss has increased significantly. As of 2020, there were 1.3 million public EVCSs worldwide, including high-wattage stations with charging rates up to 350 kW [12].
3) **Improving EV charging experience:** Smart EVCSs with features like remote control via smartphone applications enhance convenience and accessibility. Smartphone apps provide real-time information on EVCS locations, availability, and pricing [12].

III. Cyber-Physical Outlook of EV Charging

This section summarizes the cyber-physical outlook of EV charging. We refer to [15] for the details.

A. Physical Layer

At the physical layer, in the context of power transfer, EVs consist of battery energy storage, power conditioning units, motor loads, and auxiliary loads. EVs can interact with power grids through Grid-to-Vehicle (G2V) and Vehicle-to-Grid (V2G) technologies, enabling bi-directional flow of electrical energy. EVs connect to power grids through EVCSs, which include power conditioning units that transform grid voltage to the voltage required for charging EV batteries. EVCSs can provide both AC charging, where AC grid voltage is converted to DC voltage by an on-board charger, and DC charging, which directly converts AC voltage to DC to charge the vehicle battery. EVCSs are classified into different charging levels based on their power capacity, such as Level 1 (L1), Level 2 (L2), and Level 3 (L3) chargers, with L3 chargers offering the highest charging power [15].

The power grid, in the context of EV charging, refers to the system that transports electrical energy from generators to consumers. It involves medium-voltage transmission lines, distribution substations, and low-voltage distribution lines to deliver electricity to industrial, commercial, and residential customers. The integration of distributed renewable energy resources and grid interactive programs like demand-response (DR) adds complexity to power system operations [15].

B. Cyber Layer

The cyber layer for EV charging includes the internal and external cyber layers.

Internally, EVs are equipped with Electronic Control Units (ECUs), which are connected to a central gateway through communication channels such as Controller Area Network (CAN) buses, Local Interconnect Networks, Media Oriented Systems Transport, and FlexRay. ECUs perform various control tasks and communicate with different components of the vehicle. Externally, EVs are connected to Original Equipment Manufacturers (OEMs), road-side infrastructures, internet service portals, and other vehicles through cellular networks, WiFi, and near-field communication.

In EVCSs, the internal cyber layer depends on the charging levels. L2 and L3 chargers have more complex internal cyber layers compared to L1 chargers. EVCSs are connected to various entities, including EVs, EVCS servers, EV fleet servers, smartphones, OEMs, Building Energy Management Systems, power utilities, and third-party DR aggregators, through cellular networks, WiFi, and LANs. Communication protocols such as ISO 15118, OCPP, and OpenADR are used for communication between different entities in the EV charging ecosystem [15]–[18].

The cyber layer of the power grid involves Transmission System Operators (TSOs) or Independent System Operators (ISOs), Distribution System Operators (DSOs) or utilities, SCADA systems, Phasor Measurement Units (PMUs), and Remote Terminal Units (RTUs). TSOs and ISOs operate power grids using centralized SCADA systems, while DSOs/utilities generate and supply electricity to customers, engage in grid-interactive programs, and report their operations to ISOs [15].

IV. Security Issues in EV Charging

This section discusses the fundamental causes of cyber attacks in EV charging.

A. Lack of EV Charging Standards/Protocols

The absence of uniform communication standards and protocols for EV charging and grid interactive programs like DR and V2G programs introduces vulnerabilities in EVs and EVCSs [19]. Non-standard cyber-physical interfaces make EVs and EVCSs susceptible to attacks, potentially enabling large-scale, demand-side cyberattacks on power grids. Attackers can leverage non-standardized charging to inject malware and intercept charging data to form a EV botnet. Recently, North American Charging Standard (NACS) is being developed and adopted in EV charging in North America [20].

B. Public Data-Enabled Business Model

EVCS operators and urban power grids release public data, including EV charging location, availability, prices, and grid planning and operational data, as part of their business models. While power grid data is fragmented, EVCS data is widely accessible. This public data facilitates remote attackers in planning (e.g., EV charging botnet topology identification) and executing cyberattacks on EV charging infrastructure and grid.

C. Data-Enabled Operation

Power grid, EVCS, and EV fleet operators rely on data-driven operational decisions, utilizing artificial intelligence and machine learning techniques. The accuracy of these decisions depends on the quality and availability of data. However, the use of private data, collected through IoT devices and public communication channels, poses security and privacy risks, potentially leading to identifying private EV charges. For instance, attackers can exploit EVCS data markets and launch False Data Injection Attacks (FDIA), undermining the accuracy of operational decisions [21].

D. Unobserved Cyber Hygiene of Users

Power grid operators lack direct monitoring of end-use appliances such as EVCSs, EVs, and air-conditioners, which hinders continuous validation of their trustworthiness. EVCS operators also have limited visibility into the operation and cyber hygiene of EV users. Malicious users can exploit poor security practices and complex supply chains to compromise EVCSs (e.g., via common passwords, embedded malware in devices and software) and turn end-user devices into attack vectors targeting the EV charging infrastructure and grid.

V. *MaDEVIoT* Attacks on Power Grids

Attackers can exploit vulnerabilities in EV charging to launch demand-side cyberattacks on power systems, with the goal of distorting the operation of power grids. Such attacks involve forming a botnet of compromised EVCSs or EVCS servers to manipulate the power consumption of EVCSs. Demand-side cyberattacks pose significant threats to power grids compared to utility-side attacks. There are several reasons for this:

1) **Large demand-side attack surfaces:** Demand-side attacks have more access points compared to utility-side attacks due to multiple actors and complex supply chains. Utility-side devices often have strong defense mechanisms, while end-user devices, such as EVCSs, may lack robust security measures.
2) **Unobserved demand-side devices:** Power grid operators do not continuously monitor high-wattage demand-side appliances like EVs and EVCSs, making it difficult to detect and respond to attacks in a timely manner.
3) **Stealthiness of demand-side attacks:** Demand-side attacks can remain stealthy because malicious power alterations, such as changes in EV charging demand, can be difficult to distinguish from regular demand fluctuations.
4) **Demand-side attacks are inexpensive:** Attackers require a large number of compromised EVCSs or EVCS servers to impact the power grid significantly. The cost of compromising EVCSs and their servers is relatively low, with phishing campaigns, espionage, keylogging, and remote access trojans being affordable attack resources. Attackers may also sell ready-made botnets formed by compromised EVCSs, further lowering the cost of launching demand-side attacks on grids [22], [23].

VI. Data

This section provides an overview of the data sets used in this study, which include EV charging data and power grid data for Manhattan, New York.

A. Power Grid Data

The power grid data used in this study is based on the publicly available 7-bus Manhattan power grid [6]. This islanded transmission-level network represents a portion of the power network controlled by the New York Independent System Operator (NYISO). The power grid model, load data, and other parameters are obtained from various public resources, including the U.S. Energy Information Administration, NYISO

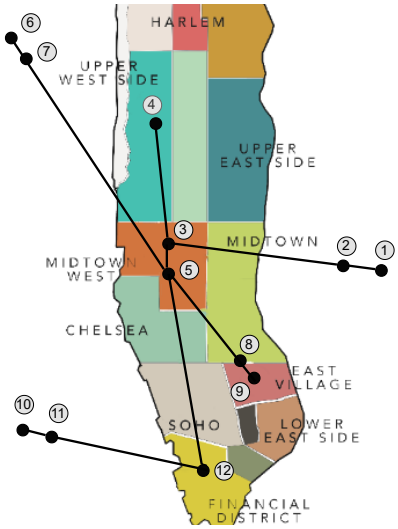

Fig. 1. Topology of transmission-level 12-bus power grid in Manhattan, NY.

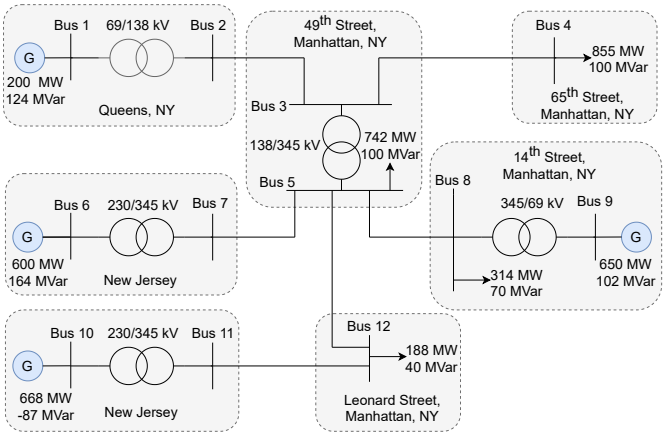

Fig. 2. 12-bus power grid in Manhattan, NY, as simulated in PowerWorld.

real-time dashboard, Con Edison (the local utility in NYC), power system component manufacturer catalogues, and IEEE standards. The transmission line topology, generator locations and capacities, and substation locations are determined using Geographical Information System (GIS) tools such as Google Maps. Load and generation data are derived from NYISO real-time dashboard and load distribution surveys in New York City. The model parameters of generators are obtained from IEEE standards and manufacturer catalogues. The 7-bus power grid model is expanded to a 12-bus power grid to improve its accuracy and incorporate additional features necessary for transient analysis. The 12-bus power grid topology and key parameters are shown in Figures 1 and 2. The line and transformer impedances of the power grid in Figs. 1 and 2 are in Appendix A.

B. EV Charging Data

The EV charging data used in this study is obtained from the Alternative Fuels Data Center website for 2022 [24]. To analyze the commercial landscape of EV charging in Manhattan, the distribution of EVCSs across load buses in

TABLE I
EV CHARGERS POWER (MW) IN MANHATTAN, NY, BASED ON THE NYC DEPARTMENT OF TRANSPORTATION ELECTRIFICATION GOAL [27].

Year	Bus#4		Bus#5		Bus#8		Bus#12	
	All	Tesla	All	Tesla	All	Tesla	All	Tesla
2022	1.94	1.85	1.52	1.40	0.85	0.79	0.46	0.46
2030	101.6	96.8	79.6	73.1	44.7	41.4	24.01	24.01
2050	617.1	588.2	483.8	444.1	271.9	251.9	145.8	145.8

TABLE II
LINE LOADINGS (IN % LINE CAPACITY) ACROSS BUSES IN MANHATTAN POWER GRID DUE TO THE INCREASE IN EV CHARGING LOAD IN TABLE I.

Year	Bus 2-3	Bus 3-4	Bus 5-7	Bus 5-8	Bus 5-12	Bus 11-12
2022*	52	79	62	34	62	67
2022	52	79	62	34	62	68
2030	55	88	64	30	92	94
2050	82	136	79	21	249	232

* Without EV charging load.

Manhattan is mapped using zip codes served by the load buses. The data reveals that Tesla dominates the EV charging market in Manhattan, NY. Furthermore, future projections for EV charging in Manhattan indicate a significant increase in penetration. The New York City Department of Transportation and the Mayor's Office of Climate and Sustainability have set ambitious electrification goals, aiming for 40,000 Level 2 (L2) chargers and 6,000 DC fast chargers in NYC by 2030, with further expansions by 2050. Based on these goals, the estimated peak charging power demand for EVs in Manhattan ranges from 400 MW to 900 MW [25]. Table I shows the current (2022) and projected (2030 and 2050) EV charging loads across load buses in the Manhattan power grid, considering both total EV charging loads and Tesla charger-specific loads.

VII. CASE STUDY AND RESULTS

This section presents the impact of the *MaDEVIoT* attack on the power grid in Manhattan, New York. The analysis considers a scenario where the attack leads to sudden and simultaneous shutdowns of active charging at EVCSs. The results demonstrate the deviations in line load, bus frequencies, and bus voltages as the total EV load increases in 2030 and 2050, as outlined in Table I. The numerical simulations are performed using PowerWorld simulator [26], a widely used power system simulation software in academia and industry.

A. EV Growth Overloads and Trips Lines

Table II presents the line loadings relative to the capacity of each line in the Manhattan power grid. Currently, the EV charging load has an insignificant effect on line loading levels. However, by 2030, the line loading levels significantly increase, particularly for the lines connecting buses #5 and 12, as well as buses #11 and 12, where the line loadings approach the line capacity. By 2050, three of the six transmission lines exceed their capacity, which can trip line overload protection relays and potentially result in system-wide blackouts, highlighting the need for transmission capacity expansion. Notably, the loading on the line connecting buses #5 and 8 decreases in 2050 compared to 2022, as the increased EV charging load

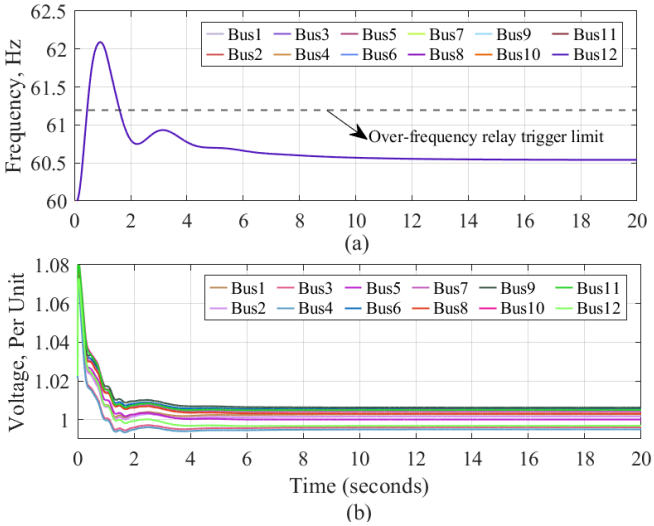

Fig. 3. Bus frequency (a) voltages (b) in the Manhattan power grid when all EVCSs in Manhattan, New York are manipulated in 2030.

at bus #8 consumes more power generated at bus #9, leaving less power to transmit via the line connecting buses #8 and 5.

B. EV Growth Can Suddenly Trip Generator

This section illustrates the evolution of frequency and voltage profiles in the Manhattan power grid under the *MaDEVIoT* attacks on all the EVCSs in Manhattan, New York. The *MaDEVIoT* attack is launched suddenly and simultaneously while the EVCSs are charging EVs. As of September 2022, the maximum frequency deviation caused by the *MaDEVIoT* attack is 60.04 Hz, and the power grid restores the frequency to 60.01 Hz within 15 seconds. Similarly, the peak bus voltage due to the *MaDEVIoT* attack is 1.0018 per unit (p.u.). These voltage and frequency excursions are not enough to trigger generator over-frequency (OF) and over-voltage (OV) protection relays.

However, considering the EVCS usage projection in 2030, the feasibility of the *MaDEVIoT* attack dramatically changes. As shown in Fig. 3(a), the *MaDEVIoT* attack launched in 2030 causes a frequency excursion to 62.095 Hz, and the power grid restores the frequency to 60.54 Hz within 20 seconds. This frequency excursion exceeds the relay trigger limits under both the North American power system practice ($\geq$ 61.2 Hz) [4] and the IEEE 1547 Standard ($\geq$ 62 Hz) [28]. Consequently, the generator OF relays are triggered, causing all generators to disconnect and leading to a system-wide blackout. Additionally, the *MaDEVIoT* attack distorts bus voltages up to 1.082 p.u., as depicted in Fig. 3(b), which is close to the maximum allowable deviation of 1.1 p.u. [29].

The EV growth in 2050 overloads the Manhattan power grid, leading to automatic system-wide blackouts, as indicated in Table II. Therefore, frequency and voltage excursions for the *MaDEVIoT* attack in 2050 are not simulated.

C. Attack on EVCS Network Trips Generator

This section analyzes the feasibility of *MaDEVIoT* attacks on limited EVCS networks with the growth in EV adoption.

TABLE III
MANHATTAN POWER GRID FREQUENCY (IN HZ) DUE TO THE *MaDEVIoT* ATTACK IN INDIVIDUAL EVCS NETWORK IN 2030.

Freq	Tesla	EV Connect	Greenlots	Blink	ChargePoint
Peak	61.952	60.041	60.028	60.027	60.012
Steady	60.5	60.012	60.006	60.008	60.004

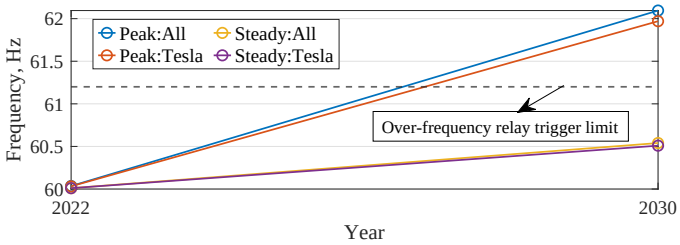

Fig. 4. Evolution of peak and steady-state frequency in the Manhattan power grid when all EVCS and Tesla EVCSs in Manhattan, New York are manipulated across 2022-2030. Peak-All and Peak-Tesla are peak frequencies when all and Tesla EVCS are manipulated. Steady-All and Steady:Tesla are steady-state frequencies when all and Tesla EVCS are manipulated.

In 2022, launching a *MaDEVIoT* attack only on the Tesla EVCS network in Manhattan, New York, achieves a frequency excursion to 60.036 Hz, insufficient to trigger the OF relays. However, the attack feasibility changes in 2030.

The *MaDEVIoT* attack launched by manipulating Tesla EVCSs in 2030 disturbs the power grid frequency to 61.952 Hz, and it restores the frequency to 60.5 Hz in 20 seconds. This frequency excursion triggers the OF protection relays of all generators in the Manhattan power grid, potentially leading to a system-wide blackout. The attack also disturbs bus voltages up to 1.077 per unit, making the power grid vulnerable but not tripping the over-voltage protection relays.

As Table III shows, unlike attacks on Tesla's network, attacks launched by manipulating other EVCSs do not trigger OF protection relays. Launching *MaDEVIoT* attacks on all EVCSs except Tesla EVCSs causes a frequency excursion to 60.115 Hz, and the grid restores the frequency to 60.032 Hz. This excursion is not enough to trigger OF relays.

Fig. 4 shows the evolution of peak and steady-state frequencies when all EVCSs and Tesla EVCSs are compromised. The *MaDEVIoT* attacks launched via manipulating only Tesla chargers are feasible before 2030. To disturb the power grid frequency to 61.2 Hz, attackers require access to 148.3770 MW of active charging, which refers to only compromising 63% of Tesla chargers in 2030. This attack is feasible by compromising a centralized server of Tesla charging network. However, attackers would need to compromise servers for multiple charging networks to launch the same attack if the penetration of a single charger business was less. Thus, EV infrastructure plans, such as NEVI Formula Program [11], should consider the relationship between monopoly in high-power chargers and risk of *MaDEVIoT* attacks.

VIII. DEFENSE MECHANISMS

Defense mechanisms against attacks on EV charging can be classified into preventive and corrective means. Preventive measures include standardization of communication (e.g., ISO 15118 and OCPP updates [16], [17]), intrusion detection systems, and machine learning-based charging operations (e.g., EVCS data markets that increases the difficulty of FDIA [21]). Charging standards across EV ecosystem reduces the risk of attacks steaming from vulnerable proprietary EV charging. Also, effective intrusion detection systems keep the attack from spreading across the EV ecosystem. Although these measures decrease attack feasibility, they are not foolproof. Thus, corrective means like cyber insurance [30] are necessary to mitigate financial losses and incentivize preventive investments. Combining both preventive and corrective means is essential for the security of the EV charging ecosystem.

TABLE IV
LINE AND TRANSFORMER IMPEDANCES IN PER UNIT OF THE POWER GRID IN MANHATTAN, NEW YORK, IN FIGS. 1 AND 2.

Line	Resistance (pu)	Reactance (pu)	Voltage (kV)
Bus 1-2	0.000047	0.000473	69/138
Bus 2-3	0.003490	0.000433	138/138
Bus 3-4	0.000078	0.000220	138/138
Bus 3-5	0.001400	0.01400	138/345
Bus 5-7	0.000150	0.001490	345/345
Bus 5-8	0.000140	0.001390	345/69
Bus 5-12	0.000295	0.003650	345/345
Bus 6-7	0.000160	0.0000154	230/345
Bus 8-9	0.000140	0.001390	345/69
Bus 10-11	0.000160	0.001540	230/345
Bus 11-12	0.001500	0.001490	345/345

* Base MVA = 100.

IX. CONCLUSION

This paper assesses the feasibility of demand-side cyber-attacks launched through internet-connected EVCSs in Manhattan, New York, for 2030 and 2050. Data on EV charging comes from plans by the New York City Department of Transportation and the Mayor's Office of Climate and Sustainability, while power grid data is obtained from public sources. Results indicate that such demand-side cyberattacks can disrupt the power grid's frequency beyond IEEE and North American operational limits. Additionally, the monopoly in EVCS businesses can exacerbate the attacks. Note that the analysis does not consider potential future power grid upgrades, which may impact the feasibility of *MaDEVIoT* attacks in 2030 and 2050.

APPENDIX A
DATA ON THE MANHATTAN GRID

Table IV shows the resistances and reactances of the lines and transformers in the Manhattan power grid in Figs. 1 and 2. The per unit values are calculated using 100 MVA base.

ACKNOWLEDGMENT

We would like to express our gratitude to Dr. Robert Mieth at Rutgers University for discussions related to this study and especially for assisting in setting up Powerworld simulations and for advance access to the data in [25]. We also thank Abdullahi Bamigbade at New York University for his input on dynamic grid modelling and Dr. Malini Ghosal at Pacific Northwest National Laboratory for proofreading the paper.

REFERENCES

[1] Energy Security Sentinel: Cyberattacks surge in 2022 as hackers target commodities. https://tinyurl.com/yw3htdnw. Accessed on 2022-11-3.

[2] K. Harnett *et al.*, "DoE/DHS/DoT volpe technical meeting on electric vehicle and charging station cybersecurity report," Tech. Rep., 2018.

[3] R. Metere *et al.*, "Securing the electric vehicle charging infrastructure," *arXiv preprint arXiv:2105.02905*, 2021.

[4] S. Soltan *et al.*, "Blackiot: IoT botnet of high wattage devices can disrupt the power grid," in *USENIX Security*, 2018, pp. 15–32.

[5] B. Huang *et al.*, "Not everything is dark and gloomy:power grid protections against IoT demand attacks," in *USENIX Security*, 2019.

[6] S. Acharya *et al.*, "Public plug-in electric vehicles+ grid data: Is a new cyberattack vector viable?" *IEEE Trans. on Smart Grid*, 2020.

[7] M. A. Sayed *et al.*, "Electric vehicle attack impact on power grid operation," *Intl. J. of Electrical Power & Energy Sys.*, vol. 137, 2022.

[8] D. Kern *et al.*, "Analysis of e-mobility-based threats to power grid resilience," in *Computer Science in Cars Symposium*, 2021, pp. 1–12.

[9] M. Ghafouri *et al.*, "Coordinated charging and discharging of EVs: A new class of switching attacks," *ACM Trans. on Cyber-Phy. Sys.*, 2022.

[10] T. Nasr *et al.*, "Power jacking your station: In-depth security analysis of ev charging station management systems," *Comp. & Sec.*, 2022.

[11] State plans for electric vehicle charging. https://tinyurl.com/4n2hwcu6.

[12] (2022) Global EV outlook 2022. https://tinyurl.com/4syvj5uc.

[13] Cop26: Together for our planet. https://tinyurl.com/2p93m87j.

[14] (2022) President biden's bipartisan infrastructure law. https://www.whitehouse.gov/bipartisan-infrastructure-law/. Accessed on 2022-8-9.

[15] S. Acharya *et al.*, "Cybersecurity of smart electric vehicle charging: A power grid perspective," *IEEE Access*, vol. 8, 2020.

[16] ISO 15118-20:2022 Road vehicles — Vehicle to grid communication interface — Part 20: 2nd generation network layer and application layer requirements. https://www.iso.org/standard/77845.html.

[17] Open charge alliance global platform for open protocols. https://www.openchargealliance.org. Accessed on 2022-8-10.

[18] OpenADR. https://www.openadr.org. Accessed on 2022-8-10.

[19] D. M. Steward, "Critical elements of vehicle-to-grid (v2g) economics," NREL, Golden, CO (United States), Tech. Rep., 2017.

[20] Opening the north american charging standard. https://tinyurl.com/38t5p6xa. Accessed on 2023-07-11.

[21] S. Acharya *et al.*, "False data injection attacks on data markets for electric vehicle charging stations," *Advances in Applied Energy*, 2022.

[22] (2018) Black-market ecosystem. https://tinyurl.com/34eyeadk.

[23] N. Yuri, "The economics of botnets," Kaspersky, Massachusetts, USA, https://tinyurl.com/2zpktabm.

[24] Alternative fueling station locator. https://tinyurl.com/3hnm3xby.

[25] J. Zhang *et al.*, "Quantifying electricity demand for 100% electrified transportation in new york city," *arXiv preprint arXiv:2211.11581*, 2022.

[26] Powerworld simulator. https://www.powerworld.com/.

[27] (September, 2021) An electric vehicle vision plan for new york city. https://tinyurl.com/mswbj99p. Accessed on 2022-12-1.

[28] "IEEE standard for interconnecting distributed resources with electric power systems - amendment 1," *IEEE Std 1547a-2014*, pp. 1–16, 2014.

[29] Voltage disturbance. https://voltage-disturbance.com/voltage-quality/voltage-tolerance-standard-ansi-c84-1/. Accessed on 2022-12-18.

[30] S. Acharya *et al.*, "Cyber insurance against cyberattacks on electric vehicle charging stations," *IEEE Trans. on Smart Grid*, 2021.