EV ŞARJ İSTASYONLARINDA OCPP TABANLI SİBER GÜVENLİK VE YAPAY ZEKA DESTEKLİ ANOMALİ TESPİTİ

Kural Tabanlı + Makine Öğrenimi (ML) Destekli Hibrit Anomali Tespiti

---

HAZIRLAYAN: MUHAMMED AZIZI – 190541606
DERS: BILGI SISTEMLERI VE GÜVENLIĞI
DÖNEM: 2025 GÜZ

1) Anomali Tanımı

OCPP bağlantısı kesildiği hâlde şarj istasyonunun enerji aktarmaya devam etmesidir. Bu durum, normal davranışın dışına çıkarak hem kontrolün kaybedilmesine hem de güvenlik ve faturalandırma ihlallerine yol açar.Bu çalışmada söz konusu anomali, hem kural tabanlı **(rule-based)** kontroller hem de makine öğrenimi **(Isolation Forest)** ile tespit edilmektedir.

2) Rule-Based kısmın Senaryosu

Zaman	Durum
t0	EV şarj oturumu başlatıldı — OCPP bağlantısı **aktif**
t1	Enerji aktarımı → **2.1 kWh**
t2	OCPP bağlantısı **kesildi (Disconnected)**
t3	Beklenen → Enerji kesilmeli
	Gerçekleşen → Enerji akışı **devam ediyor**
t4	Sayaç değeri: **6.4 kWh**
t5	Backend kontrol kaybı → **ANOMALİ**

Sonuç: OCPP oturumu sonlandırıldığı hâlde contactor açık kalmış ve enerji aktarımı sürmüştür.

3) ML-Based kısmın Senaryosu

Zaman	Durum
t0	EV şarja bağlandı — OCPP bağlantısı **aktif**
t1	Enerji akışı → Normal profil (0.7 kWh → Δe=0.7)
t2	Enerji akışında beklenmedik artış → (1.9 kWh → Δe=1.2)
t3	OCPP hâlâ **aktif**, contactor **kapalı değil**
t4	ML skoru eşik altında → Model anomalisi işaretledi
t5	Backend alarm üretir → ML-TABANLI ANOMALİ

Bu senaryo, OCPP bağlantısı kopmadan gerçekleşen davranışsal sapmaların, yalnızca **ML-tabanlı yaklaşımla** tespit edilebildiğini gösterir.

4) Kural-Tabanlı Tespit

```
IF connection_status == "DISCONNECTED"
AND meter_value > 0
AND contactor_state == CLOSED
THEN anomaly_detected = TRUE
```

5) ML-Tabanlı Tespit (Isolation Forest)

```
IF ML_score < threshold:
    anomaly = TRUE
```

Kullanılan Özellikler (Features)

- Enerji (e)
- Enerji değişimi (Δe / ΔkWh)
- Zaman aralığı (Δt)
- OCPP bağlantı durumu
- Contactor durumu

Çalışma Akışı

- Her ölçüm adımında veri toplanır
- Özellik vektörü oluşturulur
- Isolation Forest skor üretir → ML_score
- ML_score < threshold → ANOMALİ

6) Hibrit Karar Mekanizması

Kural tabanlı ve ML tabanlı karar birlikte değerlendirilir:

```
rule_based = (
    connection_status == "DISCONNECTED"
    and meter_value > 0
    and contactor_state == CLOSED
)
ml_based = (ML_score < threshold)
anomaly_detected = rule_based OR ml_based
```

7) Örnek Log Çıktıları

Kural tabanlı ve ML tabanlı karar birlikte değerlendirilir:

2025-11-11 23:26:23 | ML NORMAL | adım=1 | e=1.35 | Δ=0.45 | skor=-0.442

2025-11-11 23:26:30 | ✕ OCPP Kesildi

2025-11-11 23:26:30 | RULE ANOMALİ | adım=15 | e=11.20 | Δ=0.71

2025-11-12 00:54:16 | ML ANOMALİ | adım=17 | e=31.55 | Δ=19.90 | skor=-0.761

8) SWOT Analizi

Güçlü Yön

Hibrit tespit ile yüksek doğruluk

Zayıf Yön

Model yeniden eğitim ihtiyacı |

Fırsat

Dinamik güvenlik adaptasyonu

Tehdit

Sensör arızası / veri enjeksiyonu

9) SMART Hedefler Analizi

	S	M	A	R	T
Güvenli Kapatma	OCPP kesildiğinde contactor'ı kapatmak	%100 kesme	Firmware güncellemesiyle mümkün	Güvenlik için kritik	4 hafta
ML Tespit Başarısı	ML ile anomali tespit etmek	≥ %90 doğruluk	Mevcut verilerle eğitim	Kural tabanını tamamlar	6 hafta
Gelişmiş Loglama	Δe, bağlantı, ML skoru kaydetmek	≥ %95 tam kayıt	Yazılım güncellemesi yeterli	İzlenebilirlik sağlar	2 hafta
Anlık Alarm	Anomalide backend alarmı	≤ 1 sn	API ile mümkün	Müdahaleyi hızlandırır	3 hafta
Yıllık Revizyon	Kural + ML eşiğini gözden geçirmek	Yılda ≥ 1 güncelleme	Periyodik bakım	Sistem davranışı değişir	12 ay

10) Sonuç

OCPP bağlantısının kopmasına rağmen güç aktarımının sürmesi; güvenlik, faturalandırma ve protokol uyumu açısından kritik bir zafiyettir.

Bu çalışmada:

Kural tabanlı algılama

Isolation Forest tabanlı ML modeli

birleştirilerek hibrit bir tespit mekanizması uygulanmıştır.