Mehmet Sefa İMAMOĞLU — 230541038

Anomali: Hayalet Filo (Phantom Fleet) V2G Piyasa Manipülasyonu – Koordineli Siber-Finansal Saldırı Anomalisi

1. Anomali Tanımı

"Hayalet Filo" V2G Manipülasyonu, V2G (Araçtan Şebekeye) teknolojisinin getirdiği çift yönlü enerji akışını ve entegre enerji piyasalarını hedef alan, gelişmiş bir siber-finansal saldırı anomalisidir. Bu saldırı, basit enerji hırsızlığından farklı olarak, doğrudan enerji piyasasını ve şebeke operatörlerini (DSO/TSO) dolandırmayı amaçlar.

Nasıl Çalışıyor ? Saldırgan, bir Şarj İstasyonu Yönetim Sistemi (CSMS) veya V2G Toplayıcı (Aggregator) platformuna sızar. Ardından, iki hileyi birden yapar:

1. **Varlık Sahteciliği (Spoofing):** Fiziksel olarak şebekeye bağlı olmayan, batarya kapasitesi yetersiz olan veya *hiç var olmayan* binlerce elektrikli aracı (Hayalet Filo), sisteme "V2G deşarjına hazır" olarak tanıtır.
2. **Sahte Veri Enjeksiyonu (FDIA):** Enerji fiyatlarının en yüksek olduğu (pik talep anları) zamanlarda, şebeke operatöründen veya toplayıcıdan "enerji bas" (deşarj) sinyali aldığında, bu hayali filonun *sanki şebekeye milyonlarca watt enerji basıyormuş gibi* sahte metervalue (sayaç) ve durum verilerini sisteme enjekte eder.

Bu hile, enerji piyasası operatörünün , *fiziksel olarak asla sağlanmamış* bir şebeke hizmeti (örn. frekans düzenleme) için saldırgana (veya onun paravan şirketine) ödeme yapmasına neden olur. Sonuç, şebeke istikrarını riske atan sistemik bir finansal dolandırıcılıktır.

2. Olası Nedenler

Kategori	Olası Sebep	Açıklama (Basitçe)
Protokol Güvenliği	Eski veya Güvensiz OCPP Sürümleri	OCPP 1.6 gibi şifrelenmemiş veya zayıf kimlik doğrulamalı protokollerin kullanılması, saldırganın araya girerek (MitM) sahte V2G mesajları göndermesini sağlar.
Merkezi Sistem Zafiyeti	CSMS Tedarik Zinciri "Gölge Kanalları"	Şarj istasyonu yönetim yazılımını (CSMS) üreten ana firmanın, operatörlerin bilmediği "gölge" yönetim kanalları bırakması. Saldırgan bu arka kapıyı keşfederse, binlerce istasyonu tek noktadan kontrol edebilir.

Doğrulama Zafiyeti	Siber-Fiziksel Doğrulama Eksikliği	Sistemin (Toplayıcı/CSMS), bir istasyondan gelen dijital veriye (örn. "Şebekeye 5MW basıyorum"), fiziksel dünyadaki (örn. Trafo Merkezi sensörleri) bir karşılığı olup olmadığını kontrol etmeden *güvenmesi*.
Piyasa Mekanizması	AI Tabanlı Piyasa Modellerinin İstismarı	V2G hizmetlerini yöneten toplayıcıların AI (Yapay Zeka) platformlarının, sahte verilerle (Data Poisoning) "zehirlenmesi". AI, hayali filoyu gerçek bir varlık sanarak ona ödeme yapılmasını tetikler.

3. Olası Riskler ve Etkiler

- **Yüksek Gizlilik ve Düşük Sinyal:** Bu saldırı, protokol kurallarına uygun (sözdizimsel olarak geçerli) ancak anlamsal olarak yalan mesajlar gönderir. Geleneksel siber saldırı tespit sistemleri (IDS) için bu trafik normal görünür , bu da tespiti zorlaştırır.
- **Sistemik Finansal Kayıp:** Saldırı, bireysel faturaları değil, enerji toptan satış pazarını hedefler. Başarılı bir saldırı, tekil istasyonlar yerine tüm bir "filo" üzerinden haksız kazanç (arbitraj) sağlayarak muazzam finansal kayba yol açar.
- **Kritik Altyapı Tehdidi (Fiziksel Etki):** En tehlikeli risktir. Bir şebeke operatörü (DSO), pik talep anında Hayalet Filo dan geleceğine güvendiği (örneğin) 50MW'lık sanal desteği hesaba katarsa ve bu enerji fiziksel olarak *gelmezse*, bu durum bölgesel şebeke istikrarsızlığına, voltaj çöküşlerine ve hatta fiziksel kesintilere (brownout) yol açabilir.
- **Piyasa Güvenilirliğinin Çökmesi:** V2G teknolojisine ve tekerlekli pil konseptine olan güveni temelden sarsar. Bu durum, düzenleyicilerin teknolojiyi yavaşlatmasına ve yenilenebilir enerji entegrasyonunun sekteye uğramasına neden olabilir.

4. İlgili Standartlar ve Kurallar

- **OCPP (Open Charge Point Protocol):** Özellikle OCPP 2.1 sürümü , Çift Yönlü Şarj(Bidirectional Charging) ve DER Kontrolü (Dağıtık Enerji Kaynağı) için yeni fonksiyonel bloklar tanımlar. Saldırı, bu V2G'ye özgü protokol mesajlarının içeriğini (örn. deşarj edilen enerji miktarı) manipüle eder.
- **ISO 15118 (-20):** Aracın (EV) şarj istasyonuyla (EVSE) V2G dahil olmak üzere gelişmiş iletişim kurmasını sağlayan "Plug & Charge" standardıdır. Saldırganın, EV'nin batarya durumunu (SoC) ve deşarj kapasitesini sahte olarak bildirmesi için bu iletişimi taklit etmesi veya ele geçirmesi gerekir.
- **Enerji Piyasası Kuralları (DSO/TSO):** Saldırı, V2G varlıklarının frekans düzenleme, talep yanıtı gibi "Yan Hizmetler Piyasalarına" katılım kurallarındaki boşlukları istismar eder.
- **Siber-Fiziksel Sistem (CPS) Güvenliği:** Bu saldırı, siber (OCPP/CSMS) ve fiziksel (trafo/şebeke) alanlar arasındaki boşluğu hedefler. Tespit için bu iki dünyanın verilerinin (Siber-Fiziksel Korelasyon) birlikte analiz edilmesi şarttır.

5. Simülasyon Sonuçları

Hayalet Filo saldırısı, sizin örneğinizdeki DLI saldırısı gibi basit zamanlama gecikmelerine dayanmaz bu nedenle geleneksel log analizleri (örn. TDD) bu saldırıyı tespit edemez çünkü mesajlar geç değil doğrudan yalan dır.

Bu saldırıyı tespit etmek için bir Hardware-in-the-Loop (HIL) veya tam simülasyon test ortamı gereklidir. Bu ortamda iki temel metrik karşılaştırılmalıdır:

1. Log Analizi Metriği (Siber-Fiziksel Enerji Uyumsuzluğu - CPEU):

Bu, "Hayalet Filo" anomalisinin temel tespit metriğidir. "Siber" dünyada (CSMS/Toplayıcı logları) 5 raporlanan enerji ile "Fiziksel" dünyada (DSO/SCADA trafo sensörleri) ölçülen gerçek enerji arasındaki farkı (Delta) analiz eder.

Anomali Log Kayıtları (Kavramsal Simülasyon Tablosu):

Tabloda, "Bölge A"daki "Hayalet Filo"nun (saldırgan kontrolünde) ve "Bölge B"deki meşru filonun verileri karşılaştırılmaktadır. Saldırı 18:01'de başlamıştır.

Zaman Damgası	**Raporlanan Varlık**	**Siber Veri (CSMS/OCPP)**	**Fiziksel Veri (DSO/SCADA)**	**Uyumsuzluk (Delta)**	**Durum**
18:00:00	Bölge A (Filo 1)	- 0.2 MW (Şarj Raporlandı)	- 0.2 MW (Gerçek Şarj)	0.0 MW	Normal
18:00:00	Bölge B (Filo 2)	- 0.3 MW (Şarj Raporlandı)	- 0.3 MW (Gerçek Şarj)	0.0 MW	Normal
18:01:00	Bölge A (Filo 1)	**+ 5.0 MW (Deşarj Raporlandı)** [7]	- 0.1 MW (Normal Yük)	**5.1 MW**	**ANOMALİ**
18:01:00	Bölge B (Filo 2)	+ 2.0 MW (Deşarj Raporlandı)	+ 1.9 MW (Gerçek Deşarj)	0.1 MW	Normal

18:02:00	Bölge A (Filo 1)	**+ 5.0 MW (Deşarj Raporlandı)**	- 0.1 MW (Normal Yük)	**5.1 MW**	**ANOMALİ**
18:02:00	Bölge B (Filo 2)	+ 2.0 MW (Deşarj Raporlandı)	+ 1.9 MW (Gerçek Deşarj)	0.1 MW	Normal

2. Log Analizi Metriği (Protokol Durum İhlali - FSM):

Saldırganın yüzlerce sahte aracı yönetirken yapacağı mantıksal protokol hatalarının (Finite-State Machine - FSM) 12 tespiti.

- **Fiziksel Olarak İmkansız Durum Geçişleri:** Bir aracın bataryasının 2 dakika içinde %20'den %90'a (şarj), sonraki 1 dakika içinde %70'e (deşarj) düşmesi gibi fiziksel olarak imkansız MeterValue raporlamaları.
- **Veri Zehirleme (Data Poisoning) Tespiti:** Toplayıcının AI modeline gelen verilerin (örn. Bölge A'daki tüm EV'ler %100 deşarja hazır) istatistiksel olarak normalin dışında (outlier) olması.

Sistem Geliştirme Odaklı Öneriler:

1. **Siber-Fiziksel Korelasyon Zorunluluğu:** DSO'lar (şebeke) ve CPO'lar (istasyonlar) arasında "Siber Veri" (OCPP) ve "Fiziksel Veri" (SCADA) akışını gerçek zamanlı doğrulayan merkezi bir denetim sistemi (ideal olarak Federe Öğrenme tabanlı) kurulmalıdır.
2. **Kriptografik Varlık Doğrulama:** V2G hizmeti sunan her EVSE/EV'nin, şebekeye bağlı olduğunu ve raporladığı kapasiteye sahip olduğunu PKI (Açık Anahtar Altyapısı) tabanlı sertifikalarla (örn. ISO 15118-20) kriptografik olarak kanıtlaması zorunlu hale getirilmelidir.

6. Sonuç ve Değerlendirme

"Hayalet Filo" V2G Manipülasyonu, mevcut anomali matrislerinin (örn. enerji hırsızlığı, QR kod dolandırıcılığı, operasyonel arızalar) tamamen ötesinde, yeni nesil bir siber-finansal tehdittir. Bu saldırı, tekil şarj istasyonlarını veya son kullanıcıları değil, doğrudan **enerji piyasasını bütünlüğünü** ve **şebeke altyapısının fiziksel güvenliğini** hedef alır. Bu analiz, V2G ekosistemine geçiş yapılırken, siber güvenlik paradigmalarının bireysel fatura güvenliğinden sistemik piyasa ve şebeke güvenliğine doğru evrilmesi gerektiğini göstermektedir.Geleneksel log takibi ve zamanlama analizi (DLI örneğinde olduğu gibi) yetersizdir artık siber ve fiziksel verilerin gerçek zamanlı korelasyonu bir zorunluluktur

Alıntılanan çalışmalar

1. Critical Elements of Vehicle-to-Grid (V2G) Economics - NREL, erişim tarihi Kasım 10, 2025, https://www.nrel.gov/docs/fy17osti/69017.pdf
2. Open charge point protocol - Open Charge Alliance, erişim tarihi Kasım 10, 2025, https://openchargealliance.org/protocols/open-charge-point-protocol/
3. Anomaly Detection in Electric Vehicle Charging Stations Using Federated Learning - arXiv, erişim tarihi Kasım 10, 2025, https://arxiv.org/html/2509.18126v1
4. Anomaly detection with grid sentinel framework for electric vehicle charging stations in a smart grid environment - PMC - PubMed Central, erişim tarihi Kasım 10, 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC12056157/
5. The state of EV charging in America: Harvard research shows chargers 78% reliable and pricing like the 'Wild West' | Institute for Business in Global Society, erişim tarihi Kasım 10, 2025, https://www.hbs.edu/bigs/the-state-of-ev-charging-in-america
6. Common EV Charging Problems and Issues - Sino Energy, erişim tarihi Kasım 10, 2025, https://sinoevse.com/common-ev-charging-problems-and-issues/
7. Massive analysis of EV charging stations finds reliability issues galore - A new report by ChargerHelp calls lack of interoperability “the overarching threat to system reliability and broader EV adoption” in the US : r/electriccars - Reddit, erişim tarihi Kasım 10, 2025, https://www.reddit.com/r/electriccars/comments/1euqvba/massive_analysis_of_ev_charging_stations_finds/
8. (PDF) OCPP Protocol: Security Threats and Challenges - ResearchGate, erişim tarihi Kasım 10, 2025, https://www.researchgate.net/publication/313781416_OCPP_Protocol_Security_Threats_and_Challenges
9. Elektrikli Araç Şarj İstasyonlarında Yeni Tehdit: Quishing Dolandırıcılığına Dikkat!, erişim tarihi Kasım 10, 2025, https://www.lojistikdefteri.com/elektrikli-arac-sarj-istasyonlarinda-yeni-tehdit-quishing-dolandiriciligina-dikkat
10. Elektrikli Araç Şarj Kutusuna Dikkat! #araba #elektrik #şarj #ödeme - YouTube, erişim tarihi Kasım 10, 2025, https://www.youtube.com/watch?v=1ERZ1kdBtY0
11. Intentional and unintentional fraud in EV charging - Deftpower, erişim tarihi Kasım 10, 2025, https://www.deftpower.com/resources/white-papers/intentional-and-unintentional-fraud-in-ev-charging
12. What is an RFID card for EV charging? - Chargemap Blog: news and tips on electric cars, erişim tarihi Kasım 10, 2025, https://blog.chargemap.com/how-does-an-ev-charging-card-work/
13. Vehicles-to-Grid Integration Assessment Report - Department of ..., erişim tarihi Kasım 10, 2025, https://www.energy.gov/sites/default/files/2025-01/Vehicle_Grid_Integration_A

sseessment_Report_01162025.pdf
14. Regression Based Anomaly Detection in Electric Vehicle State of Charge Fluctuations Through Analysis of EVCI Data - arXiv, erişim tarihi Kasım 10, 2025, https://arxiv.org/html/2401.01580v1
15. Cybersecurity and V2G: Consumers need a secure connection for their batteries on wheels, erişim tarihi Kasım 10, 2025, https://thedriven.io/2025/10/14/cybersecurity-and-v2g-consumers-need-a-secure-connection-for-their-batteries-on-wheels/
16. Optimization Challenges in Vehicle-to-Grid (V2G) Systems and Artificial Intelligence Solving Methods - MDPI, erişim tarihi Kasım 10, 2025, https://www.mdpi.com/2076-3417/14/12/5211
17. Vehicle-to-grid (V2G) Reactive Power Operation Analysis of the EV/PHEV Bidirectional Battery Charger, erişim tarihi Kasım 10, 2025, https://trace.tennessee.edu/utk_graddiss/1749/
18. Case study (UK): Electric vehicle-to-grid (V2G) charging - Ofgem, erişim tarihi Kasım 10, 2025, https://www.ofgem.gov.uk/publications/case-study-uk-electric-vehicle-grid-v2g-charging
19. Cybersecurity in Vehicle-to-Grid (V2G) Systems: A Systematic Review - arXiv, erişim tarihi Kasım 10, 2025, https://arxiv.org/html/2503.15730v1
20. Electric Vehicle Charging: A Survey on the Security Issues and Challenges of the Open Charge Point Protocol (OCPP), erişim tarihi Kasım 10, 2025, https://openresearch.surrey.ac.uk/view/pdfCoverPage?instCode=44SUR_INST&filePid=13169250180002346&download=true
21. Disrupting EV Charging Sessions and Gaining Remote Code Execution with DoS, MITM, and Code Injection Exploits using OCPP 1.6 - - INL Research Library Digital Repository - Idaho National Laboratory, erişim tarihi Kasım 10, 2025, https://inldigitallibrary.inl.gov/sites/sti/sti/Sort_65949.pdf
22. Cyber Attack Detection in Electric Vehicle Charging Stations Using Topological Data Aided Learning - The University of Texas at Dallas, erişim tarihi Kasım 10, 2025, https://personal.utdallas.edu/~jiezhang/Conference/Zhang_2025_IEEE_PESGM_EV_cyberattack.pdf
23. Economic study of the different scenarios - V2Market, erişim tarihi Kasım 10, 2025, https://v2market-project.eu/wp-content/uploads/2023/01/D4.1-Economic-Studies_ESC.pdf
24. How Irdeto is protecting EV charging infrastructure from cyber-attacks, erişim tarihi Kasım 10, 2025, https://chargedevs.com/features/how-irdeto-is-protecting-ev-charging-infrastructure-from-cyber-attacks/
25. OCPPStorm: A Comprehensive Fuzzing Tool for OCPP Implementations - ORCA – Online Research @ Cardiff, erişim tarihi Kasım 10, 2025, https://orca.cardiff.ac.uk/id/eprint/172592/1/vehiclesec2024-69-paper-v2.pdf
26. Exploiting Hidden Supply-Chain Vulnerabilities to Attack EV Chargers and CPOs - SaiFlow, erişim tarihi Kasım 10, 2025,

https://www.saiflow.com/blog/exploiting-hidden-supply-chain-vulnerabilities-to-attack-ev-chargers-and-cpos
27. Addressing Security in OCPP: Protection Against Man-in-the-Middle Attacks - ResearchGate, erişim tarihi Kasım 10, 2025, https://www.researchgate.net/publication/324179098_Addressing_Security_in_OCPP_Protection_Against_Man-in-the-Middle_Attacks
28. (PDF) A Novel OCPP-Centric Hybrid Testbed and Dataset for EV Charging Infrastructure Security Threats Feasibility Testing - ResearchGate, erişim tarihi Kasım 10, 2025, https://www.researchgate.net/publication/396359849_A_Novel_OCPP-Centric_Hybrid_Testbed_and_Dataset_for_EV_Charging_Infrastructure_Security_Threats_Feasibility_Testing
29. Prediction and analysis of relative error in electric vehicle charging stations based on an improved ConvFormer model - PMC - NIH, erişim tarihi Kasım 10, 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC11379984/
30. MitM Cyber Risk Analysis in OCPP enabled EV Charging Stations - NTU > IRep, erişim tarihi Kasım 10, 2025, https://irep.ntu.ac.uk/id/eprint/54419/1/2478037_Brown.pdf
31. Addressing Security in OCPP: Protection Against Man-in-the-Middle Attacks - NICS Lab, erişim tarihi Kasım 10, 2025, https://www.nics.uma.es/pub/papers/1692.pdf
32. CIC EV charger attack dataset 2024 (CICEVSE2024) - University of New Brunswick, erişim tarihi Kasım 10, 2025, https://www.unb.ca/cic/datasets/evse-dataset-2024.html
33. Electric Vehicle Charging Station Reliability - CLEAResult, erişim tarihi Kasım 10, 2025, https://www.clearesult.com/sites/default/files/2024-05/EV-WATTS_White-Paper_Charging-Station-Reliability.pdf
34. Enhancing the Detection of Cyber-Attacks to EV Charging Infrastructures Through AI Technologies - MDPI, erişim tarihi Kasım 10, 2025, https://www.mdpi.com/2079-9292/14/21/4321
35. Federated detection of open charge point protocol 1.6 cyberattacks - OAE Publishing Inc., erişim tarihi Kasım 10, 2025, https://www.oaepublish.com/articles/ces.2025.04
36. EVs are great! But who's keeping tabs on fraud risk at charging stations?, erişim tarihi Kasım 10, 2025, https://www.infosysbpm.com/blogs/bpm-analytics/evs-are-great-but-whos-keeping-tabs-on-fraud-risk-at-charging-stations.html
37. EV CPO Under Siege: A New Attack Exposed the Cybersecurity and Privacy Risks of EV Charging Networks - Upstream Security, erişim tarihi Kasım 10, 2025, https://upstream.auto/blog/cybersecurity-and-privacy-risks-of-ev-charging-networks/
38. EV Charging Station Applications – a Growing Cyber Security Risk | Radware Blog, erişim tarihi Kasım 10, 2025, https://www.radware.com/blog/application-protection/ev_charging_station_cy

ber_threats/
39. Collaborative anomaly detection system for charging stations - NICS Lab, erişim tarihi Kasım 10, 2025, https://www.nics.uma.es/pub/papers/Alcaraz2022c.pdf