# Elektrikli Araç Şarj Sistemlerinde Denial of Service (DoS) Anomalilerinin Tespiti ve Önlenmesi

## Özet

Elektrikli araç (EV) şarj altyapıları, yüksek bağlantı yoğunluğu nedeniyle DoS (Denial of Service – Hizmet Reddi) saldırılarına ve performans anomalilerine karşı savunmasızdır. Bu makale, şarj istasyonlarında görülen DoS kaynaklı anomalileri, saldırı vektörlerini ve tespit/önleme yöntemlerini incelemektedir. Özellikle OCPP (Open Charge Point Protocol) üzerinden gönderilen aşırı komut yüklerinin sistem kaynaklarını tüketerek hizmet kesintisine yol açtığı senaryolar analiz edilmiştir.

## 1. Giriş

Akıllı şarj sistemleri, enerji yönetimi ile ağ iletişimini birleştiren siber-fiziksel sistemlerdir. OCPP protokolü, şarj istasyonlarının uzaktan kontrolünü mümkün kılar; ancak bu da saldırganlara potansiyel bir kapı aralar. Hizmet reddi (DoS) saldırıları, sistemin normal çalışmasını engelleyerek kullanıcıların şarj oturumu başlatamamasına veya durduramamasına neden olur. Bu durum, hem kullanıcı deneyimini bozar hem de operasyonel gelir kaybı oluşturur.

## 2. DoS Anomalisi Nedir?

DoS anomalisi, bir sistemin kaynaklarının (CPU, bellek, ağ trafiği) olağandışı şekilde tüketilmesi sonucu erişilemez hâle gelmesi durumudur. Normal durumda saniyede birkaç komut işleyen şarj istasyonu, bir saldırı esnasında saniyede yüzlerce “StartTransaction” veya “StopTransaction” isteği alabilir. Bu yoğunluk, sistemin kuyruğunu doldurarak işlem gecikmeleri, zaman aşımları ve bağlantı kesintileri oluşturur.

## 3. Olası Nedenler ve Saldırı Vektörleri

• Komut Spam’i: Saldırgan kısa aralıklarla yüzlerce OCPP komutu gönderir.  
• Flooding (Taşkın Trafik): Ağ seviyesinde aşırı istek gönderimiyle bant genişliği tüketilir.  
• Yazılım Hataları: Rate limiting veya kaynak sınırlandırma mekanizması eksikliği.  
• Yanlış Konfigürasyon: Kuyruk boyutlarının yetersiz belirlenmesi veya TLS bağlantılarının yeniden kurulma hataları.

## 4. Anomali Tespiti Yöntemleri

4.1. Kural Tabanlı Tespit  
Saniyede gelen komut sayısı belirli bir eşiği aşarsa anomali olarak işaretlenir. Örnek: “5 saniyede 10’dan fazla komut” potansiyel DoS olarak değerlendirilir. CPU, RAM veya thread kullanımında ani artışlar gözlemlenir.  
  
4.2. İstatistiksel Yöntem  
Zaman serisi analizi ile normal işlem yükü profili oluşturulur. Ortalama + 3σ (standart sapma) üzerinde değerler anomali olarak etiketlenir.  
  
4.3. Makine Öğrenmesi Yaklaşımı  
Denetimsiz modeller (Isolation Forest, One-Class SVM) kullanılarak normal davranıştan sapmalar tespit edilir. Özellikler: komut frekansı, işlem süresi, yanıt oranı, CPU kullanımı.

## 5. Önleme ve Savunma Stratejileri

• Rate Limiting: Kullanıcı başına veya IP başına belirli zaman aralığında maksimum komut limiti.  
• Circuit Breaker: Sistem aşırı yük algıladığında yeni istekleri geçici olarak reddeder.  
• Doğrulama Katmanı: OCPP komutlarının yetkili kullanıcıdan geldiğini doğrulamak için API anahtarları veya dijital imzalar.  
• IDS/IPS Sistemleri: Anormal trafik yoğunluğunu algılayıp otomatik engelleme.  
• Kaynak İzleme: CPU ve bellek kullanımı için otomatik alarm eşikleri.

## 6. Sonuç

DoS anomalileri, akıllı şarj istasyonlarının sürekliliği açısından en kritik tehditlerden biridir. Bu çalışma, OCPP tabanlı şarj istasyonlarında aşırı komut yüküne bağlı hizmet reddi senaryolarını incelemiş ve tespit/önleme stratejileri önermiştir. DoS tespiti için kural tabanlı hızlı analiz ve ML tabanlı derin izleme yaklaşımlarının birlikte kullanılması önerilmektedir.

## Kaynakça

[1] Open Charge Alliance, OCPP 2.0.1 Specification, 2021.  
[2] IEEE, Smart Grid Security: DoS Attack Analysis, 2023.  
[3] OWASP, DoS and Flooding Mitigation Guide, 2024.  
[4] ENISA, Cybersecurity in EV Charging Infrastructure, 2022.