**Konu: Elektrikli Araçlar ile Şarj İstasyonları Arasındaki Etkileşimde Ani Yük Düşürme Saldırısı (Sudden Load Shed Attack)**

**🔹 1. Giriş**

Elektrikli araçlar (EV - Electric Vehicle) günümüzde enerji ekosisteminin önemli bir parçası haline gelmiştir. Bu araçlar, **şarj istasyonları ve enerji dağıtım şebekesi** arasında çift yönlü veri alışverişi yaparak enerji akışını optimize eder. Ancak bu sistemlerin internete bağlı olması, **siber güvenlik açıklarını** da beraberinde getirir.  
Bu raporda, elektrikli araç şarj ağlarında ortaya çıkabilecek **“Ani Yük Düşürme Saldırısı (Sudden Load Shed Attack)”** incelenmiştir.

**🔹 2. Temel Kavramlar**

* **Akıllı Şebeke (Smart Grid):** Enerji üretimi, iletimi ve tüketimini dijital sistemler aracılığıyla izleyen ve yöneten akıllı enerji altyapısıdır.
* **V2G (Vehicle-to-Grid):** Elektrikli araçların hem enerji çekebildiği hem de fazla enerjiyi şebekeye geri verebildiği sistemdir.
* **Şarj Yönetim Sistemi (Charging Management System):** Şarj istasyonlarını yöneten ve komutları dağıtan merkezi yazılımdır.

**🔹 3. Ani Yük Düşürme Saldırısının Tanımı**

**Ani Yük Düşürme Saldırısı (Sudden Load Shed Attack)**, bir saldırganın aynı anda çok sayıda şarj istasyonuna **“şarjı durdur”** komutu göndererek **şebekede ani bir yük azalması (load drop)** yaratmasıdır.  
Bu saldırı, enerji dengesini bozar ve özellikle:

* Elektrik üretim sistemlerinde **ani gerilim dalgalanmalarına**,
* Şebeke kararlılığının bozulmasına,
* Şalt cihazlarının (switchgear, trafo vb.) aşırı yüklenmesine,
* Ve bazı durumlarda **bölgesel elektrik kesintilerine** yol açabilir.

**🔹 4. Saldırının Gerçekleşme Aşamaları**

1. **Keşif (Reconnaissance):**  
   Saldırgan, şarj istasyonlarının IP adreslerini, API uç noktalarını veya iletişim protokollerini keşfeder.
2. **Yetkisiz Erişim Sağlama:**  
   Zayıf kimlik doğrulama veya açıkta bırakılmış yönetici paneli üzerinden sisteme sızılır.
3. **Komut Gönderimi:**  
   Saldırgan, kontrol sunucusu gibi davranarak binlerce şarj istasyonuna “şarjı durdur” komutu yollar.
4. **Ani Yük Azalması:**  
   Aynı anda çok sayıda araç şarjı kesilir, bu da şebekede dengesizliğe neden olur.
5. **Sonuçlar:**  
   Elektrik arz-talep dengesi bozulur, sistem çökebilir veya bazı bölgelerde kesinti yaşanabilir.

**🔹 5. Olası Etkiler**

| **Etki Türü** | **Açıklama** |
| --- | --- |
| **Enerji Dengesizliği** | Ani yük değişimi, frekans dalgalanmasına ve kararsızlığa neden olur. |
| **Cihaz Hasarı** | Şebeke koruma sistemleri ani değişimlere karşı tepki veremeyebilir, cihaz arızaları yaşanabilir. |
| **Hizmet Kesintisi** | Şarj altyapısı geçici olarak devre dışı kalabilir. |
| **Kullanıcı Güveni Kaybı** | Müşteriler sistemin güvenilirliğini sorgular. |
| **Finansal Kayıp** | Hem enerji sağlayıcılar hem de kullanıcılar ekonomik zarara uğrar. |

**🔹 6. Anomali Tespiti (Detection)**

Bu tür saldırılar, normal şebeke davranışına göre **ani ve eş zamanlı yük düşüşleri**yle kendini belli eder.  
Anomali tespitinde kullanılabilecek bazı yöntemler:

* **Makine Öğrenmesi Modelleri:**
  + *Isolation Forest*, *Autoencoder*, *LSTM* gibi algoritmalarla yük düşüşlerini tespit etmek.
* **Zaman Serisi Analizi:**
  + Şarj yük profillerinde normalden sapan ani değişimleri yakalamak.
* **Korelasyon Analizi:**
  + Aynı anda çok sayıda istasyonda gerçekleşen durdurma olaylarını ilişkilendirmek.

**🔹 7. Önleme ve Güvenlik Önerileri**

* **Kimlik Doğrulama Güçlendirme:** Her şarj istasyonu ile merkez arasında güçlü sertifika tabanlı kimlik doğrulama uygulanmalıdır.
* **Veri Şifreleme:** Komutlar TLS veya VPN üzerinden şifreli kanallardan iletilmelidir.
* **Anomali İzleme Sistemleri:** Sürekli olarak yük değişimlerini izleyen otomatik alarm sistemleri kurulmalıdır.
* **Komut Doğrulama Mekanizması:** Her “şarjı durdur” komutu çok faktörlü doğrulama veya onay gerektirmelidir.
* **Ağ Segmentasyonu:** Şarj istasyonları, genel internet erişiminden izole edilmelidir.

**🔹 8. Sonuç**

Ani Yük Düşürme Saldırısı, elektrikli araç şarj altyapılarının güvenliğinde kritik bir zafiyet alanını temsil eder. Bu saldırı, yalnızca bireysel kullanıcıları değil, **ulusal enerji sistemlerinin kararlılığını** da tehdit edebilir.  
Gelişmiş izleme sistemleri, güvenli iletişim protokolleri ve makine öğrenmesi tabanlı anomali tespiti yöntemleriyle bu tür saldırılar büyük ölçüde önlenebilir.

**🔹 9. Kaynaklar**

1. H. Liu et al., *“Cybersecurity in Smart Grid and Electric Vehicle Charging Systems”*, IEEE Transactions on Smart Grid, 2023.
2. H. Zhang et al., *“Load Manipulation Attacks in EV Charging Networks”*, IEEE Access, 2022.
3. N. Komninos, *“Cyber Attacks Against Electric Vehicle Charging Systems”*, Computers & Security, 2021.
4. U.S. Department of Energy, *“Electric Vehicle Infrastructure Cybersecurity Best Practices”*, 2020.