

# “Evil Twin” (Wi-Fi SSID Taklidi) Tabanlı Anomali Tespit Projesi

## 1. Proje Başlığı

Evil Twin (Wi-Fi SSID Spoofing) Tabanlı MITM Saldırılarının Dijital Simülasyonla Tespiti ve Yapay Zekâ Destekli Müdahalesi

## 2. Özet

Bu proje, elektrikli araç şarj istasyonları (EV charging points) ortamında ortaya çıkabilecek Evil Twin / Wi-Fi SSID taklidi türündeki Man-In-The-Middle (MITM) saldırılarını simülasyonla canlandırıp, ağ-cihaz-kullanıcı katmanlarında toplanan telemetri ve log bilgileri ile yapay zekâ tabanlı anomali tespiti gerçekleştirerek erken uyarı ve otomatik/insanlı müdahale mekanizmaları geliştirmeyi amaçlar. Proje açık kaynak araçlarla (Docker, mitmproxy, OpenSearch, Python) prototip düzeyinde uygulanacaktır.

## 3. Amaç ve Hedefler

Evil Twin saldırı senaryosunu güvenli, izole bir test ortamında simüle etmek.

Ağ, cihaz ve oturum (session) düzeyinde toplanacak loglardan anlamlı öznitelikler (features) çıkarıp ML modelleriyle anomali tespiti sağlamak.

Kritik durumlarda otomatik veya SOC (Security Operations Center) destekli müdahale (ör. cihaz izolasyonu, OTA/ödeme durdurma) öneri ve mock-ürünü sunmak.

OCPD gibi protokollere özgü kimlik-yeniden-kullanım (idTag replay) saldırılarına karşı deterministik kurallar geliştirmek ve bunları ensemble detektörüne entegre etmek.

## 4. Kapsam

Sadece laboratuvar/izole ağ ortamında simülasyon yapılacaktır (canlı kamu ağlarında test yapılmayacaktır).

Hedef, üretim seviyesinde tam güvenlik ürünü değil; akademik/prototip düzeyinde tespit yeteneği ve SOC playbook göstergesi sunmaktır.

Ödeme veya gerçek kişisel veri kullanılmayacak; tüm örnek veriler maskelenmiş veya sentetiktir.

## 5. Yöntem ve Mimari (kısa)

Simülasyon bileşenleri: Docker konteynerlerde çalışacak basit “şarj istasyonu” (Flask app: /auth, /telemetry, /ota) ve “istemci” scriptleri.

MITM simülasyonu: mitmproxy container ile istemci trafiğinin yakalanması/manipüle edilmesi. (Gerçek Wi-Fi Evil Twin kurulumu fiziksel donanım gerektirir; bu proje simülasyona odaklanır.)

Log toplama: mitmproxy çıktıları, uygulama logları ve simüle edilmiş DHCP/association verileri OpenSearch’e gönderilecek.

ML katmanı: Jupyter + Python ile feature extraction → Isolation Forest / Time-series Autoencoder (LSTM) → ensemble scoring.

Detektör orkestrasyonu: Basit Python servis, kural tabanlı yüksek-öncelikli alarmları ve ML skorlarını birleştirir; eşik aşıldığında mock-aksiyon tetikler (ör. isolate\_device API çağrısı).

## 6. Toplanacak Veri ve Öznitelikler

Ağ / Wi-Fi meta: SSID, BSSID (MAC), gateway\_mac, lease time, association time.

TLS / DNS meta: TLS sertifika fingerprint, SNI, DNS cevap IP'leri, IP değişim oranı.

Telemetri / uygulama: heartbeat interval, paket frekansı, firmware\_version, authorize/start/stop transaction eventleri.

OCPP-özgü (opsiyonel): idTag authorize / StartTransaction zamanları, connectorId, meterStart/Stop verileri.

Örnek feature: distinct\_bssid\_last\_1h, tls\_fingerprint\_change\_count, dns\_ip\_flip\_rate, heartbeat\_deviation, distinct\_ips\_per\_user\_1h.

## 7. Modelleme Stratejisi

Deterministik kurallar: imzasız firmware, TLS fingerprint mismatch, idTag overlap → anında yüksek öncelik alarmı.

ML modelleri:

Ağ anomali: Autoencoder veya Isolation Forest (tabular flow meta).

Cihaz davranışı: LSTM / time-series autoencoder (telemetri).

Oturum analizi: Isolation Forest (session features).

Ensemble: Her katmandan gelen skor ağırlıklı toplanır; final\_score > 0.8 ise otomatik karantina mock'u; 0.5–0.8 arası SOC uyarısı.

## 8. Test Planı ve Değerlendirme

Senaryolar: Basit Evil Twin (trafik yakalama), DNS spoofing, idTag replay (OCPP simüle), telemetri frekans manipülasyonu.

Metrikler: Recall (tespit oranı), Precision, False Positive Rate, Time-to-Detect (TTD). Hedef: simüle edilmiş saldırılarda yüksek recall, FP düşük tutmak.

Deney: Her saldırı tipi için kontrollü yürütme, log kaydı, modellerin skor çıktıları ve aksiyonların doğruluğu raporlanır.

## 9. Etik ve Hukuki Hususlar

Proje boyunca sadece izole test ağları kullanılacak; canlı ağlarda MITM veya trafiğe müdahale yapılmayacaktır.

Kişisel ve ödeme verileri kullanılmayacaktır; tüm veriler maskelenmiş veya üretilmiş olacak.

Elde edilen bulgular ve araçlar yalnızca savunma/araştırma amaçlı kullanılacaktır.

## 10. Sonuç / Talep

Bu proje, EV řarj altyapılarında kritik bir risk olan Wi-Fi tabanlı MITM saldırılarını, güvenli simölasyon ortamında tespit etmek ve AI destekli cevap mekanizmaları geliřtirmek üzere tasarlanmıřtır.