Elektrikli Araç Şarj Ekosisteminin Güvenlik Değerlendirmesi: "A Detailed Security Assessment of the EV Charging Ecosystem" (Antoun vd., 2020) Makalesinin Kapsamlı GZFT Analizi ve 2025 Tehdit Manzarası Bağlamında Stratejik İncelemesi

Yönetici Özeti

Küresel ulaşım sektörünün hızla elektrifikasyonu, siber güvenlik araştırmalarında paralel bir evrimi zorunlu kılmıştır. Elektrikli Araçlar (EA), niş bir pazar olmaktan çıkıp kritik altyapı bileşenlerine dönüşürken; Elektrikli Araç Tedarik Ekipmanları (EVSE), Şarj İstasyonu Yönetim Sistemleri (CSMS) ve güç şebekesini kapsayan şarj ekosisteminin güvenliği hayati bir endişe kaynağı haline gelmiştir. 2020 yılında Joseph Antoun ve arkadaşları tarafından *IEEE Network* dergisinde yayımlanan "A Detailed Security Assessment of the EV Charging Ecosystem" (EA Şarj Ekosisteminin Detaylı Güvenlik Değerlendirmesi) başlıklı çalışma, bu alandaki siber tehditleri kategorize eden, zafiyetleri değerlendiren ve gelecekteki araştırmalar için bir boşluk analizi sunan temel bir eser olarak kabul edilmektedir.[1]

Bu rapor, söz konusu makalenin uzman seviyesinde, ayrıntılı bir GZFT (Güçlü Yönler, Zayıf Yönler, Fırsatlar ve Tehditler) analizini sunmaktadır. Ancak, gerçekten nüanslı bir anlayış sağlamak adına, bu analiz yalnızca yayınlandığı yılın bağlamında değil, 2025 yılı tehdit manzarası ve teknolojik gelişmeleri ışığında gerçekleştirilmiştir. Antoun ve arkadaşlarının çalışmasının kalıcı geçerliliği; Açık Şarj Noktası Protokolü (OCPP) 2.0.1 ve 2.1'in benimsenmesi, ISO 15118-20 standardının yükselişi, yapay zeka destekli saldırı ve savunma mekanizmalarının ortaya çıkışı ve ABD'deki Ulusal Elektrikli Araç Altyapısı (NEVI) programı ile AB'nin Alternatif Yakıtlar Altyapı Tüzüğü (AFIR) gibi katı düzenleyici çerçevelerin yürürlüğe girmesiyle şekillenen

bir dönemde değerlendirilmektedir.[4]

Analizimiz, Antoun ve arkadaşlarının (2020), özellikle kullanıcı mahremiyeti ve şebeke kullanılabilirliği konularında tehditlerin temel bir taksonomisini sağladığını ortaya koymaktadır. Ancak, makalenin "Zayıf Yönleri" ve karşılaştığı "Tehditler", büyük ölçüde analiz ettiği protokollerin (OCPP 1.6J ve ISO 15118-2) hızlı eskimesinden ve o dönemde teorik veya bilinmeyen fiziksel katman saldırılarının (örneğin Brokenwire saldırısı) ortaya çıkmasından kaynaklanmaktadır. Buna karşılık, 2020 yılında tanımlanan "Fırsatlar", bugün aktif araştırma alanlarına dönüşmüş durumdadır; özellikle saldırı tespiti için Yapay Zeka (YZ) kullanımı ve merkeziyetsiz güvenlik için blokzincir entegrasyonu bu alanların başında gelmektedir. Bu rapor, belirli bir akademik çalışmanın eleştirisi olmanın ötesinde, 2025 yılı itibarıyla EA şarj güvenliğinin en son durumunu ortaya koyan kapsamlı bir inceleme niteliğindedir.

---

1. Giriş ve Bağlamsal Çerçeve: EA Şarj Tehdit Manzarasının Evrimi (2020–2025)

Antoun ve arkadaşlarının çalışmasıyla ilişkili Güçlü Yönler, Zayıf Yönler, Fırsatlar ve Tehditleri doğru bir şekilde değerlendirmek için, öncelikle 2020 ekosistemi ile 2025 ekosistemi arasındaki teknolojik ve operasyonel farkı (delta) tesis etmek gerekmektedir. Bu evrim, makalenin geçerliliğini ve tarihsel önemini belirleyen temel faktördür.

1.1 2020 Temel Çizgisi: Parçalı ve Savunmasız Bir Ekosistem

Antoun ve ekibi değerlendirmelerini yürüttüğünde, elektrikli araç şarj altyapısı agresif ancak genellikle güvensiz bir genişleme evresindeydi. Şarj cihazı yönetimi için hakim protokol, standart uygulamasında genellikle zorunlu şifrelemeden yoksun olan OCPP 1.6 (özellikle JSON varyantı, OCPP 1.6J) idi. O dönemde güvenlik profilleri isteğe bağlıydı ve birçok Şarj Noktası Operatörü (CPO), güvenli WebSockets (wss://) yerine düz metin WebSockets (ws://) kullanarak istasyonları konuşlandırıyordu.[6]

Ayrıca, araç-şebeke (V2G) iletişim standardı olan ISO 15118-2, çift yönlü enerji akışı güvenliğinden ziyade öncelikle "Tak ve Şarj Et" (Plug & Charge) kolaylık özelliğine odaklanmıştı. Ekosistem, kullanılabilirlik ve kapsama alanının gizlilik ve bütünlükten öncelikli olduğu bir "arazi kapma" zihniyetiyle karakterize ediliyordu. EA'ların şebeke üzerindeki etkisi, somut bir operasyonel gerçeklikten ziyade simülasyonlarda modellenen teorik bir endişeydi. Antoun ve arkadaşları, STRIDE gibi çerçeveleri kullanarak kullanılabilirlik, bütünlük ve gizliliğe yönelik

saldırıları kategorize ederek, bu dağınık riskleri tutarlı bir tehdit modelinde birleştirdikleri için çalışmaları kritik bir öneme sahipti.[1]

1.2 2025 Gerçekliği: Düzenleme, Standardizasyon ve Sofistike Tehditler

2025 yılına gelindiğinde, manzara kökten değişmiştir. Dağıtık ve düzensiz yapı, titiz düzenlemeler ve teknolojik zorunluluklarla disipline edilmiştir.

- **Düzenleyici Sertleşme (Regulatory Hardening):** Amerika Birleşik Devletleri'nde NEVI programı, finanse edilen şarj cihazlarının ISO 15118'e ve belirli siber güvenlik planlarına uymasını zorunlu kılmaktadır. Avrupa'da AFIR, kamu altyapısında "akılsız" şarj cihazlarını etkili bir şekilde yasaklayarak dijital bağlantı ve anlık (ad-hoc) ödeme güvenliği gerektirmektedir.[4]
- **Protokol Olgunlaşması:** OCPP 2.0.1 ve ardından gelen 2.1, yeni kurulumlar için standart haline gelmiş, Taşıma Katmanı Güvenliği'ni (TLS) zorunlu kılmış ve uyumlu ağlarda şifresiz iletişim seçeneğini ortadan kaldıran farklı güvenlik profilleri sunmuştur.[7]
- **Fiziksel ve RF Tehditleri:** Yazılım yığınları sertleştikçe, saldırganlar katmanlarda aşağıya doğru hareket etmiştir. HomePlug Green PHY kontrol pilot sinyalini hedef alan "Brokenwire" ve güç tarafı kanal saldırıları (McHammer) gibi saldırılar, fiziksel katmanın önemli bir güvenlik açığı olmaya devam ettiğini göstermektedir.[8]
- **Yapay Zeka ve Otomasyon:** Hem savunma hem de saldırı otomatikleşmiştir. YZ tabanlı saldırı tespit sistemleri (IDS) artık uçta (şarj cihazında) ve bulutta konuşlandırılırken, CPO'lara karşı sofistike oltalama veya fuzzing (bulanıklaştırma) saldırıları oluşturmak için düşman yapay zekası kullanılmaktadır.[10]

Bu dönüştürülmüş ortamda, Antoun ve arkadaşlarının "Detaylı Güvenlik Değerlendirmesi", tarihsel bir kıyaslama noktası olarak durmaktadır. Bu rapor, bulgularının ne kadar iyi yaşlandığını ve tanımlanan boşlukların nerede doldurulduğunu veya genişlediğini değerlendirmektedir.

---

2. Antoun vd. (2020) Çalışmasının Detaylı Analizi

GZFT analizine geçmeden önce, incelenen makalenin temel katkılarını damıtmak esastır. Joseph Antoun, Mohammad Ekramul Kabir, Bassam Moussa, Ribal Atallah ve Chadi Assi tarafından yazılan makale, 160'tan fazla atıf alarak alanında yüksek etkili bir çalışma olarak

kalmıştır.[3]

2.1 Temel Hedefler ve Kapsam

Yazarlar, EA, EVSE, Akıllı Sayaç ve Şebeke/Aggregator'ı entegre eden bir siber-fiziksel sistem olarak tanımladıkları EA şarj altyapısındaki güvenlik endişelerini tanımlamayı ve sınıflandırmayı amaçlamışlardır. Birincil motivasyonları, ilgili oyuncuların ve teknolojilerin çeşitliliğinin, şebeke istikrarını ve kullanıcı mahremiyetini etkileyen geniş bir saldırı yüzeyi oluşturduğu gözlemidir.[1]

2.2 Tehdit Modeli ve Varlık Analizi

Makale, varlıklar arasındaki etkileşimlere odaklanarak tehditleri kategorize etmek için sistematik bir yaklaşım kullanmaktadır:

- **Ev Şarjı:** Akıllı Sayaç ve Akıllı Şarj Cihazı arasındaki iletişimdeki güvenlik açıklarını, özellikle şarj programlarını değiştirebilecek veya tüketim verilerini tahrif edebilecek mesaj enjeksiyon saldırılarını tanımlamıştır.
- **Kamu Şarjı:** EA, Şarj İstasyonu (CS) ve Kontrol Merkezi (Aggregator) arasındaki karmaşık etkileşim ağına odaklanmıştır. Tanımlanan temel tehditler arasında, şarj isteklerinin sel gibi gönderilmesiyle yapılan Hizmet Reddi (DoS) saldırıları ve ödeme dolandırıcılığı veya kimlik hırsızlığına olanak tanıyan Ortadaki Adam (MitM) saldırıları yer almaktadır.[1]

2.3 Kritik Bulgular

- **Gizlilik Riskleri:** Makale, kamu şarj istasyonlarının hassas kullanıcı verilerini (kimlik, konum, ödeme bilgisi) talep ettiğini ve bunun siber saldırılar için bir işaret fişeği görevi gördüğünü açıkça vurgulamıştır. Kimlik doğrulama için kullanılan RFID kartlarının kolayca klonlanabilir olduğu belirtilmiştir.[1]
- **Protokol Zayıflıkları:** Yazarlar, dönemin hakim protokollerini (üstü kapalı olarak OCPP 1.6 ve erken ISO 15118 uygulamaları), açık metin iletişim kurdukları veya üreticilerin maliyetleri düşürmek için sıklıkla göz ardı ettiği isteğe bağlı güvenlik özelliklerine sahip oldukları için eleştirmişlerdir.
- **Şebeke Etkisi:** Güvenliği ihlal edilmiş EA'ların veya CS'lerin, güç şebekesine karşı koordineli saldırılar başlatmak, talebi manipüle ederek istikrarsızlığa neden olmak için bir

botnet'e dönüştürülebileceğini tespit etmişlerdir. Bu kavram, o günden bu yana "Siber-Fiziksel" güvenlik araştırmalarının ana odak noktası haline gelmiştir.

---

3. GZFT Analizi: Güçlü Yönler (İçsel Faktörler)

Makalenin 2024/2025 itibarıyla aldığı yüksek atıf sayısı, temel güçlü yönlerinin bir kanıtıdır.

3.1 Varlıklar ve Etkileşimlerin Kapsamlı Taksonomisi

Makalenin en önemli güçlü yönlerinden biri, şarj ekosisteminin bütünsel haritalanmasıdır. Yalnızca EA veya Akıllı Şebekeye odaklanan önceki çalışmaların aksine, Antoun ve arkadaşları *karşılıklı bağımlılıkları* başarıyla modellemiştir.

- **Siber-Fiziksel Bağlantı:** EA şarj ekosisteminin sadece bir BT ağı değil, bir Siber-Fiziksel Sistem (CPS) olduğunu doğru bir şekilde tanımlamışlardır. Dijital bir saldırının (mesaj enjeksiyonu) fiziksel bir sonuca (batarya bozulması veya şebeke kararsızlığı) nasıl dönüştüğünü haritalandırmışlardır.
- **Varlık İlişkileri:** Etkileşimlerin (EA ↔ EVSE, EVSE ↔ CSMS, Akıllı Sayaç ↔ Aggregator) dökümü, sonraki araştırmacılar için net bir yapısal çerçeve sağlamıştır. Bu taksonomi, araştırmacıların belirli bir bağlantıya (örneğin ISO 15118 aracılığıyla EA-EVSE bağlantısı) odaklanırken, bunun daha geniş sistemdeki yerini anlamalarına olanak tanıyan modüler tehdit modellemesine izin vermektedir.

3.2 Kritik Bir Vektör Olarak Mahremiyetin Erken Tespiti

2020 yılında endüstrinin odak noktası büyük ölçüde "menzil kaygısı" ve şarj cihazı bulunabilirliği üzerindeydi. Antoun ve arkadaşları, **mahremiyeti** benimsemenin önündeki kritik bir engel olarak vurgulayan belirgin sesler arasındaydı.

- **Granüler Veri Analizi:** Makale, tam olarak *hangi* verilerin risk altında olduğunu detaylandırmıştır: Konum geçmişi, şarj alışkanlıkları (yaşam tarzı kalıplarını ortaya çıkaran) ve faturalandırma verileri.
- **Düzenleyici Endişelerin Öngörülmesi:** Makale, mahremiyeti vurgulayarak, GDPR ve Kaliforniya Tüketici Mahremiyeti Yasası (CCPA) gibi düzenlemelerde görülen katı veri koruma gereksinimlerini öngörmüştür. Bu öngörü, makaleyi 2023-2025 yıllarında

geliştirilen mahremiyet koruyucu şarj şemaları (örneğin blokzincir tabanlı anonim kimlik doğrulama) için geçerli bir referans noktası haline getirmektedir.[13]

3.3 Sağlam Boşluk Analizi Çerçevesi

Makale sadece tehditleri listelemekle kalmamış; boşlukları güvenlik gereksinimlerine göre kategorize etmiştir: Kullanılabilirlik (Availability), Gizlilik (Confidentiality), Bütünlük (Integrity) ve Kimlik Doğrulama (Authenticity).

- **Yapılandırılmış Eksiklikler:** Örneğin, "Kullanılabilirlik DoS tarafından tehdit edilmektedir... ve OCPP tasarım hataları" şeklinde açıkça belirterek, yazarlar gelecekteki geliştiriciler için bir kontrol listesi sunmuştur.[14]
- **Daha Güçlü Kriptografi Çağrısı:** Makale, dağıtılan sistemlerde zorunlu simetrik/asimetrik şifreleme anahtarı yönetiminin eksikliğini göze çarpan bir boşluk olarak doğru bir şekilde tanımlamıştır. Bu, ISO 15118-20'deki "Tak ve Şarj Et" PKI (Açık Anahtar Altyapısı) geliştirmesiyle mükemmel bir uyum içindedir.[15]

---

4. GZFT Analizi: Zayıf Yönler (İçsel Faktörler)

Çığır açıcı olmasına rağmen, makale kapsamı ve metodolojisinden kaynaklanan ve sonraki literatürde eleştirilen bazı sınırlamalara sahiptir.

4.1 Deneysel Doğrulama Eksikliği

Sonraki araştırmacılar (örneğin Kaur vd., 2025; [17] kaynaklarında atıf yapanlar) tarafından makaleye yöneltilen birincil eleştiri, ampirik testler yerine teorik tehdit modellemesine dayanmasıdır.

- **Simülasyon vs. Gerçeklik:** Makale, "mesaj tahrifatı" veya "DoS" gibi saldırıları büyük ölçüde soyut olarak tartışmaktadır. Belirli bir OCPP 1.6J mesajının nasıl ele geçirildiğini veya değiştirildiğini gösteren bir test ortamından veri sunmamaktadır.
- **Sonraki Çalışmalarla Karşılaştırma:** Buna karşılık, sonraki çalışmalar (örneğin "Brokenwire" araştırması veya 2024'teki sızma testi çalışmaları [3]), somut kavram kanıtları (PoC), sinyal izleri ve donanım etki analizi sağlamaktadır. Antoun ve arkadaşlarının

çalışması tanımlayıcıdır, gösterici değildir; bu da belirli güvenlik açıklarını yeniden üretmeye veya yamalamaya çalışan mühendisler için faydasını sınırlamaktadır.

4.2 Tedarik Zinciri ve Fiziksel Güvenlik Üzerindeki Sınırlı Kapsam

Analiz, ağ katmanı tehditlerine (MitM, DoS) ağırlık vermektedir. O zamandan beri öne çıkan fiziksel ve tedarik zinciri risklerini yeterince temsil etmemektedir.

- **Fiziksel Erişim:** Makale USB portu istismarından kısaca bahsetmektedir [1], ancak kamu şarj cihazlarının fiziksel güvensizliğini (örneğin kolayca açılan kabinler, açıkta bırakılan hata ayıklama portları veya yan kanal saldırıları) derinlemesine analiz etmemektedir.
- **Tedarik Zinciri Kör Noktası:** Ürün yazılımı menşei, güvenliği ihlal edilmiş donanım bileşenleri (örneğin PLC modemleri) riski veya yazılım tedarik zinciri (örneğin OCPP yığınlarında kullanılan üçüncü taraf kütüphanelerdeki güvenlik açıkları) hakkında çok az tartışma vardır. 2025 yılında, Yazılım Malzeme Listesi'nin (SBOM) standart bir gereklilik haline gelmesiyle (örneğin NEVI'de), bu ihmal dikkat çekici bir zayıflıktır.[5]

4.3 Protokol Analizinin Eskimesi

Makale, ekosistemi kabaca 2019'da var olduğu şekliyle analiz etmektedir.

- **OCPP 1.x Odağı:** OCPP eleştirisi, OCPP 1.6 ve daha öncesine özgü güvenlik açıklarına (şifreleme eksikliği, açık metin kimlik doğrulama) odaklanmaktadır. Makale yayınlandığı sırada piyasaya sürülen OCPP 2.0.1'deki veya 2024'teki IEC 63584 standardizasyonundaki [7] sağlam güvenlik mekanizmalarını hesaba katmamaktadır.
- **ISO 15118-2 Kısıtları:** Araçtan şebekeye iletişim tartışması ISO 15118-2'ye dayanmaktadır. Zorunlu TLS 1.3 ve çift yönlü güç aktarımı güvenliğini getiren ISO 15118-20'nin (2022'de yayınlandı) nüanslarını kaçırmaktadır.[15] Sonuç olarak, V2G güvenliğine ilişkin önerileri, -20 standardında tanımlanan belirli kontrollere kıyasla biraz genel kalmaktadır.

---

5. Teknolojik Evrim: 2025 Temel Çizgisi

Antoun ve arkadaşlarının (2020) mevcut durumdaki geçerliliğini analiz etmek için, protokollerin ve teknolojilerin 2025 yılındaki durumunu detaylandırmak gerekir. Aşağıdaki tablolar, makalenin

analiz ettiği dönem ile günümüz arasındaki uçurumu göstermektedir.

5.1 Protokol Manzarası: Üç Sürümün Hikayesi

Özellik	OCPP 1.6J (2020 Standardı)	OCPP 2.0.1 (2025 Standardı)	OCPP 2.1 (Gelecek Vizyonu)
Şifreleme	Opsiyonel (Genellikle yok veya VPN ile)	Zorunlu (Güvenlik Profili 2/3)	Zorunlu ve Gelişmiş
Kimlik Doğrulama	Zayıf (HTTP Basic Auth, Açık Metin)	Karşılıklı TLS (mTLS), Sertifika Tabanlı	Merkeziyetsiz Kimlik (DID) Desteği
Cihaz Yönetimi	Sınırlı (Sadece belirli parametreler)	Kapsamlı (Cihaz Modeli, İzleme)	DER ve V2X Entegrasyonu
Güvenlik Açığı	MitM, DoS, Replay Saldırılarına Açık	İmza Doğrulama ile Bütünlük Koruması	Gelişmiş V2G Güvenliği

Analiz: Antoun ve arkadaşlarının eleştirdiği "güvenlik eksikliği", OCPP 1.6J için geçerlidir. Ancak 2025 yılında NEVI ve AFIR düzenlemeleri, yeni kurulumlarda OCPP 2.0.1 kullanımını fiilen zorunlu kılarak bu zayıflığı "teknik olarak" çözmüştür.[7]

5.2 Araç-Şebeke İletişimi: ISO 15118-2 vs. ISO 15118-20

Özellik	ISO 15118-2 (Antoun Dönemi)	ISO 15118-20 (2025 Dönemi)
Şifreleme Protokolü	TLS 1.2 (Bazı durumlarda opsiyonel)	TLS 1.3 (Zorunlu)

Çift Yönlü Şarj (V2G)	Sınırlı / Desteklenmiyor	Tam Destek (AC ve DC BPT)
Tak ve Şarj Et (PnC)	Var, ancak sertifika yönetimi karmaşık	Gelişmiş, Çoklu Sözleşme Desteği
Fiziksel Katman	HomePlug Green PHY	HomePlug Green PHY + Kablosuz (WPT)

Analiz: Makale, V2G güvenliği konusunda genel uyarılarda bulunurken, ISO 15118-20 bu uyarıları somut güvenlik önlemlerine (TLS 1.3 zorunluluğu, dijital imzalar) dönüştürmüştür.[15]

---

6. GZFT Analizi: Fırsatlar (Dışsal Faktörler)

Antoun ve arkadaşlarının (2020) çalışmasındaki boşluklar ve bulgular, sonraki araştırmalar ve endüstriyel gelişim için verimli bir zemin oluşturmuştur. Bu "Fırsatlar", makalenin alanı nasıl teşvik ettiğini ve hala nasıl alakalı olduğunu temsil eder.

6.1 YZ Destekli Saldırı Tespit Araştırmaları İçin Katalizör

Makalenin "veri değişimi" ve "mesaj tahrifatı" risklerini tanımlaması, Makine Öğrenimi (ML) uygulamaları için doğrudan bir fırsat yaratmıştır.

- **İmzalardan Anomalilere:** Antoun ve arkadaşları, çeşitli aktörlerin toplu veri alışverişinde bulunduğunu vurgulamıştır. Bu karakterizasyon, YZ tabanlı güvenlik için problem tanımı görevi görmektedir. 2024/2025 yıllarındaki araştırmacılar [10], OCPP trafiğindeki anomalileri tespit etmek için LSTM (Uzun Kısa Süreli Bellek) ve Otomatik Kodlayıcılar (Autoencoders) kullanımını haklı çıkarmak için bu tür değerlendirmelere atıfta bulunmuşlardır. Özellikle CICEVSE2024 veri seti gibi girişimler, bu teorik riskleri eğitilebilir modellere dönüştürmüştür.[11]
- **Davranışsal Analiz:** Makalenin ifşa edilen "şarj alışkanlıkları" hakkındaki endişesi, ham kullanıcı verilerini paylaşmadan farklı CPO'lar arasında saldırı tespit modellerini eğitmek için Federe Öğrenme (Federated Learning) kullanan *mahremiyet koruyucu* ML fırsatını öne çıkarmaktadır.

6.2 Blokzincir Entegrasyonu İçin Gerekçe

Makale, ekosistemde bir "güven" açığı tanımlamaktadır; özellikle dolaşım (roaming) yapan kullanıcıların kimliklerinin nasıl doğrulanacağı ve tek bir başarısızlık noktası olarak hareket eden merkezi bir otorite olmadan ödemelerin nasıl işleneceği konusunda.

- **Merkeziyetsiz Güvenlik:** Bu boşluk, blokzincir için kesin kullanım durumudur. 2023-2025 yıllarındaki çok sayıda makale [22], otomatik, güven gerektirmeyen faturalandırma için blokzincir tabanlı PKI veya akıllı sözleşmeler önermek amacıyla Antoun ve arkadaşları tarafından tanımlanan güvenlik açıklarına atıfta bulunmaktadır. Makale, blokzincir araştırmacılarının şu anda çözmekte olduğu problemi etkili bir şekilde çerçevelemiştir.

6.3 Politika ve Standardizasyon Üzerindeki Etki

Zorunlu güvenlik eksikliğine ilişkin "Boşluk Analizi", düzenleyiciler tarafından etkili bir şekilde "operasyonelleştirilmiştir".

- **Düzenleyici Doğrulama:** NEVI programının ISO 15118 ve güvenli ödeme ağ geçitleri (PCI DSS) gerekliliği, Antoun ve arkadaşları tarafından vurgulanan kesin güvenlik açıklarına (şifrelenmemiş veri, güvensiz ödemeler) bir politika yanıtı olarak görülebilir.[5] Buradaki fırsat, makalenin bu düzenlemelerin *neden* gerekli olduğuna dair tarihsel bir kanıt olarak hizmet etmesi ve politika etki değerlendirmeleri için yararlı olmasıdır.

---

7. GZFT Analizi: Tehditler (Dışsal Faktörler)

Bu faktörler, makalenin sonuçlarının 2025 manzarasındaki devam eden geçerliliğini veya doğruluğunu tehdit etmektedir.

7.1 Hızlı Protokol Evrimi ("Çözülmüş Problem" Tehdidi)

Makalede belirtilen spesifik güvenlik açıklarının çoğu, daha yeni standartlar tarafından teorik

olarak "çözülmüştür", bu da makalenin spesifik eleştirilerini güncelliğini yitirmiş hale getirmektedir.

- **Zorunlu Şifreleme:** Makale, açık metin iletişimi konusunda uyarmaktadır. Ancak, OCPP 2.0.1 Güvenlik Profili 2 ve 3 TLS'yi *zorunlu kılar*.[6] Bir CPO, OCPP 2.0.1'i (NEVI'nin gerektirdiği şekilde) doğru bir şekilde uygularsa, "açık metin OCPP mesajlarını koklama" tehdidi etkisiz hale getirilir. Makaleye yönelik tehdit, yavaş yavaş kullanımdan kaldırılan eski bir teknolojinin (OCPP 1.6) eleştirisi haline gelmesidir.
- **TLS 1.3 Benimsenmesi:** ISO 15118-20, 2020'de geçerli olabilecek eski şifreleme paketlerini ve el sıkışma (handshake) güvenlik açıklarını ortadan kaldıran TLS 1.3'ü zorunlu kılar.

7.2 Fiziksel Katman Saldırılarının Ortaya Çıkışı ("Yeni Vektör" Tehdidi)

Tehdit manzarası, Antoun ve arkadaşlarının kapsamadığı katmanlara kaymıştır.

- **Sinyal Karıştırma ve Yanıltma (Brokenwire):** [8] kaynaklarında detaylandırıldığı üzere, HomePlug Green PHY standardının CSMA/CA davranışını hedef alan "Brokenwire" güvenlik açığının keşfi, şarj oturumlarını kablosuz olarak ve uzaktan durdurabilen bir saldırı sınıfını temsil etmektedir. Bu, Antoun ve arkadaşlarının öngörmediği bir saldırı türüdür; onların odak noktası *protokol* mantığı (mesajlar) iken, Brokenwire bir *sinyal* saldırısıdır ve 12 milyon aracı etkileme potansiyeline sahiptir.[25]
- **Donanım Tabanlı Saldırılar:** Yazılım sertleştikçe, saldırganlar donanıma yönelmektedir. Makalenin donanım güvenliğine (Güvenilir Platform Modülleri - TPM, Güvenli Önyükleme - Secure Boot) odaklanmaması, saldırganların anahtarları çıkarmak için bir kamu şarj cihazına fiziksel olarak müdahale edebileceği 2025 dönemi tehditlerine karşı onu daha az alakalı hale getirmektedir.

---

8. Stratejik Boşluk Analizi 2.0: 2020 Önerileri ve 2025 Gerçekliği

Bu raporun kritik bir bileşeni, Antoun ve arkadaşlarının gerçekleştirdiği "Boşluk Analizi"ni değerlendirmektir. Endüstri bu uyarıları dikkate aldı mı? Bu boşluklar kapatıldı mı?

8.1 Kullanılabilirlik (Availability)

- **2020 Boşluğu:** Makale, DoS ve DDoS'u kullanılabilirliğe yönelik birincil tehditler olarak tanımlamış ve standart protokollerde koruma eksikliğine dikkat çekmiştir.
- **2025 Durumu: Kısmen Kapatıldı.**
  - *İlerleme:* OCPP 2.0.1, ağ kesintileri sırasında kullanılabilirliği sürdürmek için kalp atışı (heartbeat) mekanizmalarını ve çevrimdışı davranış mantığını iyileştirmiştir.[26]
  - *Kalan Boşluk:* CSMS bulut arka ucuna yönelik Dağıtık Hizmet Reddi (DDoS) saldırıları büyük bir tehdit olmaya devam etmektedir. Ayrıca, "Brokenwire" saldırısı, yazılım protokollerinin kolayca düzeltemeyeceği *fiziksel* bir DoS vektörü sunmaktadır, çünkü iletişim ortamını (PLC) karıştırmaktadır.

8.2 Gizlilik ve Mahremiyet (Confidentiality & Privacy)

- **2020 Boşluğu:** İletişim bağlantılarında şifreleme eksikliği; kullanıcı kimliği ve konumunun sızması.
- **2025 Durumu: Standartlarda Çoğunlukla Kapatıldı, Uygulamada Açık.**
  - *İlerleme:* TLS, OCPP 2.0.1 (Profil 2/3) ve ISO 15118-20'de artık zorunludur. "Tak ve Şarj Et" standardı şifreli sertifikalar kullanır.
  - *Gerçeklik Kontrolü:* 2024 tarihli bir çalışma [2], *konuşlandırılmış* şarj cihazlarının yalnızca %12'sinin TLS uyguladığını tespit etmiştir. *Standartlar* boşluğu düzeltmiş olsa da, *dağıtım* (deployment) önemli ölçüde geride kalmaktadır. ws:// üzerinden çalışan eski OCPP 1.6J şarj cihazları hala yaygındır.

8.3 Bütünlük (Integrity)

- **2020 Boşluğu:** Mesaj tahrifatı (SoC veya fatura verilerini değiştirme).
- **2025 Durumu: Dijital İmzalarla Adreslendi.**
  - *İlerleme:* ISO 15118-20 ve OCPP 2.0.1, verilerin aktarım sırasında değiştirilmediğinden emin olmak için dijital imzalar (XML/JSON imzaları veya TLS bütünlük kontrolleri) kullanır.
  - *Yeni Boşluk: Ürün yazılımının* (firmware) bütünlüğü artık savaş alanıdır. Güvenli Önyükleme ve imzalı ürün yazılımı güncellemeleri (OCPP 2.0.1'de zorunlu kılınmıştır) yeni savunmadır, ancak eski şarj cihazları fiziksel portlar aracılığıyla kötü amaçlı yazılım enjeksiyonuna karşı savunmasız kalmaya devam etmektedir.

8.4 Kimlik Doğrulama (Authenticity)

- **2020 Boşluğu:** EA veya Şarj İstasyonlarının taklit edilmesi (Impersonation).
- **2025 Durumu: PKI ile Resmileştirildi.**
  - *İlerleme:* Endüstri, sağlam bir Açık Anahtar Altyapısına (PKI) doğru ilerlemiştir. ISO 15118-20, OEM'ler ve CPO'lar tarafından yüklenen sertifikaları kullanarak karşılıklı kimlik doğrulamayı (araç şarj cihazını, şarj cihazı aracı doğrular) zorunlu kılar.
  - *Zorluk:* Sertifika yönetimi karmaşıktır. Antoun ve arkadaşları kimlik doğrulama ihtiyacını doğru bir şekilde tanımlamışlardır, ancak küresel, birlikte çalışabilir bir PKI'nın *uygulanması* (Hubject modeli veya diğerleri) bir sürtünme noktası ve potansiyel bir merkezi başarısızlık noktası olmaya devam etmektedir.[27]

---

9. Sonuç ve Gelecek Perspektifi

"A Detailed Security Assessment of the EV Charging Ecosystem" (Antoun vd., 2020), e-mobilite güvenliği kütüphanesinde temel bir belge olarak kalmaya devam etmektedir. Çalışmanın **Güçlü Yönü**, mahremiyet, kullanılabilirlik ve şebeke istikrarı gibi kritik vektörleri, bunlar ana akım endişeler haline gelmeden çok önce doğru bir şekilde tanımlayan kapsamlı, yapısal tehdit modelleme yaklaşımında yatmaktadır.

Ancak, makalenin **Zayıf Yönleri**—özellikle deneysel doğrulama eksikliği ve hızla eskidiyen protokollere odaklanması—2025 yılına gelindiğinde daha belirgin hale gelmiştir. Geçerliliğine yönelik **Tehditler**, teknolojik bir paradigma değişimi (OCPP 2.0.1, ISO 15118-20) ve güvenliği "önermekten" "zorunlu kılmaya" geçen bir düzenleyici ortam (NEVI, AFIR) tarafından yönlendirilmektedir.

Yine de, makaleden doğan **Fırsatlar** derindir. Mevcut teknolojilerin (Blokzincir, YZ IDS, PKI) şu anda çözmekte olduğu problem alanını tanımlamıştır. 2025 yılındaki bir araştırmacı veya analist için Antoun ve arkadaşları (2020), mevcut güvenlik açıklarına yönelik bir rehber olarak değil (bunların çoğu yamalanmış veya aşılmıştır), EA şarj saldırı yüzeyinin temel mimari diyagramı olarak değerlidir. Modern güvenlik standartlarının "neyi" içerdiğinin arkasındaki "neden"i sağlamaktadır.

Sonuç olarak, Antoun ve arkadaşlarının spesifik teknik eleştirileri öncelikle eski altyapı için geçerli olsa da, güç şebekesine yönelik siber-fiziksel risklere ilişkin sistemik analizleri acil ve geçerli olmaya devam etmektedir. Ekosistem çift yönlü enerji akışına doğru ilerlerken, yazarların "entegrasyonun... saldırganlara birden fazla sektörün işlevselliğini bozma gücü verdiği" yönündeki uyarısı her zamankinden daha ileri görüşlüdür.

Atıflar:
.1

Alıntılanan çalışmalar

1. A_Detailed_Security_Assessment_of_the_EV_Charging_Ecosystem.pdf
2. Current Affairs: A Security Measurement Study of CCS EV Charging Deployments - arXiv, erişim tarihi Kasım 22, 2025, https://arxiv.org/html/2404.06635v2
3. A Detailed Security Assessment of the EV Charging Ecosystem - Semantic Scholar, erişim tarihi Kasım 22, 2025, https://www.semanticscholar.org/paper/A-Detailed-Security-Assessment-of-the-EV-Charging-Antoun-Kabir/43e9e3be70a58d0fc1eda7e5e47e19d21e898e4d
4. AFIR Update Spring 2025: ISO 15118-20, Smart Charging - Pionix, erişim tarihi Kasım 22, 2025, https://www.pionix.com/news/afir-regulation-update-spring-2025
5. Privacy and Cybersecurity Standards for NEVI Funded EV Charging Station Projects, erişim tarihi Kasım 22, 2025, https://www.bakerdonelson.com/privacy-and-cybersecurity-standards-for-nevi-funded-ev-charging-station-projects
6. OCPP 1.6 vs OCPP 2.0: A Detailed Comparison for EV Chargers - Luxman Energy, erişim tarihi Kasım 22, 2025, https://www.luxmanenergy.com/ocpp-1-6-vs-ocpp-2-0-a-detailed-comparison-for-ev-chargers/
7. OCPP (Open Charge Point Protocol), erişim tarihi Kasım 22, 2025, https://openchargealliance.org/protocols/open-charge-point-protocol/
8. Brokenwire Attack, erişim tarihi Kasım 22, 2025, https://www.brokenwire.fail/
9. CVE-2022-0878 - NVD, erişim tarihi Kasım 22, 2025, https://nvd.nist.gov/vuln/detail/CVE-2022-0878
10. Enhancing the Detection of Cyber-Attacks to EV Charging Infrastructures Through AI Technologies - ResearchGate, erişim tarihi Kasım 22, 2025, https://www.researchgate.net/publication/397267663_Enhancing_the_Detection_of_Cyber-Attacks_to_EV_Charging_Infrastructures_Through_AI_Technologies
11. Enhancing the Detection of Cyber-Attacks to EV Charging Infrastructures Through AI Technologies - MDPI, erişim tarihi Kasım 22, 2025, https://www.mdpi.com/2079-9292/14/21/4321
12. Joseph antoun - Google Scholar, erişim tarihi Kasım 22, 2025, https://scholar.google.ae/citations?user=DBSBM_EAAAAJ&hl=iw
13. [PDF] Electric Vehicle Charging: A Survey on the Security Issues, erişim tarihi Kasım 22, 2025, https://www.semanticscholar.org/paper/Electric-Vehicle-Charging%3A-A-Survey-on-the-Security-Garofalaki-Kosmanos/77e7d7af7b4d498dce940dd407344e4a8f1f3883
14. A Detailed Security Assessment of the EV Charging Ecosystem - IEEE Xplore, erişim tarihi Kasım 22, 2025, https://ieeexplore.ieee.org/document/8994200

15. EV Cybersecurity & ISO 15118 for Secure Charging Infrastructure - PlaxidityX, erişim tarihi Kasım 22, 2025, https://plaxidityx.com/blog/blog-post/iso-15118-ev-cybersecurity-guide/
16. Electric vehicle Plug and Charge technology 101 - Irdeto Insights, erişim tarihi Kasım 22, 2025, https://irdeto.com/blog/electric-vehicle-plug-and-charge-technology-101
17. Federated detection of open charge point protocol 1.6 cyberattacks - OAE Publishing Inc., erişim tarihi Kasım 22, 2025, https://www.oaepublish.com/articles/ces.2025.04
18. CMC | Free Full-Text | Comprehensive Black-Box Fuzzing of Electric Vehicle Charging Firmware via a Vehicle to Grid Network Protocol Based on State Machine Path - Tech Science Press, erişim tarihi Kasım 22, 2025, https://www.techscience.com/cmc/v84n2/62867/html
19. OCPP 1.6 vs. OCPP 2.0: A Comprehensive Comparison - Ampcontrol, erişim tarihi Kasım 22, 2025, https://www.ampcontrol.io/post/ocpp-1-6-vs-ocpp-2-0-a-comprehensive-comparison
20. Intelligent Charging With the New ISO 15118-20 Standard - Vector, erişim tarihi Kasım 22, 2025, https://cdn.vector.com/cms/content/know-how/_technical-articles/Emobility_ISO15118-20_Charging_emobliltytec_202210_PressArticle_EN.pdf
21. Transfer learning for securing electric vehicle charging infrastructure from cyber-physical attacks - PMC - PubMed Central, erişim tarihi Kasım 22, 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC11920061/
22. A Hybrid Blockchain Solution for Electric Vehicle Energy Trading: Balancing Proof of Work and Proof of Stake - MDPI, erişim tarihi Kasım 22, 2025, https://www.mdpi.com/1996-1073/18/7/1840
23. Blockchain-Based Secure Firmware Updates for Electric Vehicle Charging Stations in Web of Things Environments - MDPI, erişim tarihi Kasım 22, 2025, https://www.mdpi.com/2032-6653/16/4/226
24. The Role of Blockchain in Securing EV Charging Transactions | by AppVin Technologies, erişim tarihi Kasım 22, 2025, https://medium.com/@appvintechnologies/the-role-of-blockchain-in-securing-ev-charging-transactions-1d73460206ad
25. Your EV Charger Is a 47-Meter Security Disaster: The Brokenwire Wake-Up Call, erişim tarihi Kasım 22, 2025, https://thesmallbusinesscybersecurityguy.co.uk/blog/brokenwire-ev-charging-attack-security-disaster-2025
26. A comprehensive guide to OCPP 2.0.1 - eDRV, erişim tarihi Kasım 22, 2025, https://www.edrv.io/guide/ocpp-2-0-1-comprehensive-guide
27. ISO 15118: Definition, key features, benefits, adoption, and compliance - Monta, erişim tarihi Kasım 22, 2025, https://monta.com/en/blog/iso-15118/
28. Electric Vehicle Charging: A Survey on the Security Issues and Challenges of the Open Charge Point Protocol (OCPP) - ResearchGate, erişim tarihi Kasım 22, 2025, https://www.researchgate.net/publication/361447469_Electric_Vehicle_Charging_

a_Survey_on_the_Security_Issues_and_Challenges_of_the_Open_Charge_Point_Protocol_OCPP
29. EU Alternative Fuels Infrastructure Regulation (AFIR) | Charging and Hydrogen Networks, erişim tarihi Kasım 22, 2025, https://netzerocompare.com/policies/eu-alternative-fuels-infrastructure-regulation-eu-afir
30. National Electric Vehicle Infrastructure Formula Program Annual Report: Plan Year 2023-2024, erişim tarihi Kasım 22, 2025, https://driveelectric.gov/files/nevi-annual-report-2023-2024.pdf