Anomali Senaryosu Raporu

Proje Başlığı:

Dalgalı Yük Saldırısı (Oscillatory Load Attack) – Elektrikli Araç Şarj Altyapısında Siber-Fiziksel Anomali Senaryosu

Ad-Soyad : Yunus Emeç

Öğrenci No : 235541044

Rapor Oluşturulma Tarihi : 04/11/2025

1. Giriş

Elektrikli araçların (EV) dünya genelinde hızla yaygınlaşmasıyla birlikte, bu araçların güvenli, hızlı ve akıllı bir biçimde şarj edilmesini sağlayan altyapılar da karmaşık siber-fiziksel sistemlere dönüşmüştür ***(Zhang et al., 2022).*** Bu dönüşüm, siber güvenlik ve enerji mühendisliğini doğrudan kesiştiren yeni risk alanlarını beraberinde getirmiştir. Özellikle ISO 15118 ve OCPP gibi iletişim protokollerinin kullanılması, sistemleri daha akıllı hale getirirken, aynı zamanda yeni saldırı vektörleri doğurmuştur ***(Pundir et al., 2022).***

EV şarj sistemleri yüksek güçlü elektrik akımlarıyla çalıştığı için, sadece dijital güvenlik açıkları değil, aynı zamanda fiziksel etkiler de ciddi sonuçlar doğurabilir. Bu çalışmada, şarj istasyonları ile elektrikli araç arasındaki etkileşimi hedef alan, literatürde az işlenmiş bir anomali tanımlanmıştır: **Dalgalı Yük Saldırısı (Oscillatory Load Attack)**. Bu senaryo, dijital bir saldırının fiziksel çıktılar yoluyla şebeke istikrarını bozabileceğini göstermektedir ***(Gao et al., 2021)***.

2. Literatür Özeti

Çeşitli araştırmalar EV güvenliği üzerine odaklanmıştır. Cho & Shin (2016), araç içi ağ (CAN-Bus) güvenliğine yönelik saldırıların, doğrudan kontrol birimlerine erişim sağlayabileceğini göstermiştir. Gao et al. (2021) ise otonom sürüş güvenliği bağlamında sensör manipülasyonlarının sistem davranışını değiştirebileceğini ortaya koymuştur. Alalewi et al. (2021) tarafından yapılan bir incelemede, 5G tabanlı V2X haberleşme protokollerinde zamanlama tabanlı saldırıların olası olduğu belirtilmiştir. Tüm bu çalışmalar, EV altyapısının karmaşıklığını ve çok katmanlı saldırı yüzeyini göstermektedir.

Ancak bu araştırmaların çoğu, doğrudan **güç kalitesi parametreleri** üzerinden yapılan siber-fiziksel saldırılara değinmemektedir. Literatürde flicker, harmonik distorsiyon veya güç dengesizlikleri genellikle sistem arızası olarak ele alınmıştır ***(IEEE Std 519-2014).*** Bu çalışma, bu fiziksel bozulmaların kasıtlı olarak üretilebileceği ve saldırı biçimine dönüştürülebileceğini öne sürmektedir.

3. Senaryo Tanımı ve Saldırı Akışı

Dalgalı Yük Saldırısı'nda (Oscillatory Load Attack) saldırgan, şarj istasyonu veya araç içi şarj yazılımına sızarak, şarj akımını periyodik biçimde yükseltip düşürür. Bu, saniyede birkaç kez maksimum ve minimum akım arasında salınım yapan bir yük profili oluşturur ***(Petit et al., 2015)***. Böyle bir davranış, sistem açısından doğal görünse de şebekede **gerilim dalgalanmaları (flicker)** ve **harmonik artış** yaratır.

Saldırı adımları:

1. Saldırgan, zafiyet içeren istasyon yazılımına erişim sağlar.

2. Şarj oturumu başlatılır, sistem normal çalışmaya başlar.

3. Araç kontrol algoritması manipüle edilerek akım salınımları başlatılır.

4. Şebekede flicker etkisi artar, trafolar ve röleler anormal davranır.

5. Sistem kararsız hale gelir ve hizmet kesintisi yaşanır.

Bu saldırı, hem enerji sistemlerini hem de dijital kontrol mekanizmalarını hedef alan çok katmanlı bir tehdittir ***(Aliwa et al., 2021).***

4. Tespit Yöntemi ve AI Yaklaşımı

Bu tür anomalilerin tespiti, klasik kural tabanlı sistemlerle zordur çünkü yük değişimleri kısa süreli ve periyodiktir. Bu nedenle yapay zekâ tabanlı yöntemler önerilmektedir ***(Nagarajan et al., 2023).*** Önerilen yöntem, iki katmandan oluşur:

- **Zaman Serisi Anomali Tespiti:** Akım/gerilim verileri Autoencoder modeliyle analiz edilir. Model, normal yük profillerini öğrenir ve yeniden oluşturma hatası (reconstruction error) üzerinden anormallikleri belirler.

- **Korelasyon Analizi:** OCPP mesajlarındaki güç değerleri, fiziksel ölçümlerle karşılaştırılır ***(Alalewi et al., 2021)***. Eğer sistem "normal" bildirim yaparken sensörler dalgalı profil gösteriyorsa, bu tutarsızlık anomali olarak işaretlenir.

Ayrıca harmonik oranlarının değişimi, IEEE 519 standardına göre eşik bazlı olarak denetlenir. Bu sayede hem dijital hem de fiziksel verilerden beslenen hibrit bir tespit mimarisi oluşturulur.

5. Kullanılan Veriler

Çalışmada kullanılacak veri türleri şunlardır:

- Akım ve gerilim zaman serileri (≥1 kHz örnekleme)

- Şarj seansı logları (başlangıç, bitiş, enerji tüketimi)

- OCPP mesajları (MeterValues, StopTransaction)

- Güç kalitesi ölçümleri (flicker, THD)

- Sensör tabanlı ısı, voltaj, akım ölçümleri ***(Aliwa et al., 2021)***

6. Performans Analizi

Tespit sisteminin performansı aşağıdaki metriklerle değerlendirilir:

- Tespit Oranı (TPR) ≥ %95

- Yanlış Pozitif Oranı (FPR) ≤ %3

- F1 Skoru ≥ 0.92

- Tespit Gecikmesi ≤ 2 saniye (IEEE 519 sınırları içinde)

Denemelerde, tespit doğruluğu ve sistem gecikmesi değerlendirilecek, geleneksel istatistiksel yöntemlerle karşılaştırma yapılacaktır ***(Gao et al., 2021).***

7. Savunma ve Müdahale Mekanizmaları

Bu saldırının etkilerini önlemek için aşağıdaki yöntemler önerilmektedir:

- Şarj seansı esnasında yük değişim oranının sınırlanması (ΔI/Δt)

- AI tabanlı anomali tespitiyle otomatik yük kesme (fail-safe)

- PQ monitörleri ile anlık harmonik izleme

- Blokzincir destekli loglama ***(Xu et al., 2022)***

- Firmware imza doğrulaması ve zorunlu güncellemeler ***(ISO 15118)***

Bu yöntemler, sadece tespiti değil, aynı zamanda **önleyici koruma** mekanizmasını da kapsamaktadır.

8. Sonuç ve Gelecek Çalışmalar

Dalgalı Yük Saldırısı senaryosu, elektrikli araç altyapısının fiziksel katmanını hedef alan siber-fiziksel bir tehdit olarak tanımlanmıştır. Bu tür saldırılar, sistemlerde doğrudan gözlemlenebilen fakat dijital düzeyde fark edilmesi zor anomaliler yaratır. Gelecekte yapılacak çalışmalar, bu saldırıların simülasyonu ve gerçek donanım üzerinde test

edilmesiyle savunma mekanizmalarının geliştirilmesine odaklanmalıdır ***(Sharma et al., 2021; Loukas et al., 2019).***

9. Kaynakça

- ISO 15118 Standard: Road Vehicles – Vehicle to Grid Communication Interface
- Open Charge Point Protocol (OCPP) 1.6/2.0.1 Guidelines
- IEEE Std 519-2014: Recommended Practice and Requirements for Harmonic Control
- Cho, K. T., & Shin, K. G. (2016). Fingerprinting electronic control units for vehicle intrusion detection.
- Gao, C., Wang, G., et al. (2021). Autonomous driving security: State of the art and challenges.
- Petit, J., et al. (2015). Remote attacks on automated vehicle sensors.
- Zhang, K., Shi, Y., et al. (2022). Advancements in industrial cyber-physical systems.
- Alalewi, A., Dayoub, I., & Cherkaoui, S. (2021). On 5G-V2X use cases and enabling technologies: A comprehensive survey.
- Pundir, A., Singh, S., et al. (2022). Cyber-physical systems enabled transport networks in smart cities.
- Aliwa, E., Rana, O., et al. (2021). Cyberattacks and countermeasures for in-vehicle networks.
- Sharma, S., Kumar, A., & Chaudhary, R. (2021). Connected autonomous vehicle cybersecurity: A taxonomy of vulnerabilities, threats, and attacks.
- Loukas, G., Karapistoli, E., et al. (2019). A taxonomy and survey of cyber-physical intrusion detection approaches for vehicles.
- Nagarajan, J., Mansourian, P., et al. (2023). Machine Learning based intrusion detection systems for connected autonomous vehicles: A survey.
- Xu, C., Wu, H., et al. (2022). Blockchain-oriented privacy protection of sensitive data in the internet of vehicles.