# “Şarj Esnasında Deşarj Olma” Anomalisinin Teknik İncelemesi

## 1. Anomali Tanımı ve Teknik Açıklaması

“Şarj esnasında deşarj olma” anomalisi, elektrikli aracın bataryası şarj olurken eşzamanlı veya ardışık olarak **deşarj edilmesi** durumudur. Bu anormal durum, bir **V2G (Vehicle-to-Grid)** sistemi içindeki kötü niyetli müdahaleler sonucu ortaya çıkar. Normalde V2G yeteneği, araç bataryasının gerektiğinde şebekeye enerji geri verebilmesini sağlar. Ancak bu senaryoda saldırgan, şarj sürecini kesintiye uğratarak bataryadan istem dışı enerji çekmektedir. Sonuç olarak **araç şarj oluyor gibi görünse de bataryanın doluluk oranı düşer** (yani araç enerji kaybeder). Bu durum hem **batarya ömrüne** zarar verir hem de **şebeke dengelerini** bozar. Bataryanın bu şekilde plan dışı döngülere maruz kalması, kimyasal yapısına stres uygulayarak kapasite kaybına ve performans düşüşüne neden olabilir.

Bu çok katmanlı anomali senaryosunda, saldırgan birden fazla yöntemi aynı anda kullanarak hem araç tarafını hem de şebeke tarafını hedef alır. **Üç bileşenli saldırı** şu şekildedir:

- **MITM ile Akım Yönünün Tersine Çevrilmesi:** Saldırgan, iletişim hattına Man-in-the-Middle (Ortadaki Adam) saldırısı gerçekleştirerek şarj istasyonu ile araç veya istasyon ile merkezi sunucu arasındaki mesajları yakalar ve değiştirir. Bu sayede normalde **bataryaya doğru akan akım tersine çevrilir**, yani araçtan şebekeye doğru akmaya başlar. Örneğin, saldırgan sahte ölçüm veya kontrol sinyalleri göndererek şarj cihazının sanki araç şebekeye enerji verecekmiş gibi davranmasını sağlar. Bu fiziksel düzeyde, **bataryanın deşarj edilerek şebekeye güç beslemesi anlamına gelir.**

- **Sahte OCPP Komutları ile İstenmeyen Enerji Gönderimi:** Saldırgan, EV şarj istasyonu ile yönetim sistemi arasındaki **OCPP protokolü** trafiğine müdahale eder. Burada merkezi sunucu (CPO/CSMS) ya da istasyon rolünü taklit ederek sahte komutlar enjekte eder. Bu komutlar, istasyona araçtan şebekeye enerji vermesini söyleyen **yetkisiz “deşarj” talimatları** olabilir. Örneğin saldırgan, OCPP üzerinden bir **RemoteStartTransaction** veya **SetChargingProfile** mesajını değiştirerek istasyonun maksimum gücü negatif yönde (şebekeye doğru) uygulamasını emredebilir. Meşru durumda OCPP, uzaktan başlat/durdur gibi komutlarla şarj işlemlerini kontrol edebilir. Ancak zayıf güvenlikli bir sistemde saldırgan bu kabiliyeti suistimal ederek araca haber vermeksizin **ters yönde enerji akışı başlatır.**

- **Yetkisiz V2G Deşarj Emirlerinin İletilmesi:** Saldırgan, V2G özelliklerini istismar ederek araca veya şarj ünitesine doğrudan deşarj komutu verir. Bu, ya aracın bağlı olduğu akıllı şebeke yönetim sistemine sızarak ya da araç-şarj istasyonu haberleşmesini (örneğin ISO 15118 protokolü) manipüle ederek yapılabilir. Amaç, **kullanıcının izni ve kontrolü dışında** aracın bataryasını şebekeye boşaltmaktır. Sonuçta araç sahibi, aracını şarj ettiğini düşünürken aslında enerji kaybederek bataryasının beklenenden daha **düşük bir SOC** ile kalmasına maruz kalır.

Bu anomali senaryosu teknik açıdan hem **siber** hem **fiziksel** boyuta sahiptir. Saldırı, iletişim protokollerine yönelik olsa da etkileri elektriksel düzlemde görülür. Batarya kontrol sistemleri ve güç elektroniği aniden ters yönde çalışmaya zorlandığı için **donanım seviyesinde de riskler** oluşur (ör. aşırı ısınma, hücre dengesizlikleri). Ayrıca bu istenmeyen deşarj, şebekeye planlanmamış bir güç akışı yaratacağı için **şebeke tarafında gerilim/frekans dalgalanmaları** meydana gelebilir.

Özetle, “şarj esnasında deşarj” anomalisinin teknik karakteristiği, **şarj işlemi maskesi altında gerçekleşen gizli bir enerji boşaltımı olmasıdır.** Aşağıdaki bölümlerde bu senaryonun nasıl mümkün kılındığı, hangi açıklardan faydalandığı ve sonuçlarının neler olduğu detaylı olarak ele alınacaktır.

## 2. Saldırıların OCPP Protokolü Üzerindeki İşleyişi

**Open Charge Point Protocol (OCPP)**, şarj istasyonları ile merkezi yönetim sistemleri arasındaki iletişimi sağlayan standart protokoldür. OCPP ile istasyonların uzaktan kontrolü (ör. şarj başlatma/durdurma), durum izleme, akıllı şarj profilleri ve hatta V2G enerji geri beslemesi gibi işlemler yapılabilir. Bu zengin komut seti maalesef ki saldırganlar tarafından suistimal edilebilir durumdadır, özellikle protokolün eski sürümleri ve güvenlik özelliği etkin olmayan kurulumlarda.

**Saldırı vektörü:** Saldırgan, OCPP trafiğine bir MitM (Makine-arası Ortadaki Adam) saldırısı düzenleyerek araya girer ve mesajları değiştirir veya yenilerini enjekte eder. OCPP 1.6 gibi eski sürümlerde, iletişim çoğunlukla WebSocket üzerinden şifrelenmemiş şekilde yapılır ve kimlik doğrulama zayıftır. Bu durum, saldırganın istasyon ile sunucu arasındaki mesajları kolaylıkla okuyup değiştirebilmesine olanak tanır. Örneğin, literatürde saldırganların **şifrelenmemiş WebSocket iletişimini keserek** şarj oturumlarını sonlandırdığı, uzaktan kod çalıştırdığı ve şarj cihazlarına kötü amaçlı firmware yüklediği gösterilmiştir. Özellikle TLS yapılandırmasındaki zafiyetler MitM’i kolaylaştırır; yanlış sertifika doğrulama veya TLS kullanılmaması sonucunda saldırgan, iletim halindeki veriyi yakalayıp değiştirerek komutların içeriğini manipüle edebilir.

**Sahte komutların enjekte edilmesi:** OCPP protokolünde merkezi sistemin istasyona gönderebildiği çeşitli komutlar vardır. Bunlara örnek olarak **RemoteStartTransaction** (uzaktan yeni bir şarj/deşarj oturumu başlatma) ve **RemoteStopTransaction** (devam eden oturumu durdurma) komutları verilebilir. Saldırgan, MitM pozisyonunda bu komutları taklit ederek istasyona yanıltıcı talimatlar gönderir. Örneğin:

- Saldırgan, tüm mesajları okuyabildiği için bir **RemoteStartTransaction** isteğini yakalayıp içeriğini değiştirir. Normalde araçtan şarj çekmek için gelen komutu “aracın şebekeye güç vermesi” şeklinde değiştirebilir. İstasyona, sözde merkezi sistemden geliyormuş gibi, aracı belirli bir güçte **deşarj etmesini emreden** bir komut ulaşır. İstasyon da güven ilişkisi gereği bu komutu uygular. Bu yöntem, **akım yönünün tersine çevrilmesine** yol açar.

- Benzer şekilde saldırgan, merkezi yazılımdan geliyormuş gibi bir **SetChargingProfile** mesajı gönderip, şarj akım limitini negatif bir değere ayarlayabilir (OCPP 2.0’de çift yönlü akım değerleri tanımlanabilmektedir). Böylece istasyon, bu profile uyarak bataryadan grid’e doğru enerji akışı başlatır.

- OCPP üzerindeki diğer kritik bir komut da **ChangeConfiguration** veya özel **DataTransfer** komutlarıdır. Saldırgan istasyonun konfigürasyon parametrelerini değiştirerek V2G modunu izinsiz aktif hale getirebilir ya da istasyon yazılımındaki arka kapıları tetikleyebilir. Örneğin OCPP ile pilin maksimum deşarj kapasitesine dair bir parametre değiştirilip daha yüksek akım çekilmesi sağlanabilir.

**Gerçekleşen anomali akışı:** Söz konusu saldırı ile **arka planda bir "ters şarj" oturumu** işletilmektedir. İstasyon, kullanıcının normal şarj talebini almıştır; araç fişe takılıdır ve kullanıcı arayüzünde her şey normal gözükür. Saldırgan ise OCPP üzerinden **eşzamanlı ikinci bir komut kanalı** yaratır. Bu sahte kanal üzerinden araç-şebeke arasındaki güç akışını kullanıcıdan habersiz kontrol eder. OCPP'nin **kimlik doğrulama eksikliği** ve bir istasyondan gelen birden fazla bağlantıya karşı yetersiz kontrol mekanizmaları, saldırganın bu işlemleri yapabilmesini kolaylaştırır.

Sonuç olarak OCPP üzerinde gerçekleştirilen bu saldırılar, **kullanıcıyı aldatıp** şarj işleminin normal seyrinde gittiği izlenimini verirken arka planda aracın bataryasını boşaltır. Bu durum bir çeşit **"şarj reddi" (Denial-of-Charging)** ve aynı zamanda **enerji hırsızlığı** olarak değerlendirilebilir. Saldırgan, araç ve istasyon arasındaki mesajları değiştirerek şarj akısını artırıp azaltabilmiş, hatta tamamen durdurabilmiştir. Bu tür bir kontrol, eğer çift yönlü şarj destekleniyorsa, **şarj yerine deşarj yaptırmakta** da kullanılabilir. Ayrıca aynı çalışma, birden fazla noktadaki senkron saldırıların halinde **geniş ölçekli elektrik şebekesi riskleri** oluşturacağını, grid kararlılığını tehdit edeceğini vurgulamaktadır.

**OCPP 2.0 ve güvenlik önlemleri:** Yeni sürüm OCPP 2.0, bu tür saldırıları zorlaştırmak amacıyla çeşitli güvenlik profilleri sunar. Örneğin, **Güvenlik Profili 3** ile karşılıklı kimlik doğrulama ve sertifikalarla uçtan uca şifreleme uygulanır. Ayrıca sertifika yönetimiyle hem istasyonun hem de sunucunun kimliğinin doğrulanması ve sahte cihazların ağa sızmasının engellenmesi hedeflenir. Ne var ki OCPP 2.0, eski 1.x sürümleriyle geriye dönük uyumlu değildir ve mevcut istasyonların firmware güncellemesini gerektirir. Birçok işletme henüz 2.0'a geçiş yapmadığından, protokol seviyesinde güvenlik açıkları pratikte devam etmektedir. Bu nedenle, geçici çözüm olarak OCPP 1.6 kullanan sistemlerde **VPN/SSH tünelleme, TLS 1.2+ zorunluluğu** gibi ek güvenlik katmanları uygulanması önerilmektedir.

## 3. V2G Mimarisindeki Güvenlik Açıkları

Bir V2G sistemi, elektrikli araç, şarj istasyonu, merkezi yönetim yazılımı ve elektrik şebekesi gibi birden çok bileşenden oluşan karmaşık **bir siber-fiziksel sistem**dir. Bu mimaride güvenlik zafiyetleri farklı katmanlarda ortaya çıkabilir:

- **İletişim Protokolü Açıkları:** Yukarıda detaylandırılan OCPP protokolü zayıflıkları bunun başında gelir. OCPP dışında, araç ile istasyon arasındaki haberleşme protokolleri (ISO 15118, CHAdeMO, CCS gibi) de hedef olabilir. Örneğin ISO 15118'de araç ve istasyon kimlik doğrulaması için sertifikalar öngörülmüştür, ancak uygulamada tüm istasyonların güncel sertifika kontrolü yapmaması riski vardır. Eğer saldırgan araç-istasyon haberleşmesine girebilirse (ör. PLC kanalı üzerinden**)**, **sahte şarj limiti, sahte izin** gibi mesajlarla aracı aldatabilir. AC şarjda PWM sinyaliyle verilen maksimum akım bilgisini manipüle etmek dahi mümkündür – bu, aracın istemeden daha fazla akım vermesine (ya da çekmesine) yol açabilir.

- **Kimlik Doğrulama ve Yetkilendirme Eksikleri:** V2G senaryosunda bir aracın şebekeye güç verebilmesi için normalde kullanıcının onayı ve bir üst kuruluşun (ör. enerji şirketi veya CPO) izni gereklidir. Fakat pratikte, birçok sistem bu süreci otomatikleştirmiş ve güvenliği sadece backend'e bırakmıştır. Eğer kullanıcı kimliği veya cihaz sertifikası çalınırsa, **saldırgan kendi aracını veya sahte bir aracı sisteme dahil ederek** V2G komutları gönderebilir. OCPP 1.6'da istasyon tarafında genelde yalnızca sabit kimlikler (Station ID) ve basit şifreleme kullanıldığı

için, bir saldırgan yetkisiz bir şarj noktası gibi davranarak merkezi sisteme bağlanabilir. Bu da ona sistemde komut yürütme imkanı tanır.

- **Güvenilmeyen Yazılım ve Donanım:** Şarj istasyonlarının birçoğu IoT mantığında çalışır, yani uzaktan güncellenebilir bir firmware'e sahiptir. Eğer istasyon yazılımı güncel değilse ve bilinen açıklar (ör. uzaktan kod çalıştırma zafiyeti) içeriyorsa, saldırgan bu açıklardan faydalanarak **istasyonun tam kontrolünü** ele geçirebilir. Böyle bir durumda OCPP güvenli olsa bile, istasyon içerden kompromize olduğundan yanlış işlemler yapabilir (ör. kendi başına V2G deşarja geçebilir).

- **Şebeke Entegrasyonu Açıkları:** V2G'nin amacı araçların şebekeye entegre olup gerektiğinde destek sağlamasıdır. Ancak bu entegrasyon çift yönlü akım demektir, dolayısıyla şebeke tarafında da kontrol mekanizmaları olmalıdır. Eğer dağıtım şebekesi veya enerji yönetim sistemi, istasyonlardan gelen beklenmedik güç akışlarına karşı hazırlıklı değilse, bir saldırgan bu durumu kullanabilir. Örneğin, bir bölgede 10 aracın aynı anda aniden şebekeye güç basması normalde düşük bir ihtimaldir. Yönetim sistemi bu tür anormal bir durumu algılayıp engellemiyorsa, **saldırı siber-fiziksel etkiyi büyüterek** lokal bir enerji taşıma problemine yol açar. Bu noktada akıllı şebeke altyapısının anomalileri tanıyacak şekilde izleme yapması kritik bir savunma unsurudur.

**Örnek Açıkların Birleşimi:** Mevcut senaryomuzdaki çok katmanlı saldırı, yukarıdaki açıkların birkaçı aynı anda kullanılarak mümkün hale gelmiştir. İletişim kanalındaki zafiyet (şifrelenmemiş OCPP), kimlik doğrulama eksikliği (istasyonun sahte komutları ayırt edememesi) ve cihaz güvenliği açığı (istasyon yazılımının manipüle edilebilmesi) birleştiğinde, saldırgan **hem protokol seviyesinde hem cihaz seviyesinde** sistemi kandırabilir. Saldırgan bir yandan OCPP mesajlarını değiştirip yanlış yönlendirme yaparken, diğer yandan belki de istasyon içindeki yazılıma enjekte ettiği bir zararlı kodla istasyonun **ölçüm değerlerini yanıltıcı** göndermesini sağlar (örneğin araçtan çekilen akımı düşük raporlayarak merkezi sistemin durumu fark etmesini engellemek gibi). Bu sayede **çok katmanlı gizlilik** elde edilir: Ne kullanıcı ne de merkezi sistem hemen bir terslik olduğunu anlayamaz

**V2G Özelliğinin İstismarı:** V2G mimarisinin doğası gereği, enerji akışı iki yönlüdür. Bu çift yönlülük, saldırgan açısından bakıldığında normal bir sistemde yapamayacağı türden etkilere kapı açar. Örneğin sıradan bir (yalnızca şarj destekleyen) istasyonda saldırgan en fazla şarjı durdurabilir veya geciktirebilir. Fakat V2G destekli bir istasyonda, saldırgan **aktif bir eylem olarak şebekeye enerji basabilir veya enerjiyi çekebilir**. Bu, tıpkı elektrik şebekesine yönelik bir silah haline gelebilir. Nitekim bir senaryoda saldırganın binlerce V2G istasyonunu ele geçirip hepsine aynı anda **"Maksimum güçte şarj ol"** komutu verdiği düşünülürse, şebekede yapay bir talep zirvesi oluşturulabilir. Tersine, hepsine **"deşarjı durdur"** emri verilirse, şebekeye sağlanan beklenen destek aniden kesilecek ve arz düşüşü yaşanacaktır.

Bu tür koordineli saldırılar, elektrik şebekesinde frekansın tehlikeli şekilde düşmesine veya yükselmesine neden olur. Bizim incelediğimiz daha küçük ölçekli senaryoda (10 istasyon), etkiler bölgesel ve sınırlı kalsa da, temel mekanizmalar aynıdır ve büyük ölçekte uygulanabilir.

## 4. Saldırı Simülasyonu ve Modelleme (10 Şarj Noktası ile)

Bu bölümde, anlatılan çok katmanlı saldırı senaryosunun kontrollü bir ortamda **simülasyonu** gerçekleştirilmiştir. Amaç, 10 adet sanal şarj istasyonundan oluşan bir V2G sisteminde, saldırının batarya doluluk oranlarına ve akım yönlerine etkisini gözlemlemektir. Simülasyon ortamı, Python dili kullanılarak her bir şarj noktasının basitleştirilmiş davranışını modelleyecek şekilde kurulmuştur. Her sanal istasyon bir EV bataryasını temsil eder ve 1 dakikalık zaman adımlarıyla şarj/deşarj durumu güncellenir.

**Modelleme Varsayımları:**

- Her bir aracın batarya **State of Charge (SOC)** değeri 0-100% arası bir değerdir. Başlangıçta araçların SOC'ları rastgele 30-60% arasında belirlenmiştir.

- Normal koşullar altında tüm araçlar şebekeden güç çekerek şarj olmaktadır. Şarj hızı sabit olup modelde dakikada +1% SOC olacak şekilde alınmıştır (örneğin ~50 kWh bir batarya için ~10 kW'lık bir şarj gücüne denk gelebilir).

- Araç bataryası %100'e ulaştığında şarj akımı kesilir (SOC artık artmaz).

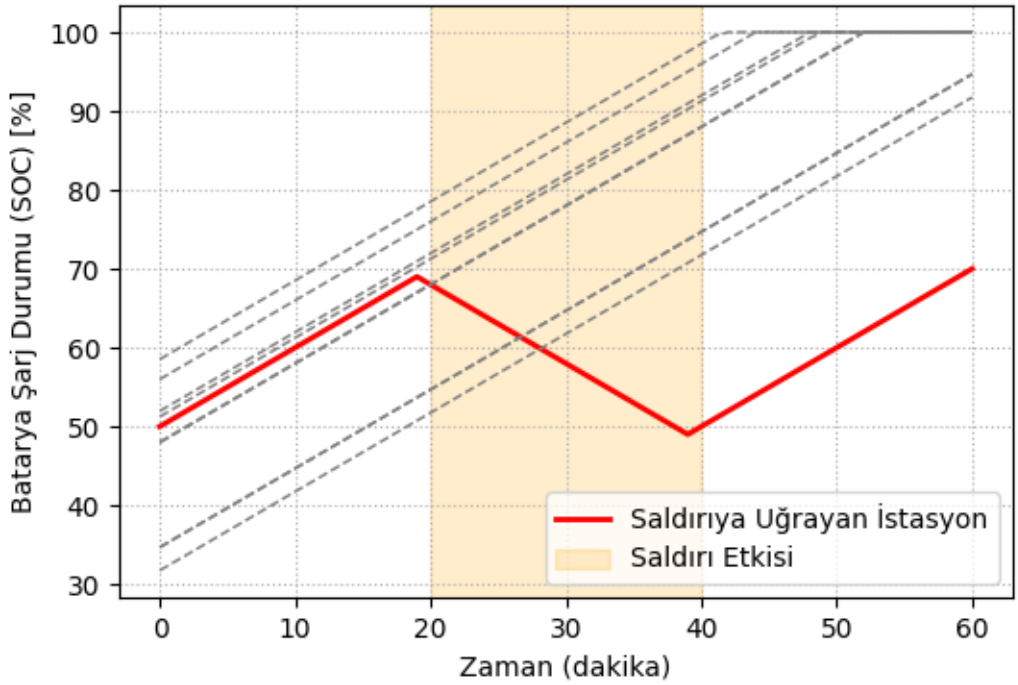
- **Saldırı senaryosu:** 0 numaralı istasyon (araç) saldırıya hedef seçilmiştir. Simülasyonda zaman t=20 dakikadan t=40 dakikaya kadar bu istasyona yukarıda tanımlanan anomalistik müdahale uygulanır. Yani 20. dakikadan 40. dakikaya dek araç **şarj yerine deşarj** moduna geçirilir. Bu, modelde bu zaman aralığında akımın +1% yerine **-1% SOC/dakika** olarak uygulanmasıyla temsil edilmiştir. 40. dakikadan sonra saldırının sona erdiği ve istasyonun normal şarja döndüğü varsayılır.

- Diğer 9 istasyon saldırıya uğramaz ve tüm süre boyunca normal şekilde şarj olmayı sürdürür.

**Kısıtlar:** Bu model gerçek sistemin basitleştirilmiş bir temsilidir. Araçların gerçek şarj/deşarj karakteristiğinde akım, SOC'ye bağlı olarak değişebilir (özellikle %80-100 civarında akım düşer). Ancak burada lineer ve sabit bir akım varsayılmıştır. Ayrıca saldırı sırasında araçtan şebekeye verilen enerji miktarının şebekede yaratacağı ani etkiler (gerilim/frekans) modellenmemiş, yalnızca her bir aracın bireysel SOC değişimleri incelenmiştir. Yine de model, anomalinin temel etkilerini net biçimde ortaya koymaktadır.

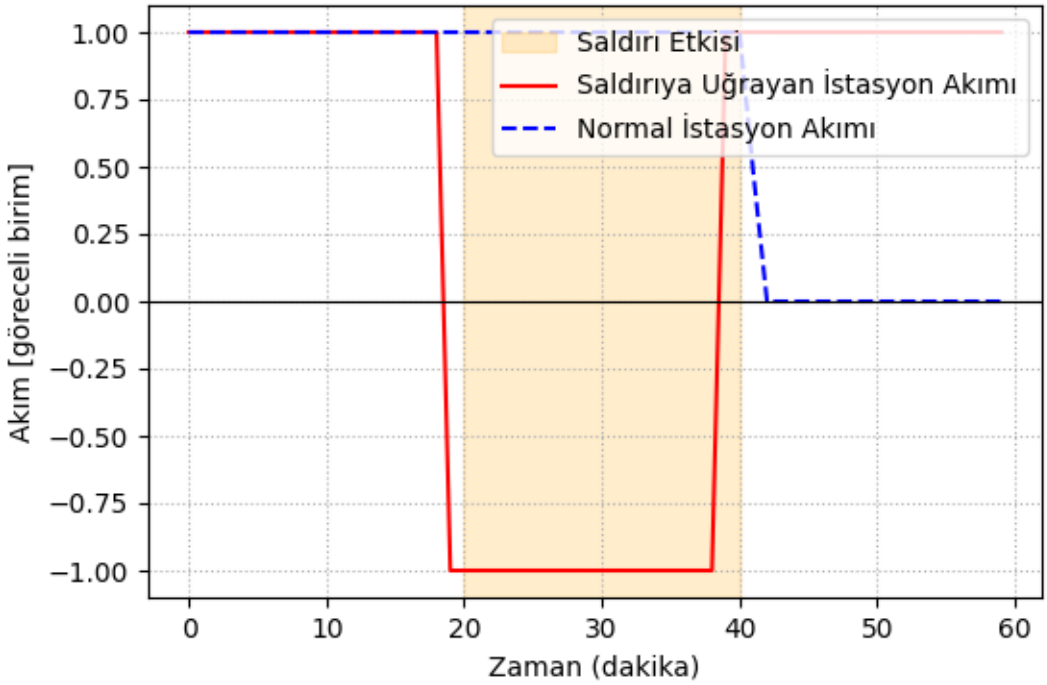
## 5. Batarya SOC Dalgalanması ve Akım Yönü Analizi

Simülasyon sonuçları, beklenildiği üzere saldırıya uğrayan araç ile diğerleri arasında belirgin bir farklılık olduğunu göstermektedir. Aşağıdaki grafiklerde**, batarya SOC değişimleri** ve **akım yönü zaman serileri** verilmiştir:




*Şekil 1: 10 istasyonlu V2G sisteminde zaman içinde batarya SOC değerleri. Kırmızı çizgi saldırıya uğrayan aracı göstermektedir. Saldırı süresince (%20–40 dk arası, turuncu taralı bölge) bu aracın SOC değerinin azaldığı (deşarj) görülüyor. Diğer gri çizgiler, normal şartlarda sürekli artan SOC'ye sahip araçlardır.*

Şekil 1'de, **saldırı etkisiyle kırmızı SOC eğrisinin düşüşe geçtiği** açıkça görülmektedir. 20. dakikaya kadar diğer araçlarla benzer biçimde yükselen kırmızı çizgi, saldırı başladıktan sonra tersine dönmekte ve ~%68 seviyesinden ~%50 seviyesine kadar gerilemektedir. 40. dakikada saldırı sona erdiğinde SOC tekrar artmaya devam etmektedir. Diğer hiçbir araçta böyle bir düşüş gözlenmez; hepsi muntazam bir şekilde (neredeyse lineer) artış göstermektedir. Bu, "şarj esnasında deşarj" anomalisinin sayısal bir göstergesidir: **Bir araç dışarıdan enerji alması gerekirken enerji kaybetmiştir.** 60. dakikada saldırıya uğramış aracın SOC'si başlangıca göre yalnızca %20 artarken, aynı başlangıç seviyesine sahip normal bir aracın SOC'si %50 artarak tam doluluğa ulaşmıştır. Aradaki %30'luk fark, saldırı süresince şebekeye gönderilen enerji miktarıyla ilişkilidir (araç %30'luk bir şarj enerjisini kaybetmiştir).




*Şekil 2: Saldırıya uğrayan ve normal bir istasyon için akım yönü ve şiddeti. Pozitif değerler şebekeden araca şarj akımını, negatif değerler araçtan şebekeye deşarj akımını temsil eder. Saldırı etkisiyle 20–40 dk aralığında kırmızı çizginin -1 birim seviyesinde olduğu (araçtan şebekeye sürekli güç aktığı) görülmektedir. Mavi kesikli çizgi normal istasyon akımıdır (saldırı yok, daima pozitif veya batarya dolunca 0). Turuncu gölgeli alan saldırı süresini belirtir.*

Şekil 2'de akım profilleri karşılaştırılmıştır. **Kırmızı çizgi**, saldırıya uğrayan araçtaki akımı göstermektedir. Saldırı yokken (0–20dk ve 40–60dk arası) bu akım +1 birimlik sabit şarj akımıdır. Ancak saldırı başladığında çizgi 1 birimden -1 birime keskin bir geçiş yapmıştır. Bu, akım yönünün anlık olarak tersine döndüğünü gösterir. 20–40 dakikalar arasında kırmızı çizgi -1 birim seviyesinde sabit kalarak aracın kesintisiz olarak deşarj edildiğini (sabit güçle şebekeye enerji aktardığını) işaret etmektedir. 40. dakikadan sonra akım tekrar pozitif değere dönerek normal şarja geçilmiştir. **Mavi kesikli çizgi** ise aynı koşullarda saldırıya uğramayan bir araca ait akımı gösterir. Bu araç 0–50dk arası +1 birim sabit akımla şarj olmuş, 50. dakikada batarya tam dolduğu için akımı 0'a düşmüştür. Hiçbir anında negatif (deşarj) bölgeye geçmemiştir. Bu karşılaştırma, saldırının varlığında akım yönünün nasıl anormal şekilde değiştiğini netleştirir. Pozitif akımın negatif olması demek, beklenen güç akışının tersine çevrilmesi ve **aracın istem dışı enerji kaybetmesi** demektir. Bu durum elektriksel ölçüm sistemlerinde, enerji sayaçlarında da anormal kayıtlar oluşturacaktır (örneğin, aracın bağlı olduğu noktada enerji çekişi yerine enerji beslemesi kaydedilecektir).

Grafikler ayrıca saldırının zamanlamasının önemini vurgular: Belirli bir süre için uygulanan ters akım, kullanıcı farkına varmadan aracın hedefine ulaşmasını (tam şarj olmasını) engellemiştir. Gerçek bir senaryoda kullanıcı aracını %80 dolu bırakmayı planlarken %60 dolu bulabilir veya şebekeye geri satılmaması gereken bir enerji miktarı satılmış olabilir. Bu bulgular, çok katmanlı saldırının pratik sonuçlarını göz önüne sermektedir.

## 6. Riskler ve Önerilen Savunma Yöntemleri

Yukarıdaki analizler ışığında, "şarj esnasında deşarj" anomalisinin ortaya çıkardığı temel riskler ve bunlara karşı alınabilecek savunma önlemleri aşağıda maddeler halinde özetlenmiştir:

**Başlıca Riskler:**

- **Batarya Hasarı ve Ömür Kısalması:** İstenmeyen deşarj döngüsü, bataryanın üretici tavsiyesi dışında bir döngüye maruz kalmasına yol açar. Bu da hücrelerde **kimyasal stres** ve ekstra yıpranma oluşturur. Sürekli tekrarlanırsa batarya kapasitesi hızla düşebilir ve kullanım ömrü kısalır.
- **Finansal Kayıp ve Enerji Hırsızlığı:** Kullanıcı, şarj için ödeme yaparken aslında enerji kaybettiği için çifte kayıp yaşar. Hem hedeflediği şarjı alamaz, hem de belki de şebekeye verdiği enerjinin bedelini alamaz. Saldırgan bu enerjiyi kendi çıkarına kullanabilir (ör. piyasaya satabilir). Bu durum kullanıcı için maddi zarardır.
- **Şebeke Dengesizliği ve Fiziksel Hasar:** Koordine veya yoğun olduğu takdirde bu saldırılar yerel şebeke dengelerini bozarak trafolarda aşırı yüklenmeye veya beklenmedik yük değişimlerine yol açabilir. Ani ve toplu deşarjlar, güç kalitesini düşürüp koruma sistemlerini tetikleyebilir; trafoların veya hatların zarar görmesi mümkündür.
- **Hizmet Reddine (DoS) Neden Olma:** Bir kullanıcı açısından bakıldığında, bu saldırı bir **Hizmet Reddi (DoS)** saldırısıdır – kullanıcı şarj hizmetinden mahrum kalır. Bir bölgedeki birçok kullanıcı aynı anda etkilenirse, şarj altyapısına güven azalır ve belki de acil durumlarda araçların kullanılamaması gibi kritik sonuçlar doğar.
- **Veri ve Gizlilik İhlali:** MITM saldırısıyla iletilen OCPP verileri ele geçirilirken, kullanıcı kimlikleri, kredi kartı bilgileri, konum verileri gibi hassas bilgiler de çalınabilir. Bu da ayrı bir siber risk (gizlilik ihlali) oluşturur.
- **İtibar ve Yasal Riskler:** Şarj ağı işletmecileri (CPO'lar) için böyle bir olay ciddi itibar kaybına yol açar. Kullanıcılar güveni sarsıldığı için farklı sağlayıcılara yönelebilir. Ayrıca yasal olarak, sağlanamayan hizmet veya uğranılan zararlar nedeniyle tazminat davaları gündeme gelebilir.

**Önerilen Savunma Yöntemleri:**

- **Güvenli İletişim ve Protokol Güncellemeleri:** Tüm şarj istasyonları ile merkezi sistem arasındaki trafiğin şifreli ve kimlik doğrulamalı olması sağlanmalıdır. Bu amaçla **OCPP 2.0.1**'e geçiş kritik bir adımdır; zira bu sürüm mutual TLS ve sertifika yönetimi gibi özelliklerle donatılmıştır. Geçiş sürecinde hemen mümkün değilse, **VPN tünelleri veya TLS eklemeleriyle** OCPP 1.6 oturumları güvenceye alınmalıdır. İstasyon ve merkezi sunucu, birbirini sertifika ile tanımalı, aksi halde iletişime izin vermemelidir. Böylece MITM saldırıları büyük ölçüde önlenebilir.
- **Cihaz Güvenliği ve Erişim Kontrolleri:** Şarj istasyonlarının firmware'leri düzenli olarak güncellenmeli **ve güvenlik açıkları kapatılmalıdır**. Özellikle bilinen RCE (uzaktan kod çalıştırma) veya yetkisiz erişim zafiyetleri üretici tarafından yamalanmalıdır. Tüm istasyonlarda **güçlü parolalar ve çok faktörlü kimlik doğrulama** kullanılmalı; varsayılan giriş bilgilerinin kalması engellenmelidir. İstasyonlar, sadece yetkili IP adresleri veya VPN üzerinden erişime izin verecek şekilde ağda izole edilmelidir (public internet'e doğrudan açık olmamalıdır). Ayrıca istasyon seviyesinde **yerleşik güvenlik modülleri** (TPM vb.) kullanılarak cihaz kimliği korunabilir ve sahte cihazların ağa girmesi önlenebilir.

- **İzleme ve Anomali Tespiti:** Hem şarj ağı operatörü hem de elektrik dağıtım şirketi, **gerçek zamanlı izleme sistemleri** kurmalıdır. Merkezi yazılım, tüm bağlı istasyonlardan gelen verileri analiz ederek anormal durumları bayraklamalıdır. Örneğin, normalde bir şarj oturumunda akım hep pozitif olmalıdır; herhangi bir istasyondan negatif akım (deşarj) değerleri raporlanırsa bu **alarma** dönüştürülmelidir. Benzer şekilde, coğrafi olarak yakındaki istasyonlardan eş zamanlı gelen sıra dışı talepler (hepsinin aynı anda deşarja geçmesi gibi) anında tespit edilmelidir. Bu amaçla yapay zeka ve makine öğrenimi algoritmaları kullanılabilir. Şebeke operatörü de, **şebeke üzerinde** beklenmedik güç dalgalanmalarını siber saldırı belirtisi olarak yorumlayıp ilgili istasyonları izole edecek sistemler geliştirmelidir. Örneğin, frekans anormalliği tespit edildiğinde belli bölgelerin V2G işlemleri otomatik kısıtlanabilir.
- **Kullanıcı Taraflı Önlemler:** EV kullanıcıları için mobil uygulamalar veya araç içi sistemler, **şarj durumu hakkında detaylı telemetri** sunabilir. Örneğin, "anlık şarj gücü" göstergesi negatif bir değer gösterirse kullanıcı hemen müdahale edebilir. Kullanıcının haberi olmadan bataryadan enerji veriliyorsa araç bir uyarı üretebilir (BMS yazılımına böyle bir kontrol eklenebilir). Ayrıca kullanıcılar, **şarj oturum özetlerini** (çekilen/verilen kWh, süre, vb.) kontrol ederek anomali olup olmadığını takip edebilir. Bu farkındalık, saldırının erken raporlanmasına yardımcı olur.
- **V2G İşlem Onayı ve Limitleri:** V2G deşarjının kötüye kullanılmasını önlemek için, **ek onay mekanizmaları** getirilebilir. Örneğin, araç sahibi mobil uygulamasından her deşarj işlemi için onay vermedikçe araçtan şebekeye enerji akışı başlamayabilir. Ya da deşarj sadece belli güvenilir senaryolarda (talep yanıt programları, acil durumlar) otomatik yapılır, onun dışında kullanıcının "araçtan güç vermeye izin ver" ayarını açık bırakması gerekir. Bu tür kullanıcı kontrollü politikalar, saldırgan protokolü kandırsa bile araca kadar etki etmesini önleyebilir. Ayrıca **deşarj hızına ve miktarına limitler** konulabilir; örneğin bir oturumda araç en fazla %10 kapasitesini verebilir, daha fazlası insan onayı gerektirir. Bu limitler anomali durumunda zararları sınırlamaya yardım eder.
- **Hukuki ve Standartlaştırma Adımları:** Son savunma katmanı olarak, düzenleyici kuruluşlar bu alanda **standartlar ve yaptırımlar** uygulamalıdır. Örneğin, yeni kurulacak tüm halka açık şarj istasyonlarında OCPP güvenlik sertifikasyonu zorunlu kılınabilir. Cihaz üreticileri için **IEC 61850 veya ISO 27000** serisi uyumluluklar talep edilebilir. Bir saldırı gerçekleştiğinde sorumluluk ve sigorta prosedürleri belirlenerek, kullanıcıların zararlarının tazmini güvence altına alınmalıdır. Bu, sektörde güvenlik bilincini artıracak ve saldırganlar için caydırıcı olacaktır.

**Alınacak önlemler çok katmanlı olmalıdır: Siber güvenlik, cihaz güvenliği ve operasyonel güvenlik** birlikte ele alınmalıdır. Örneğin, sadece protokolü şifrelemek yetmez; cihazın kendisi ele geçirilmişse içerden saldırı yapabilir. Bu yüzden yukarıdaki savunma yöntemleri birbirini tamamlayacak şekilde uygulanmalıdır. Bunlar hayata geçirildiği takdirde, "şarj esnasında deşarj" gibi anomalilerin gerçekleşme ihtimali büyük ölçüde azaltılacak, gerçekleşse bile erken tespit ile zararı minimumda tutulabilecektir.

## 7. SWOT Analizi

Bu bölümde "şarj esnasında deşarj olma" anomalisinin ve genel olarak V2G sisteminin bu tür saldırılara karşı durumunu **SWOT (Strengths, Weaknesses, Opportunities, Threats)** perspektifinde değerlendireceğiz:

- **Güçlü Yönler:** V2G sisteminin temel güçlü yanı, **çift yönlü enerji yönetimi** sayesinde elektrik şebekesine esneklik ve destek sağlayabilmesidir. Doğru uygulandığında, araç bataryaları pik talepleri dengeleyebilir ve kullanıcılar da bu hizmetten kazanç elde edebilir. Ayrıca OCPP 2.0 gibi yeni protokol sürümleri, güvenlik için **gelişmiş özellikler** (TLS şifreleme, sertifika tabanlı kimlik doğrulama vb.) sunarak bu tür saldırıların önüne geçmeyi hedeflemektedir. Sistem tasarımında rol tabanlı erişim kontrolleri, izleme mekanizmaları gibi güvenlik önlemleri teorik olarak mevcuttur. Yani, standartlar seviyesinde bakıldığında savunma imkanları tanımlanmıştır. Bir diğer güçlü yön, bu anomaliyi tespit etmenin tamamen imkansız olmaması; zira **akım yönü, enerji sayaçları ve SOC telemetrisi** izlenerek anomali sinyalleri yakalanabilir (örneğin, şarj oturumu sırasında beklenmedik negatif güç akışı tespiti). Kısacası, sistem doğru yapılandırıldığında hem enerji hem de siber güvenlik açısından avantajlar sunabilir.

- **Zayıf Yönler:** Mevcut uygulanışta en büyük zayıflık, **güvenlik protokollerinin ihmal edilmesi veya eski sürümlerin yaygın olmasıdır.** Birçok sahadaki şarj istasyonu halen OCPP 1.6 veya hatta 1.5 kullanmakta ve iletişimleri şifrelenmemiş kanallar üzerinden gerçekleşmektedir. Bu da onları MitM ve sahte komut saldırılarına açık kılar. İkinci önemli zayıflık**, kimlik doğrulama eksiklikleri** ve cihazların siber dayanıklılığının düşük oluşudur. Varsayılan şifreler, güncellenmemiş firmware'ler, güvenlik duvarı olmayan ağlar gibi zaaflar, saldırganların içeri sızmasını kolaylaştırır**. Teknoloji entegrasyonunun karmaşıklığı**, yani aracın, istasyonun, sunucunun ve şebekenin birçok standartla haberleşmesi de zayıflık yaratır; en zayıf halka kadar güvenlik sağlanabilir. Şu an için araç-şebeke etkileşimlerinde ortak bir güvenlik standardı bulunmaması, sorumluluk karmaşası doğurur (araç üreticisi mi istasyon operatörü mü sorumlu belirsiz kalabilir). Bu belirsizlikler, saldırıların fark edilmeden kalmasına yol açabilir. Ayrıca tipik bir son kullanıcı, şarj esnasında aracının aslında deşarj olduğunu **anlık olarak anlayamaz**; bu kullanım tarafındaki bir zayıflıktır (insan faktörü). Tüm bunlar, sistemin saldırılara karşı savunmasız noktalarını oluşturur.

- **Fırsatlar:** Bu anomali vakası, **güvenlik iyileştirmeleri** için önemli fırsatlar yaratmaktadır. Öncelikle, sektör genelinde **OCPP 2.0.1'e geçişin hızlanması** bir fırsattır – yeni protokolün sunduğu gelişmiş güvenlik benimsenerek eski açıklar kapatılabilir. İkinci fırsat**, ISO 15118 ve benzeri standartların tam uygulanmasıdır**; böylece araç-şarj iletişiminde sertifikalı ve şifreli yapı sayesinde MitM saldırıları zorlaşacaktır**. Makine öğrenimi tabanlı izleme ve anomali tespit sistemleri** geliştirmek de bir fırsattır. Örneğin merkezi sistem, normalde istatistiksel olarak beklenmeyen kalıpları (birden çok araçtan aynı anda gelen anormal deşarj gibi) yakalayan algoritmalar kullanabilir. Bu yalnızca güvenliği artırmakla kalmaz, enerji yönetimini de optimize edebilir. Ayrıca düzenleyici kurumlar, **standartlar ve sertifikasyon** yoluyla tüm EVSE (şarj ekipmanı) üreticilerini asgari güvenlik gereklerini karşılamaya zorunlu kılabilir – bu da sektörde fırsat penceresi açar (güvenli ürünler rekabet avantajı kazanır). Son olarak, kullanıcı farkındalığının artması da fırsattır: Eğer EV kullanıcıları bu tür risklerin farkına varırsa, **talep yönlendirmesiyle** daha güvenli hizmet sağlayıcıları ve cihazları tercih edecek, piyasayı güvenliği sağlamaya teşvik edecektir.

- **Tehditler:** Bu senaryonun ortaya koyduğu ciddi tehditler vardır. En barizi, **elektrik şebekesine yönelik fiziki hasar riski**dir. Senaryo küçük ölçekte kalsa bile, aynı yöntemle geniş bir saldırısı yapılması durumunda bölgesel hatta ulusal çapta elektrik kesintileri tetiklenebilir. Bu durum, bir **DDoS saldırısının fiziksel dünyaya yansıması** gibidir – arz-talep dengesini altüst ederek

trafo ve santralleri koruma moduna sokabilir, geniş çaplı black-out'lara neden olabilir. Bir diğer tehdit, **kullanıcı güveninin sarsılması**dır; EV sahipleri şarj altyapısına güvenmezse, elektrikli araç adaptasyonu yavaşlayabilir. Ayrıca bu tip saldırılar, finansal kayıplar ve hırsızlık tehdidi de içerir: Saldırganlar kullanıcıların elektrik enerjisini çalarak kendi çıkarına kullanabilir veya şebekeye satıp gelir elde edebilir. Bunun tespit edilmesi zor olabilir ve fatura anlaşmazlıklarına yol açabilir. **Batarya ömrü ve güvenliği** de tehdit altındadır; sık sık veya kontrolsüzce yapılan V2G döngüleri batarya sağlığına zarar verir, hatta aşırı durumlarda batarya arızalarına veya yangın riskine bile neden olabilir. Son olarak, **yasal ve düzenleyici belirsizlikler** tehdit oluşturur: Böyle bir olay gerçekleştiğinde sorumluluğun kimde olduğu (istasyon operatörü, araç sahibi, üretici vs.) net olmadığından, mağdurların zararlarının tazmini ve saldırganların cezai takibi gibi konular belirsiz kalabilir. Bu da kötü niyetli aktörlere cesaret verebilecek bir boşluktur.

## 8. Sonuç

Bu raporda, 10 şarj istasyonlu bir V2G sistemi üzerinde gerçekleştirilebilecek "şarj esnasında deşarj olma" anomalisinin teknik yönleri kapsamlı biçimde incelenmiştir. Anomali, birden çok saldırı tekniğinin birleşimiyle ortaya çıkan karmaşık bir senaryo olarak ele alınmıştır: OCPP protokolündeki güvenlik açıklardan faydalanan saldırgan, hem iletişimi manipüle edip akım yönünü tersine çevirebilmekte hem de V2G özelliklerini istismar ederek araç bataryasını habersizce boşaltabilmektedir. Bu durum, kullanıcının beklediği şarj hizmetinin aksine enerji kaybına uğramasına ve elektrik şebekesine istenmeyen yükler binmesine yol açmaktadır.

Çalışmada, söz konusu senaryo bir simülasyon ile modellenmiş ve sonuçlar görsel olarak analiz edilmiştir. Elde edilen bulgular, saldırının etkisiyle hedef araç bataryasında SOC dalgalanmaları ve düşüşler olduğunu, akım yönünün ise pozitiften negatife dramatik şekilde döndüğünü açıkça ortaya koymuştur. Bu sayede literatürde kavramsal olarak ele alınan riskler, sayısal bir örnekle somutlaştırılmıştır.

Yapılan SWOT analizi, V2G ekosisteminin bu saldırı türüne karşı mevcut durumunu değerlendirmeye yardımcı olmuş; güçlü yönler ve fırsatların yanı sıra ciddi zayıflıklar ve tehditler olduğu görülmüştür. Son bölümde ise bu anomalinin doğurduğu risklere karşı çok katmanlı savunma tedbirleri önerilmiştir. Güvenli iletişim protokollerine geçiş, cihaz güvenliğinin artırılması, anomali tespit sistemlerinin kurulması ve kullanıcı farkındalığının yükseltilmesi kilit çözüm başlıkları olarak öne çıkmaktadır. Ayrıca, düzenleyici çerçevenin güçlendirilmesi ve standartların uygulanması da uzun vadede güvenli bir V2G altyapısı için vazgeçilmezdir.

Günümüzün akıllı şebeke ve elektrikli ulaşım dünyasında, araçlar sadece enerji tüketen değil aynı zamanda enerji sağlayabilen varlıklar haline gelmiştir. Bu dönüşüm, büyük fırsatlarla birlikte yeni sorumluluklar da getirmektedir. "Şarj esnasında deşarj olma" gibi anomaliler, bu sorumlulukların ihmal edilmesi durumunda neler yaşanabileceğine dair dersler sunmaktadır. Sonuç olarak, V2G sistemlerinin güvenliği hem akademik çevrelerin hem sektör paydaşlarının yakın takibinde olmalıdır. Bu raporda ele alınan çok katmanlı saldırı senaryosu, proaktif önlemler geliştirilmezse karşılaşılabilecek riskleri gözler önüne sermiştir. Ancak aynı zamanda, alınacak doğru tedbirlerle bu risklerin yönetilebilir olduğu da vurgulanmıştır. Bu kapsamlı teknik incelemenin, gelecekte daha güvenli ve dirençli elektrikli araç şarj altyapılarının tasarlanmasına katkı sağlayacağı ümit edilmektedir.

**Kaynaklar:**


1. **Southwest Research Institute** (2020). *SwRI hacks electric vehicle charging to demonstrate cybersecurity vulnerabilities.*
2. **Dalipi**, F. et al. (2022). *EVExchange: A Relay Attack on Electric Vehicle Charging System.* arXiv:2203.05266.
3. **Roscher**, A. et al. (2022). *Brokenwire: Wireless Disruption of CCS Electric Vehicle Charging.* arXiv:2202.02104.
4. **MDPI Sensors** (2023). *Review of Electric Vehicle Charger Cybersecurity Vulnerabilities, Potential Impacts, and Defenses.*
5. **Hamdare, S**. "Cyber defense in OCPP for EV charging security risks." Int. Journal of Information Security, 24:134 (2025).
6. **Jarauta Gastelu**, J."MitM Attack to Electric Vehicle AC Chargers." (2025).
7. **Ampcontrol Tech**. "OCPP 1.6 vs. OCPP 2.0: A Comprehensive Comparison." (2024).
8. Cyber defense in OCPP for EV charging security risks | International Journal of Information Security
9. OCPP 1.6 vs. OCPP 2.0: A Comprehensive Comparison