ChatGPT

V2G Botnet Saldırısı ile Şebeke Dengesizliği Anomalisi

Anomalinin Tanımı (Siber-Fiziksel Etkilerle Birlikte)

Bu anomali, **Vehicle-to-Grid (V2G)** özellikli elektrikli araç şarj altyapısına yönelik koordineli bir siber saldırı sonucunda elektrik şebekesinde oluşan dengesizlik halini tanımlamaktadır. Kötü niyetli bir aktör, bir **botnet** ağına dönüştürdüğü birden fazla şarj istasyonunu eşzamanlı komutlarla yöneterek şebekede ani ve olağandışı yük değişimleri yaratır. Özel olarak, saldırgan aynı anda birçok istasyona OCPP protokolü üzerinden *"RemoteStartTransaction"* komutu yollayarak yüksek güçlü şarj işlemlerini başlatmakta ve bazı V2G modunda çalışan istasyonlara *"RemoteStopTransaction"* komutu yollayarak şebekeye enerji geri beslemesini (deşarjı) aniden kesmektedir [1] [2]. Bu senaryoda eşzamanlı gerçekleşen aşırı enerji çekişi (yük talebinde ani zirve) ve enerji arzındaki düşüş, şebekede ciddi dengesizlik yaratır.

Ortaya çıkan **siber-fiziksel etki**, elektrik şebekesinin anlık yük dengesini bozarak frekans ve gerilim sapmalarına yol açmasıdır. Normalde coğrafi olarak ve zamansal olarak dağılım göstermesi beklenen elektrik talebi, saldırı anında **istatistiksel olarak anormal bir şekilde tek bir zaman dilimine yoğunlaşır** [3]. Örneğin, bir şehirde binlerce EV'nin aynı birkaç saniyelik dilimde 22 kW çekmeye başlaması yerel transformatörlerin kapasitesini aşabilir ve hatları aşırı yükleyebilir [3]. Benzer şekilde, şebekenin V2G üzerinden almakta olduğu anlık destek gücünün (örneğin 100 MW) birden kesilmesi, aniden bir santralın devreden çıkmasıyla eşdeğer etki yaratır [4]. Sonuç olarak arz-talep dengesinin bozulması, şebeke frekansının güvenli sınırların dışına çıkmasına neden olur. Elektrik şebekeleri çok hassas bir dengeyle, örneğin ~50 Hz nominal frekansta çalışır; **ani talep artışları veya arz kayıpları bu frekansı tehlikeli düzeyde düşürür (under-frequency)**, tersi şekilde **ani fazla enerji beslemesi frekansı tehlikeli düzeyde yükseltir (over-frequency)** [5]. Frekansın hızlı şekilde sınırları aşması halinde devreye giren koruma röleleri, jeneratörleri ve transformatörleri korumak adına bölgesel elektrik kesintileri (koruyucu black-out) yapmak zorunda kalır [6]. Nitekim literatürde bu tür **dinamik yük değiştirme saldırılarının** (MadIoT tarzı) senkronize EV şarj manipülasyonları ile **şebekeyi kararsız hale getirip geniş çaplı kesintilere yol açabileceği** gösterilmiştir [7] [8]. Özetle, anomali hem siber boyutta (zararlı komutların koordinasyonu) hem de fiziksel boyutta (güç sisteminin dengesinin bozulması) etkisini gösteren bir **fiziksel DDoS** saldırısı biçimidir [9].

V2G Sistem Mimarisi İçindeki Rolü

Bu saldırı senaryosu, V2G sistem mimarisinin zafiyetlerinden yararlanarak ortaya çıkmaktadır. V2G teknolojisi, elektrikli araçların sadece tüketici olarak şebekeden enerji çekmesini değil, aynı zamanda birer dağıtık enerji kaynağı olarak depoladıkları enerjiyi şebekeye geri vermesini mümkün kılan çift yönlü bir yaklaşımdır [10]. Başka bir deyişle, bir elektrikli araç (EV) şarj istasyonuna bağlıyken akıllı şebeke ile etkileşim halinde bataryasını şarj edebilir veya ihtiyaç halinde bataryasındaki enerjiyi şebekeye boşaltarak *enerji sağlayıcı* rolü üstlenebilir [11]. Bu sayede V2G, özellikle yenilenebilir enerji üretiminin dalgalı olduğu durumlarda şebeke dengesini sağlamak için EV'leri birer **dağıtık depolama ünitesi** (DER) olarak kullanmayı hedefler [12]. Tipik bir V2G mimarisinde, bir **Elektrikli Araç Şarj İstasyonu (EVSE)** cihazı EV ile şebeke arasındaki fiziksel ve iletişimsel arabirimi sağlar. EVSE'ler internete bağlı, uzaktan yönetilebilir IoT cihazlarıdır ve **Akıllı Şebeke** altyapısının bir parçasıdır [13]. Birden çok

şarj istasyonunu yöneten merkezi bir **Şarj Operatörü (CPO)** veya **agregatör** sunucusu bulunur; bu merkezileştirilmiş sistem istasyonların durumunu izler, enerji akışlarını optimize eder ve faturalandırmayı yürütür [14]. CPO ile istasyonlar arasındaki iletişim, endüstri standardı **Open Charge Point Protocol (OCPP)** üzerinden sağlanır [15].

Normal şartlarda bu mimari, şebekenin kararlı çalışmasına katkıda bulunur. Örneğin, agregatör/CPO tarafı elektrik arz-talep dengesine göre EV'lerin şarj ve deşarj profilini ayarlayarak frekans regülasyonu veya tepki gücü desteği gibi **talep tarafı yönetimi** hizmetleri sunabilir [11] [12]. Ancak, mimarinin sunduğu bu esneklik ve uzaktan kontrol imkânı, aynı zamanda suistimal edilebilecek bir saldırı yüzeyi oluşturmaktadır. İncelenen anomali, V2G sistem mimarisinin **güçlü yönünü (birden çok EV'nin merkezden kontrol edilebilmesi)** tersine çevirerek bir zafiyete dönüştürür. Saldırgan, ya merkezi CPO platformunu ele geçirerek ya da her bir istasyonu bireysel olarak kompromize edip emirlerine uyan "zombi" cihazlar haline getirerek, normalde şebekeyi dengelemek için kullanılabilecek kontrol mekanizmasını şebekeyi dengesizleştirmek için kullanmaktadır. Bu senaryoda 10 adet şarj istasyonundan oluşan bir V2G altyapısı düşünülmüştür. Her bir istasyon, OCPP aracılığıyla CPO'ya bağlıdır ve çift yönlü enerji akışını gerçekleştirmektedir. Saldırı öncesinde bu istasyonlar şebeke ile **iki yönlü etkileşim** halindedir: bazı EV'ler bataryalarını şarj ederek şebekeden güç çekerken, diğerleri V2G modunda deşarj yaparak talep fazlası enerjiyi şebekeye geri vermektedir. Bu **dağıtık ve koordineli yapı**, kötü niyetli bir aktörün eline geçtiğinde tüm istasyonların senkronize bir şekilde hareket etmesi sağlanarak toplu bir yük saldırısına zemin hazırlanmaktadır. Literatürde, V2G sistemine yeni eklenen her bir bileşenin (EV, EVSE, agregatör vb.) kendi güvenlik açıklarını beraberinde getirdiği ve birden çok paydaşın dâhil olduğu bu karmaşık yapıda koordinasyon açıklarının oluşabileceği vurgulanmıştır [16]. İncelemiş olduğumuz anomali, V2G mimarisindeki bu çok bileşenli yapının güvenlik açıdan en zayıf halkalarını hedef alarak (örneğin, korunmasız şarj istasyonları veya güvenliği zayıf bir merkezi sunucu) ortaya çıkmaktadır. Sonuç olarak, V2G'nin normalde şebeke istikrarını **güçlendirme** rolü, saldırı esnasında istismar edilerek şebeke istikrarını **tehdit eden** bir araca dönüşmektedir.

OCPP Üzerinden Saldırının Nasıl Tetiklendiği

Open Charge Point Protocol (OCPP), elektrikli araç şarj istasyonları (Charge Point, EVSE) ile merkezi yönetim sistemi (Central System, CPO platformu) arasında iletişimi sağlayan, sektörde yaygın olarak benimsenmiş bir protokoldür [15]. OCPP, istasyonların durum bilgilerini, ölçüm değerlerini ve olayları merkeze iletmesine olanak tanırken; merkezin de istasyonlara çeşitli **uzaktan komutlar** göndermesine imkân tanır. OCPP mesajları genel olarak **istek-yanıt** modeline göre çalışır ve bir şarj istasyonunu uzaktan yönetmek için gerekli kritik fonksiyonları içerir [17] [18]. Örneğin, *RemoteStartTransaction* mesajı, merkezi sistem tarafından bir istasyonda uzaktan yeni bir şarj oturumu başlatmak için kullanılırken; *RemoteStopTransaction* mesajı, hâlihazırda devam eden bir şarj/deşarj oturumunu sonlandırmak için gönderilir [18]. Bu iki komut, incelenen saldırı anomalisi için temel araçlardır.

Saldırganın hedefine ulaşabilmesi için OCPP iletişimini kötüye kullanması gerekmektedir. Bunun birkaç olası vektörü bulunmaktadır: (i) Saldırgan CPO'nun arka uç sunucusunu ele geçirerek istasyonlara merkezi sistem kimliğiyle komut gönderebilir; (ii) veya her bir istasyonun zafiyetlerinden faydalanarak istasyonları kendi kontrolündeki bir sahte merkezi sisteme bağlayabilir (örneğin zayıf kimlik doğrulama mekanizmalarını atlatıp istasyonlara *kendi komuta sunucusunu* CSMS gibi tanıtmak mümkündür [19] [20]); (iii) ya da OCPP mesajlarını dinleyip tekrar oynatarak yetkisiz işlemler başlatabilir. Nitekim OCPP 1.6 protokolündeki zayıf kimlik doğrulama yüzünden bir saldırganın meşru bir istasyon kimliğini taklit ederek CSMS ile bağlantı kurması mümkün olabilmektedir [21] [22]. Bu sayede kötü niyetli aktör, *RemoteStartTransaction* ve *RemoteStopTransaction* gibi mesajları sanki merkezi yönetimden geliyormuşçasına istasyonlara iletebilir. Literatürde, OCPP mesajlarına yönelik **yeniden oynatma (replay)** saldırılarının, örneğin daha önce kaydedilmiş bir *StartTransaction* isteğini yeniden göndererek yetkisiz şarj oturumları başlatabileceği gösterilmiştir [23]. İncelenen senaryoda da benzer şekilde

saldırgan, OCPP üzerinden istasyonlara gönderilen bu kritik komutları kullanarak anomaliyi tetiklemektedir. Sızma aşamasını tamamlamış olan saldırgan, kontrolündeki istasyonların her birine eşzamanlı komutlar yollar:

- **Yüksek Güçlü Şarj Başlatma (Demand Spike)** – *RemoteStartTransaction*: Saldırgan botnet'indeki tüm uygun istasyonlara aynı anda "maksimum güçte şarja başla" komutu gönderir [24]. Bu komutu alan her istasyon, bağlı olduğu EV'nin derhal yüksek akımla şarj olmasını sağlar. Normal şartlarda, bir EV'nin uzaktan şarj edilmeye başlaması için kullanıcının yetkilendirilmesi gerekse de saldırgan ele geçirdiği sistemlerde kimlik denetimini ya atlamış ya da geçerli kimlik bilgilerini ele geçirmiştir. Dolayısıyla bir komutla birden fazla aracı saniyeler içinde şebekeden yoğun şekilde enerji çeker hale getirir.
- **V2G Deşarjı Durdurma (Supply Drop)** – *RemoteStopTransaction*: Aynı anda, o esnada şebekeye enerji veren (deşarj modunda) durumda olan tüm EV'lere "deşarjı kes" komutu yollanır [2]. Bu komut, V2G oturumunu sonlandırdığı için ilgili istasyonlarda şebekeye enerji akışı aniden durur. Örneğin normalde şebekeye belirli bir güçle destek veren 5 EV varsa, bu komut sonrası destekleri sıfırlanacaktır.

Bu şekilde saldırgan, OCPP protokolünün sunduğu uzaktan yönetim fonksiyonlarını kötüye kullanarak **eş zamanlı ve zıt yönlü enerji akışı değişimleri** yaratır. Söz konusu komutlar OCPP'de tasarım itibariyle **yararlı** işlemler (uzaktan şarj başlatma/durdurma) için bulunsa da, uygun güvenlik önlemleri alınmadığında koordineli olarak kullanıldığında birer saldırı silahına dönüşebilir. Gerçekleştirilen senaryoda 10 istasyondan oluşan bir botnet kullanılmıştır ancak aynı taktik, ele geçirilen **yüzlerce ya da binlerce istasyona ölçeklenebilirse**, talep tarafında yaratılan bu oynama ile ulusal ölçekte dahi elektrik kesintilerine yol açabilecek güçlü bir saldırı ortaya çıkacaktır [25].

Simülasyon Senaryosu: 10 Sanal Şarj İstasyonu ile Saldırının Modellenmesi

Gerçek hayatta böyle bir saldırının etkileri en çok binlerce istasyonun eşzamanlı hareketiyle ortaya çıkacaksa da, kavramsal olarak durumu incelemek üzere 10 adet sanal şarj istasyonundan oluşan küçük ölçekli bir sistemin benzetimi yapılmıştır. Bu simülasyonda her bir istasyonun anlık güç akışı (pozitif değerler şebekeden çekilen şarj gücünü, negatif değerler şebekeye verilen V2G deşarj gücünü temsil edecek şekilde) modellenmiştir. Başlangıçta sistem dengeli bir durumdadır: istasyonların yarısı şebekeden araçları şarj etmekte, diğer yarısı ise V2G modunda araç bataryalarından şebekeye güç vermektedir. Özellikle, **İstasyon 1–5** aralığı her biri yaklaşık **-10 kW** güçle (negatif işaretli) çalışarak şebekeye toplam 50 kW civarında enerji beslemektedir. **İstasyon 6–10** ise o anda aktif şarj yapmamakta (0 kW düzeyinde bekleme halindedir). Bu durum, basitleştirilmiş olarak, şebekenin EV'ler vasıtasıyla net 50 kW'lık bir destek aldığı (talebin 50 kW daha düşük göründüğü) bir denge hali anlamına gelir. Aşağıdaki tabloda saldırı öncesi ve saldırı anı sonrası istasyon güç seviyeleri özetlenmiştir:

İstasyonlar	Saldırı Öncesi Güç Durumu	Saldırı Sonrası Güç Durumu	Açıklama
1 – 5	-10 kW (V2G deşarj)	0 kW (Deşarj durduruldu)	**Arz Düşüşü** (Tip B)
6 – 10	0 kW (beklemede)	+20 kW (şarja başladı)	**Talep Artışı** (Tip A)

Yukarıdaki senaryoda saldırının gerçekleştirildiği anda (T_0) her bir deşarj halindeki istasyonun şebekeye gücü sıfıra inmiş, aynı zamanda 5 adet istasyon da aniden 20'şer kW düzeyinde şebekeden çekişe başlamıştır. Bu değerler, tipik bir AC orta seviye şarj cihazının (~20–22 kW) güç kapasitesine denk seçilmiştir. Dolayısıyla toplamda sistem, **saldırı öncesi** yaklaşık **-50 kW** net güçten (şebekeye destek) **saldırı sonrası** yaklaşık **+100 kW** net yüke (şebekeden çekiş) geçerek **150 kW'lık ani bir değişim**

yaşamıştır. Küçük bir sistem ölçeğinde 150 kW'lık sıçrama, mutlak değer olarak sınırlı görünse de, oransal olarak bakıldığında ciddi bir dengesizliktir. Daha büyük bir EV popülasyonu söz konusu olsaydı, bu güç değişimi orantılı şekilde artacak ve örneğin **150 MW** mertebelerine ulaşarak geniş alanlı elektrik kesintilerine neden olabilecekti [4].

Simülasyon kurgusunda ayrıca şebekenin EV'ler dışındaki geri kalan yük talebini temsil eden sabit bir **baz yük** değeri de tanımlanmıştır. Örneğimizde baz yük 500 kW olarak alınmıştır. Böylece saldırı öncesinde toplam şebeke yükü = 500 kW (baz) – 50 kW (EV desteği) = **450 kW** olarak sabit seyretmektedir. Saldırı anında EV'lerin ani davranış değişimi ile toplam yük = 500 kW + 100 kW (EV talebi) = **600 kW** seviyesine çıkmıştır. Bu değişimin zaman ekseninde seyri, Python kullanılarak gerçekleştirilen bir zaman adımlı simülasyonla modellenmiştir.

Python Temelli Simülasyon Kodları

Aşağıda, tanımlanan senaryoyu canlandırmak için kullanılan Python kodları sunulmuştur. Bu kod, 10 istasyonlu sistemin güç profilini zaman içinde hesaplamakta ve saldırının etkisini grafiksel olarak ortaya koymaktadır. Simülasyon için **NumPy** ve **Matplotlib** kütüphaneleri kullanılmıştır. Kod içinde önce başlangıç durumu verileri tanımlanmış, ardından T_0 anındaki saldırının istasyon güçlerine etkisi uygulanmıştır. Son olarak, şebeke baz yükü ile EV'lerin net gücünü toplayarak toplam şebeke yükünün zaman serisi elde edilmiş ve grafik çizdirilmiştir. Kodda gereken yerlere açıklayıcı yorumlar eklenmiştir:

```
import numpy as np
import matplotlib.pyplot as plt

# Zaman parametreleri
T_max = 100               # toplam simülasyon süresi (saniye)
dt = 1                    # zaman adımı (1 saniye)
t = np.arange(0, T_max+1, dt)

# Sistem parametreleri
base_load = 500           # şebekenin EV dışı baz yükü [kW]
n_stations = 10           # toplam sanal şarj istasyonu sayısı
attack_time = 60          # saldırının tetiklendiği an (saniye)

# Başlangıçta her bir istasyonun güç durumu (liste veya dizi olarak)
# İstasyon 1-5: -10 kW (V2G modunda şebekeye güç veriyor)
# İstasyon 6-10: 0 kW (beklemede, araç bağlı ama şarj almıyor)
station_powers_initial = np.array([-10]*5 + [0]*5)  # uzunluk 10

# Her zaman adımı için istasyon güç matrisini oluştur (satırlar zaman,
sütunlar istasyonlar)
station_powers = np.tile(station_powers_initial, (len(t), 1))

# Saldırı anından itibaren yeni güç değerlerini uygula:
# İstasyon 1-5 deşarjı durduracak -> güçleri 0 kW olacak
# İstasyon 6-10 şarja başlayacak -> güçleri +20 kW olacak
station_powers[t >= attack_time, 0:5] = 0    # 1-5 durduruldu
station_powers[t >= attack_time, 5:10] = 20  # 6-10 tam güç şarja başladı

# Her an için EV'lerin toplam güç çekişi (+) veya beslemesi (-) [kW]
```

```
net_EV_power = station_powers.sum(axis=1)
# her zaman adımında 10 istasyonun toplamı

# Toplam şebeke yükü = baz yük + net EV gücü (not: net EV gücü negatifse bu
şebeke yükünü azaltır)
total_grid_load = base_load + net_EV_power

# Sonuçların görselleştirilmesi
plt.figure(figsize=(8, 5))
plt.plot(t, total_grid_load, label='Saldırı Senaryosu (Toplam Yük)')
plt.axvline(attack_time, color='r', linestyle='--', label='Saldırı Anı T0')
plt.xlabel('Zaman (s)')
plt.ylabel('Şebeke Yükü (kW)')
plt.title('Şebeke Yükünün Zamanla Değişimi (Saldırı Etkisi)')
plt.legend(loc='best')
plt.grid(True)
plt.tight_layout()
plt.savefig('v2g_attack_sim.png')  # grafik çıktısını kaydet
```

Yukarıdaki kod çalıştırıldığında `v2g_attack_sim.png` adlı grafik dosyası oluşturularak simülasyonun görsel çıktısı elde edilmiştir. Simülasyonda **T=0–59 saniyeler arası** saldırı öncesi denge durumu, **T=60 saniye** itibarıyla saldırı anı ve sonrasındaki dengesiz durum hesaplanmıştır.

Not: Bu kod, senaryonun basitleştirilmiş bir modelini temsil etmektedir. Gerçek bir sistemde EV'lerin gücü zamanla sürekli değişkenlik gösterebilir, şarj/deşarj işlemleri anlık değil rampalı gerçekleşebilir ve şebeke geri bildirimiyle kontrol algoritmaları devreye girebilir. Ancak burada amaç, saldırının anlık etkisini net biçimde ortaya koymaktır.

Saldırı Sonrası Grafiksel Analiz (Şebeke Yükü vs Zaman)

Şekil: Saldırı senaryosunun simülasyonundan elde edilen şebeke yükü (kW) – zaman (saniye) grafiği. Kırmızı kesik çizgi, T_0 anında saldırının tetiklendiğini göstermektedir. Mavi çizgi, saldırı gerçekleşmediği durumda toplam şebeke yükünün zamanla sabit kaldığını (450 kW) gösterirken; turuncu çizgi, saldırı anında toplam yükün 450 kW'tan 600 kW'a ani yükselişini göstermektedir. Bu ~150 kW'lık yük sıçraması, küçük ölçekli bir sistem için dahi %33'lük ani artış demektir.

Yukarıdaki grafik, saldırının elektrik şebekesi yük profilini nasıl değiştirdiğini net bir şekilde göstermektedir. **Saldırı öncesi** (0–60 s aralığında), toplam şebeke yükü baz yük etrafında sabit seyredip ~**450 kW** değerindedir. Bu dönemde EV'ler şebekeye 50 kW civarında destek sağladığı için baz 500 kW yük düşmektedir. **T_0 anında (60. saniye)** saldırganın komutları devreye girer girmez grafikte turuncu renkle gösterilen **saldırı senaryosu** eğrisi keskin bir yükseliş yaparak ~**600 kW** seviyesine çıkmıştır. Yüksek güçlü şarjların eşzamanlı başlaması ve V2G desteklerinin kesilmesiyle birlikte toplam yükte **150 kW** kadar bir sıçrama gerçekleşmiştir. Buna karşılık, mavi renkle gösterilen **normal senaryoda** böyle bir saldırı olmadığı varsayımıyla yük ~**450 kW** seviyesinde kalmaya devam etmektedir.

Grafik analizinden görüldüğü üzere, saldırının tetiklenmesiyle şebekedeki yük profili aniden ve anomali oluşturacak şekilde değişmiştir. Bu büyüklükte ani bir yük artışı gerçek bir şebekede meydana gelseydi, jeneratörlerin döner yedek kapasitesi bu yükü anında karşılayamadığı takdirde şebeke frekansında düşüş gözlenmesi kaçınılmaz olurdu [5]. Nitekim benzetimimizde T_0 anından hemen sonra sistem frekansının anlık olarak düşeceği (under-frequency) ve bu durumun devam etmesi halinde otomatik yük

atma veya jeneratör koruma sistemlerinin tetiklenebileceği söylenebilir [6]. Küçük ölçekli bir simülasyonda bile gözlemlenen bu keskin trend, saldırının daha geniş ölçekte ne denli tehlikeli olabileceğine işaret etmektedir. Elde edilen veriler, V2G botnet saldırısının karakteristik bir imzasını sunar: **coğrafi olarak yayılmış çok sayıda kaynağın senkronize davranışı sonucu alışılmadık bir yük dalgalanması**. Bu imza, hem enerji operasyon merkezleri hem de siber güvenlik izleme sistemlerince tespit edilip alarm üretilmesi gereken bir durumdur.

SWOT Analizi

Aşağıda, inceleme konusu V2G sistemine yönelik botnet saldırısı senaryosunun **SWOT (GZFT) analizi** verilmektedir. Bu analiz, sistemin güçlü ve zayıf yönlerini, gelecekteki fırsatları ve karşı karşıya olduğu tehditleri özetlemektedir:

Güçlü Yönler (Strengths)	**Zayıf Yönler** (Weaknesses)
• V2G teknolojisi, EV bataryalarını **esnek bir enerji depolama** unsuru olarak kullanıp şebeke dalgalanmalarını dengeleme potansiyeline sahiptir. Örneğin, akıllı algoritmalarla EV'ler şebekeye frekans desteği verebilir, yenilenebilir kaynakların entegrasyonunu kolaylaştırabilir. • **Merkezi yönetim (CPO) ve OCPP standardı**, binlerce istasyonun birlikte uyumlu çalışmasını mümkün kılan bir **operasyonel verimlilik** sağlar. Bu sayede normal şartlarda yük yönetimi, yetkilendirme ve faturalandırma süreçleri etkin şekilde yürütülür. • EV kullanıcıları, V2G sayesinde **çift yönlü fayda** elde edebilir (hem araçlarını şarj etmek hem de gerektiğinde şebekeye enerji satmak), bu da uzun vadede elektrik piyasalarında dengeleyici bir unsur oluşturur ve elektrikli araç sahipliği maliyetlerini düşürebilir.	• **Siber güvenlik zafiyetleri** ciddi bir zayıf noktadır: Birçok istasyonda fabrika çıkışı varsayılan parolaların değiştirilmemiş olması, yamalanmamış yazılım açıkları ve zayıf kimlik doğrulama gibi IoT güvenlik sorunları saldırganların sisteme sızmasını kolaylaştırır [26] [27]. • OCPP 1.6 protokolünün **güvenlik uzantıları opsiyoneldir** ve sahada çoğu zaman tam uygulanmamıştır; iletilerin zayıf şifreleme veya kimlik kontrol mekanizmaları, saldırılara açık bir yüzey bırakır. Özellikle tek faktörlü kimlik doğrulama ile istasyon kimliğinin taklit edilebilmesi mümkün olabilmektedir [21]. • V2G ekosisteminde çok sayıda paydaş (araç sahibileri, CPO, dağıtım şirketi, vs.) ve cihaz olduğundan **karmaşık bir saldırı yüzeyi** oluşur. Bu kompleks yapı, koordinasyon eksikliği ve standartların tutarsız uygulanması halinde güvenlik risklerini artırmaktadır.

Fırsatlar (Opportunities)	**Tehditler** (Threats)
• V2G altyapısının güvenliği konusunda artan farkındalık, **gelişmiş güvenlik standartları ve sertifikasyon** fırsatını doğurur. Yeni nesil OCPP 2.0.1 protokolü, istasyon kimlik doğrulamasını zorunlu kılan güvenlik profilleri sunmaktadır [28]. Bu protokolün yaygınlaşması ve PKI tabanlı dijital sertifika kullanımının teşvik edilmesi, sistemin güvenliğini artıracaktır. • **Akıllı izleme ve anomalı tespiti** sistemlerinin geliştirilmesi önemli bir fırsattır. CPO altyapısına entegre edilecek makine öğrenimi tabanlı sistemler, binlerce istasyondan gelen verileri analiz ederek eşzamanlı ve şüpheli davranışları gerçek zamanlı saptayabilir [29]. Benzer şekilde, şebeke operatörleri de talep tarafı verilerini izleyip öngörülemeyen yük sıçramalarını siber saldırı göstergesi olarak algılayabilecek karar destek araçları geliştirebilir. • Düzenleyici kurumlar ve standart kuruluşları için fırsat: **zorunlu siber güvenlik düzenlemeleri** getirilerek EV şarj altyapısının asgari güvenlik gereksinimleri tanımlanabilir. Örneğin, her halka açık şarj istasyonunda varsayılan kimlik bilgilerinin değiştirilmesi, düzenli penetrasyon testleri ve güvenlik sertifikası şart koşulabilir. • V2G'nin doğru ve güvenli uygulanması, yenilenebilir enerjinin yaygınlaşması ile artan dengeleme ihtiyaçlarına bir çözüm sunar. Bu da enerji piyasalarında yeni **iş modelleri** (örneğin, EV filolarının sanal enerji santrali olarak katılımı) ve gelir fırsatları anlamına gelir.	• En ciddi tehdit, bu senaryonun gerçek hayatta **geniş ölçekli bir saldırı** olarak uygulanabilmesidir. Eğer bir saldırgan yeterli sayıda şarj istasyonunu ele geçirirse veya merkezi bir CPO sistemine sızarsa, koordineli şarj manipülasyonları ile bölgesel ya da ulusal elektrik kesintilerine yol açabilir [8]. Yapılan araştırmalar, EV penetrasyonunun yüksek olduğu gelecekte tek bir büyük şarj ağı operatörünün sunucusunun bile kompromize edilmesinin dev bir metropolü karanlıkta bırakmaya yetebileceğini göstermektedir [30]. • **Kamu güveninin sarsılması** riski bulunmaktadır: Böyle bir saldırı gerçekleşirse tüketicilerin elektrikli araçlara ve akıllı şebeke uygulamalarına güveni azalabilir. Bu da EV adaptasyonunu yavaşlatır ve temiz enerjiye geçişte istenmeyen bir geri adım anlamına gelir. • Finansal ve operasyonel tehditler: Dağıtım şebekesi ekipmanlarının (transformatör, hatlar vb.) ani yük değişimleriyle hasar görmesi durumunda bakım-onarım maliyetleri artacak; ayrıca enerji piyasalarında dengesizlik kaynaklı fiyat oynaklıkları oluşacaktır. CPO'lar ve enerji şirketleri hem itibar kaybı hem de maddi kayıplarla karşılaşabilir. • Siber tehdit aktörlerinin motivasyonu giderek artmaktadır. Devlet destekli gruplar veya çıkar amaçlı saldırganlar, kritik altyapıyı hedef alan bu tip saldırılara yönelebilir. EV şarj istasyonları gibi **yeni ve hızla büyüyen bir altyapı**, saldırganlar için henüz yeterince güçlendirilmemiş "yumuşak hedef" teşkil etmektedir.

Risk Değerlendirmesi ve Önleme Stratejileri

Yapılan analiz, V2G botnet kaynaklı şebeke dengesizliği riskinin ciddiyetini ortaya koymaktadır. Bu risk, **etki düzeyi** açısından son derece yüksek olup doğrudan kritik altyapı güvenliği konusuna girmektedir. Koordine bir saldırı sonucunda geniş çaplı elektrik kesintileri, ekipman hasarları ve hatta toplumsal düzenin geçici de olsa bozulması mümkün görünmektedir. **Olasılık düzeyi** günümüz için kısmen düşük olsa da (bugüne dek kamuya yansımış böyle bir saldırı gerçekleşmemiştir), hızla artan EV sayıları ve birçok şarj istasyonunda gözlenen güvenlik açığı, önlem alınmazsa bu saldırının **yakın gelecekte gerçek bir tehdit** haline gelebileceğini göstermektedir [31]. Özellikle 2030'lu yıllara gelindiğinde, tek bir şirketin işlettiği şarj ağı üzerinden dahi böyle bir saldırının büyük bir metropolün şebekesini çökertmesinin mümkün olacağı öngörülmektedir [30]. Dolayısıyla risk değerlendirmesi, **ihmal edilemez** seviyede bir riskle karşı karşıya olduğumuzu ortaya koymaktadır.

Bu riskin yönetimi için aşağıda belirtilen **önleme (proaktif) ve koruma (reaktif) stratejileri** önerilmektedir:

- **Cihaz Düzeyinde Güvenlik İyileştirmeleri:** Tüm şarj istasyonları için asgari siber hijyen önlemleri alınmalıdır. *IoT güvenliği* kapsamında, fabrika varsayılan parolalarının cihaz ilk kurulumu sırasında değiştirilmesi zorunlu hale getirilmelidir [32]. Düzenli aralıklarla güvenlik yamaları ve imzalı ürün yazılımı (firmware) güncellemeleri yayınlanıp istasyonlara uygulanmalıdır [33]. Bilinen yazılım açıkları (ör. uzaktan kod çalıştırma zaafiyetleri) derhal yamalanmalı, yamalanamayan eski cihazlar ağdan izole edilmelidir. Bu sayede saldırganların botnet oluşturmak için yararlandığı kolay açıklıklar kapatılacaktır.

- **Güçlü Kimlik Doğrulama ve İletişim Güvenliği:** OCPP iletişiminde *"güven modeli"* yeniden ele alınmalıdır. Özellikle OCPP 1.6-J sürümünde isteğe bağlı olan güvenlik katmanları, tüm işletimlerde mecburi hale getirilmelidir. Şarj istasyonu ile merkezi sunucu arasındaki haberleşme, imkan dahilinde OCPP 2.0.1'e yükseltilerek veya mevcut protokol için TLS tabanlı güvenlik profilleri aktif edilerek şifreli ve karşılıklı kimlik doğrulamalı yapılmalıdır [21] [28]. **Dijital sertifika (PKI) temelli kimlik doğrulama**, her bir istasyonun ve sunucunun karşı tarafın sahihliğini doğrulamasını sağlayacaktır [34]. Böylece ne sahte bir merkezi sunucu istasyonları kontrol edebilir, ne de sahte bir istasyon merkezi kandırabilir. Ayrıca OCPP mesajlarının bütünlüğünü sağlamak ve tekrar oynatma saldırılarını önlemek adına zaman damgası ve imza mekanizmaları kullanılmalıdır. Bu adımlar, OCPP'nin geliştiricilerce de önerilen daha güvenli bir versiyonunun fiilen uygulanması anlamına gelir [35].

- **Ağ ve Sistem Mimarisi Önlemleri (Zero Trust Yaklaşımı):** Şarj istasyonları, mümkün olduğunca **ayrılmış ağ segmentleri** üzerinden haberleşmelidir. Public internet üzerinden doğrudan CPO'ya kritik komutlar iletmek yerine, VPN veya özel APN gibi güvenli ağ çözümleri devreye alınabilir. Zero Trust prensipleri gereği, istasyonların ve istemcilerin her iletişimde yeniden kimlik doğrulaması yapması ve en az yetki prensibinin uygulanması sağlanmalıdır [34]. Ayrıca, merkezi sistemde anormal davranışları otomatik engelleyen politikalar uygulanmalıdır. Örneğin, tek bir istemci IP adresinden çok sayıda başarısız kimlik doğrulama denemesi gelirse o istemci belirli süre için bloke edilmelidir [36]. Bu tür aktif savunma mekanizmaları, brute-force ile bağlantı ele geçirme girişimlerini zorlaştıracaktır.

- **İzleme, Algılama ve Acil Durum Müdahalesi:** Hem şarj operasyonlarının merkezi yönetim katmanında, hem de elektrik dağıtım şebekesi katmanında, gerçek zamanlı **anomalı tespit sistemleri** kurulmalıdır. CPO yazılımı, coğrafi ve zamansal açıdan tutarsız toplu komutları algılayacak şekilde kural ve yapay zekâ tabanlı kontroller gerçekleştirmelidir [29]. Örneğin, aynı anda yüzlerce istasyondan gelen **eş zamanlı "deşarjı durdur" talepleri** veya benzer zaman damgasına sahip toplu işlem istekleri alarm üretecek şekilde işaretlenmelidir [29]. Bunun yanında, şebeke operatörünün SCADA/EMS sistemleri de beklenmeyen ani yük değişimlerini anlık olarak analiz ederek bunun bir siber saldırı göstergesi olup olmadığını değerlendirmelidir [37]. Bu amaçla enerji tahmin modellerine entegre çalışan bir *intrusion detection system (IDS)* yaklaşımı benimsenebilir. Saldırı tespit edildiğinde devreye girecek **acil durum müdahale prosedürleri** önceden hazırlanmalıdır. Örneğin, şebeke frekansı belirli bir eşik değerin altına düşerse CPO'ya bağlı tüm şarj istasyonlarına otomatik olarak yük atma (örn. şarjları kesme) sinyali gönderilebilir. Alternatif olarak, saldırı altındaki istasyonlar izole edilene dek şebeke tarafında koruyucu ayırıcılar açılarak ilgili bölge geçici olarak şebekeden ayrılabilir (kontrollü adacıklaştırma). Bu tip önlemler, saldırının yayılımını ve etkisini sınırlandıracaktır.

- **Komut ve Kontrol Mekanizmalarında Kısıtlama:** Bir merkezden çıkan komutların çok sayıda cihaza aynı anda uygulanması riskine karşı **rate limiting (hız sınırlama)** stratejileri

benimsenmelidir. Özellikle CPO yazılımı, “tüm istasyonlara broadcast” tarzı komutları tek bir zaman diliminde yollamamalıdır [38]. Bunun yerine, gerektiğinde bile toplu komutlar ufak rasgele gecikmeler (jitter) eklenerek dalgalar halinde gönderilebilir [38]. Bu sayede herhangi bir yanlış komut veya ele geçirilmiş bir operatör hesabı bile, tüm sistemde aynı anda etki doğuramayacak; zamana yayılmış bir etkiyle şebekenin tepkisi için mühlet tanınmış olacaktır. Benzer şekilde, bir EV’nin şarj gücündeki değişim oranlarına fiziksel sınırlamalar getirmek de yararlı olabilir (örneğin, *ramp-rate limiting* ile bir aracın çektiği gücü saniyede belirli bir kW’dan fazla artıramamak gibi). Bu tarz teknik kontroller, saldırının şok etkisini azaltacaktır.

- **Test, Eğitim ve Sürekli İyileştirme:** CPO’lar ve elektrik şirketleri düzenli aralıklarla **tatbikatlar ve penetrasyon testleri** yaparak bu senaryoyu prova etmelidir. Örneğin bir test ağında EV şarj botnet saldırısı simüle edilip algılama sistemlerinin performansı ölçülebilir. Elde edilen bulgulara göre acil durum planları güncellenmeli, personel eğitimi ile farkındalık artırılmalıdır. Üretici firmalar, şarj cihazlarını geliştirirken güvenlik açığı değerlendirmeleri yapmalı ve mümkün olduğunca *secure by design* prensiplerine uymalıdır. Son olarak, ilgili tüm paydaşlar (OEM’ler, CPO’lar, dağıtım şirketleri, regülatörler) arasında **iletişim ve iş birliği** tesis edilmesi, ortaya çıkabilecek yeni tehditlere karşı kolektif bir savunma geliştirilmesine olanak sağlayacaktır.

Sonuç olarak, 10 istasyonlu bir V2G sistemine yönelik botnet saldırısı senaryosu, geleceğin akıllı şebekelerinde ortaya çıkabilecek ciddi bir siber-fiziksel anomaliyi gözler önüne sermektedir. Akademik teknik incelemeler ve simülasyon sonuçları, bu tip saldırıların etkili önlemler alınmadığı takdirde şebeke stabilitesini bozma potansiyelini doğrulamaktadır. Güçlü bir savunma stratejisi; hem teknolojik tedbirleri (güvenlik protokolleri, izleme sistemleri) hem de organizasyonel önlemleri (eğitim, prosedürler, iş birliği) bir arada barındırmalıdır. Bu şekilde, V2G’nin sunduğu büyük fırsatlardan yararlanırken beraberinde getirdiği riskler de kabul edilebilir düzeye indirilebilir. Güvenli ve dirençli bir V2G ekosistemi inşa etmek, hem sürdürülebilir enerji hedefleri hem de ulusal kritik altyapı güvenliği açısından bir zorunluluk olarak karşımızda durmaktadır.

Kaynaklar:

1. **Literatür ve Standartlar:** V2G ve OCPP konusundaki standartlar ile güncel akademik çalışmalar incelenmiştir. Özellikle OCPP 1.6 güvenlik açıkları ve geliştirmeleri için Open Charge Alliance teknik dokümanları ve ilgili araştırmalar temel alınmıştır [18] [23].
2. **Akademik Araştırmalar:** EV şarj altyapısına yönelik siber saldırılar konusunda Acharya *vd.* (2024) tarafından sunulan *MaDEVIoT* çalışması ile Dalamagkas *vd.* (2025) çalışması senaryoya ışık tutmuştur [25] [39]. Bu çalışmalar, EV kaynaklı yük manipülasyonlarının şebeke frekansına etkilerini ve tespit yöntemlerini ele almaktadır.
3. **Senaryo Dokümanı:** Vaka analizindeki adımlar, tarafımızca hazırlanan “V2G Botnet’i ile Şebeke Dengesizliği” senaryo dokümanından alınmıştır [1] [40]. Bu dokümanda saldırı vektörleri, fiziksel DDoS etkileri ve alınacak önlemler Türkçe olarak ayrıntılı biçimde sunulmuştur.
4. **Simülasyon:** Python ile gerçekleştirilen simülasyon, belirlenen senaryo parametrelerine göre özgün olarak geliştirilmiştir. Kod içeriği ve üretilen grafik, raporda sunulmuştur. Simülasyon çıktıları, makalede belirtilen kuramsal beklentilerle tutarlılık göstermektedir (ani yük değişiminin frekans üzerindeki olumsuz etkisi vb.) [40].
5. **Güvenlik Tavsiyeleri:** OCPP güvenlik iyileştirmeleri ve IoT cihaz güvenliği konusunda SaiFlow (2025) teknik blog yazıları ve IRENA raporları gibi sektör kaynaklarından yararlanılmıştır [21] [33]. Bu kaynaklar, gerçek sistemlerdeki güvenlik zaaflarını ve önerilen savunma yöntemlerini somut örneklerle açıklamaktadır.

---

1 2 3 4 5 6 9 10 13 14 15 24 26 27 29 32 33 34 37 38 40
botnet_anomali_senaryosu.pdf
file://file_00000000fb2c7243933c88da08ed6b8a

7 17 23 35 Cyber defense in OCPP for EV charging security risks | International Journal of Information Security
https://link.springer.com/article/10.1007/s10207-025-01055-7

8 sos.asrg.io
https://sos.asrg.io/wp-content/uploads/2024/09/Lionel-R.-Saposnik_Presentation-Slides_SOS-2024-Updated.pdf

11 12 16 A simplified architecture showing a V2G system through an aggregator. | Download Scientific Diagram
https://www.researchgate.net/figure/A-simplified-architecture-showing-a-V2G-system-through-an-aggregator_fig1_262347345

18 OCPP messages: A glossary for diagnostics and troubleshooting
https://chargelab.co/blog/ocpp-messages-glossary

19 20 21 22 28 36 Hijacking EV Charge Points to Cause DoS
https://www.saiflow.com/blog/hijacking-ev-charge-points-to-cause-dos

25 30 31 MaDEVIoT: Cyberattacks on EV Charging Can Disrupt Power Grid Operation | Conference Paper | PNNL
https://www.pnnl.gov/publications/madeviot-cyberattacks-ev-charging-can-disrupt-power-grid-operation

39 Federated detection of open charge point protocol 1.6 cyberattacks
https://www.oaepublish.com/articles/ces.2025.04