
ANOMALİ SENARYO RAPORU

ADAPTİF ÖRNEKLEME MANİPÜLASYONU (Sampling Manipulation)
Ders: Bilgi Sistemleri Güvenliği
Proje: Şarj İstasyonlarının Güvenliği
Tarih: 01.11.2025
Hazırlayan: İbrahim Kerem Güven (Takım 10)

---

1) Özet

Şarj istasyonu veya ara katman cihazı (gateway/aggregator), enerji ölçüm örnekleme oranını (sampling rate) kasıtlı olarak azaltır veya yüksek tüketim değerlerini gizleyecek şekilde ortalama alır. Bu durumda kısa süreli **yüksek güç çekimleri faturalamaya yansımaz**, sistem "normal" göründüğü için operatör tarafından fark edilmesi zordur. Bu rapor, anomali tanımını, tespit kurallarını ve test planını içerir.

---

2) Normal Akış (Beklenen)

- Şarj başlar → istasyon belirli aralıklarla (ör. her 1 saniye) gerçek zamanlı enerji/güç ölçümü gönderir.
- Sunucu (CSMS) gelen ölçümleri kaydeder, enerji tüketimini hesaplar.
- Ölçüm frekansı sabittir (**samples/sec** veya **samples/min**).

Normal davranış:
Örnekleme frekansı *sabit + yüksek varyanslı güç verisi* içerir. (peak'ler görünür)

---

3) Anomali Tanımı (Gözlenen)

- İstasyon örnekleme oranını düşürür (ör. **1 saniyeden → 60 saniyeye**).
- Yüksek anlık tüketimler ortalamaya gömülür (peak smoothing).

- Faturalamaya yansıyan değer düşer → **eksik ücretlendirme / enerji kaybı**.

Kritik Tutarsızlık: ham ölçümler ile sunucuya ulaşan özet veri **farklı görünür**.

---

4) İzlenecek Veri Alanları

Veri Alanı	Açıklama
sampling_rate / samples_per_minute	Bir dakikada kaç örnek gönderildiği
variance (kWh / power profile)	Enerji/güç ölçümlerinin dalgalanma miktarı
meter_total_kWh	Toplam enerji tüketimi
raw_sample_count	Cihazdaki ham örnek sayısı (buffer)
timestamp	Örnek zaman damgası

---

5) Tespit Kuralları (Basit IF / THEN)

Kural-1: Sampling Düşüşü

IF samples_per_minute < MIN_EXPECTED_RATE (ör. < 30)
THEN ALARM ("Örnekleme düşürüldü")

Kural-2: Varyans Düşüşü (Energy Flatness)

IF rolling_variance(current_session) < historical_variance * 0.30
AND session_active = true
THEN ALARM ("Peak değerler gizleniyor olabilir")

Kural-3: Ham veri / gönderilen veri tutarsızlığı

IF raw_sample_count >> sent_sample_count
THEN ALARM ("Yerelde veri birikiyor → Manipülasyon şüphesi")

---

6) Etki Analizi

Alan	Etki

Faturalama	Kullanıcı daha az enerji tüketmiş gibi görünür → gelir kaybı
Operasyon	Yük profili yanlış yorumlanır → kapasite/peak planlama bozulur
Güvenlik	Şebeke koruma sistemleri (ani yük artışı algılama) devre dışı kalır

---

7) Olası Nedenler

- Bilerek yapılan *enerji hırsızlığı amaçlı manipülasyon*
- Firmware'de örnekleme frekansı oynanması
- Ağdaki bir gateway'in filtreleme yapması (proxy smoothing)
- Performans optimizasyonu bahanesiyle sampling rate düşürülmesi

---

8) Test / Senaryo Planı

Senaryo	Adımlar	Beklenen Sonuç
S1 – Örnekleme oranı düşürme	sampling_rate'i 1s → 60s yap, yüksek güç tüketimi oluştur	Kural-1 alarm verir (samples_per_minute < eşik)
S2 – Peak smoothing (ortalama alma)	Peak değerleri filtrele, ortalama değeri gönder	Kural-2 alarm (variance düşer)
S3 – Buffer manipülasyonu	Ham veriyi buffer'da tut, sunucuya göndermeme	Kural-3 alarm (raw_sample_count ≫ sent_sample_count)

---

9) Başarı Ölçütleri (Metrikler)

Metrik	Hedef	Açıklama
Tespit Oranı	≥ %95	Manipülasyon yapılan seansların yakalanma oranı
Yanlış Alarm	≤ %3	Normal seansların alarm üretmemesi
Alarm Süresi	≤ 10 sn	Manipülasyon anından alarma kadar geçen süre

---

10) Risk Azaltma Önerileri

- Minimum örnekleme zorunluluğu (`min_sampling_rate`)
- Varyans + percentile tabanlı anomaly detection (p95, p99)
- Araç / BMS verisi ile karşılaştırma (iki kaynak doğrulama)
- Örnekleme parametrelerinin firmware'de imzalanması (anti-tampering)

---

11) Kanıt / Log Örneği (Eklenecek)

```
samples_per_minute=5 (beklenen >30) → Alarm
variance=0.12 (beklenen >0.45) → Alarm
```

---

12) Sonuç

Adaptif örnekleme manipülasyonu, yüksek enerji çekişlerinin raporlanmamasına ve sessiz enerji kaybına yol açan kritik bir zafiyettir. Basit metriklerle (örnekleme oranı, varyans, buffer büyüklüğü) yüksek doğrulukla tespit edilebilir. Sisteme minimum örnekleme limiti, değişmez veri imzası ve çapraz doğrulama eklenmesi riski önemli ölçüde azaltır.

---

13) Faydalanılan Kaynaklar

Farokhi, F. (2020). Review of results on smart-meter privacy by data manipulation, demand shaping, and load scheduling. *IET Smart Grid, 3*(5), 605–613. https://doi.org/10.1049/iet-stg.2020.0129

Giaconi, Gunduz, Poor (2018) — *Privacy-Aware Smart Metering: Progress and Challenges*, **IEEE Signal Processing Magazine**. Kapsamlı derleme; veri manipülasyonu ve talep şekillendirme yaklaşımlarını ve metrikleri özetler https://www.imperial.ac.uk/media/imperial-college/research-centres-and-groups/ipc-lab/GGP_SPM_18.pdf