Şebekeden Bağımsız Güneş Enerjili Elektrikli Araç Şarj İstasyonlarına Yönelik Siber Saldırıların Araştırılması

1. GİRİŞ

Ulaşım sektörü, küresel ısınma endişelerini gidermek ve karbondan arındırma hedeflerine ulaşmak için fosil yakıtlı taşımacılıktan elektrikli taşımacılığa doğru önemli bir dönüşümün eşiğindedir. Bu dönüşümü kolaylaştırmak ve artan elektrikli araç (EA) satışlarına yanıt verebilmek için şarj istasyonlarının hızla kurulması zorunludur. Ancak, şebekenin yakın olmadığı veya şebeke yükseltme yatırımlarının pahalı olduğu uzak konumlarda, şebekeden bağımsız (off-grid) güneş enerjili EA şarj istasyonları hayati bir çözüm olarak öne çıkmaktadır. Bu istasyonlar, güneş enerjisi üretimi, batarya enerji depolama sistemleri (BEDS) ve enerji yönetim sistemlerini (EYS) birleştirir. Ancak bu entegrasyon, şarj istasyonunu siber saldırılara açık karmaşık bir siber-fiziksel sisteme dönüştürmektedir.

2. SENARYO TANIMI

Makalede ele alınan sistem, şebekeden tamamen bağımsız çalışan, güneş enerjisiyle güçlendirilmiş bir elektrikli araç şarj istasyonudur. Bu sistem şu fiziksel bileşenleri içerir: İki adet 350 kW hızlı şarj istasyonu, 1 MW'lık bir güneş enerjisi çiftliği, 1 MW/4 MWh kapasiteli bir batarya enerji depolama sistemi (BEDS) ve 1 MW'lık bir boşaltma yükü (dump load). Sistemin çalışması, Enerji Yönetim Sistemi (EYS) ve yerel kontrolörler arasındaki iletişim ağlarına dayanır. Batarya sistemi, DC bara (DC link) voltajını düzenlemekle sorumludur. Boşaltma yükü (dump load) ise bataryanın aşırı şarj olmasını önlemek için fazla güneş enerjisini tüketmek üzere kullanılan kontrol edilebilir bir DC kıyıcıdır. Saldırganın amacı, bu bileşenler arasındaki iletişimi manipüle ederek istasyonu devre dışı bırakmaktır.

3. ANOMALİ TANIMI

Bu çalışmanın odaklandığı "anomali", şarj istasyonunun iletişim ağlarına ve ölçüm cihazlarına yapılan siber saldırılardır.

- **Anomali:** Saldırganların, sistemin kullanılabilirliğini (availability) ve bütünlüğünü (integrity) hedef alarak DC bara voltajını normal sınırların dışına çıkarmasıdır.

- **Anomali Metriği (Saldırı Türleri):**
  1. **Kontrol ile İlgili Saldırılar:** Saldırganın EYS'den gelen kontrol komutlarını taklit etmesi (örneğin, batarya doluyken boşaltma yükünü devre dışı bırakmak veya güneş enerjisi varken üretimi kesmek).

  2. **Ölçümlere Yönelik Saldırılar:** Yanlış Veri Enjeksiyonu (FDI) ile voltaj ölçümlerinin değiştirilmesi veya Hizmet Reddi (DoS) saldırısı ile ölçümlerin geciktirilmesi.

- **Açıklama:** Bu saldırılar, sistemin "beyni" olan yönetim sisteminin yanlış kararlar almasına veya kontrol mekanizmasının istikrarsızlaşmasına neden olarak elektriksel koruma rölelerini tetikler.

4. BU ANOMALİNİN ETKİLERİ VE SONUÇLARI

Siber saldırı anomalisi, şebekeden bağımsız şarj istasyonları için ciddi operasyonel ve fiziksel sonuçlar doğurmaktadır:

- **Hizmet Kesintisi:** DC bara voltajındaki aşırı sapmalar, koruma rölelerini tetikleyerek şarj istasyonunu tamamen devre dışı bırakır.

- **Eş Zamanlı Çöküş:** Bu saldırı, istasyondaki tüm hızlı şarj ünitelerini aynı anda hizmet dışı bırakma potansiyeline sahiptir.

- **Kritik Altyapı Sorunları:** Özellikle şebekenin olmadığı uzak bölgelerde veya genel elektrik kesintileri (blackout) sırasında, bu istasyonların kaybı elektrikli ulaşımda ciddi aksamalara neden olabilir.

- **Donanım Riski:** Saldırılar, bataryanın aşırı şarj olması veya DC bara kapasitörünün boşalması gibi fiziksel güç dengesizliklerine yol açabilir.

5. SWOT ANALİZİ

Makalede sunulan analiz ve bulgular temel alınarak oluşturulan SWOT analizi şöyledir:

Kategori	Unsurlar	Makale Desteği ve Detaylar
GÜÇLÜ YÖNLER (Strengths)	**İlk Kapsamlı İnceleme:**	Literatürde daha önce incelenmemiş olan *şebekeden bağımsız* (off-grid) güneş enerjili EA şarj istasyonlarının siber güvenliğini ele alan ilk çalışmadır.
GÜÇLÜ YÖNLER (Strengths)	**Çoklu Saldırı Vektörü Simülasyonu:**	Hem kontrol komutlarına (EYS'den bileşenlere) hem de ölçüm verilerine (sensörlerden EYS'ye) yönelik farklı saldırı sınıflarını (FDI ve DoS) detaylı bir şekilde simüle etmiş ve kanıtlamıştır.
ZAYIF YÖNLER (Weaknesses)	**Tek Hata Noktası (Single Point of Failure):**	Çalışılan sistemde DC bara voltajı sadece batarya sistemi tarafından düzenlenmektedir, bu da sistemi batarya yönetimine yapılan saldırılara karşı aşırı hassas hale getirir.
ZAYIF YÖNLER (Weaknesses)	**Çözüm Önerisi Eksikliği:**	Makale, güvenlik açıklarını tespit etmeye odaklanmıştır; ancak saldırı tespit ve azaltma (mitigation) stratejilerini detaylandırmamış, bunları gelecek çalışmalara bırakmıştır.

FIRSATLAR (Opportunities)	**Fizik-Farkındalı Tespit Sistemleri:**	Çalışma, kimlik doğrulamanın yetersiz kaldığı durumlar için fizik tabanlı (physics-aware) saldırı tespit sistemlerinin geliştirilmesi gerekliliğini ortaya koymaktadır.
FIRSATLAR (Opportunities)	**Dağıtık Kontrol Mekanizmaları:**	DC bara voltaj regülasyonu için güneş enerjisi üretiminin de katkıda bulunduğu dağıtık kontrol mekanizmalarının araştırılması, sistemin dayanıklılığını artırabilir.
TEHDİTLER (Threats)	**İçeriden Gelen Tehditler:**	Saldırganlar, memnuniyetsiz çalışanları kullanarak veya çalınan kimlik bilgileriyle şifreleme önlemlerini aşarak sisteme erişebilir.
TEHDİTLER (Threats)	**Yüksek Hızlı Veri Zorluğu:**	Ölçüm verilerinin yüksek iletim hızları nedeniyle şifrelenmesi zordur, bu da ölçüm tabanlı saldırıların (FDI/DoS) engellenmesini zorlaştırır.

6. BU ANOMALİYİ ÇÖZMEK İÇİN YAPILABİLECEK ÖNERİLER

Makale, tespit edilen güvenlik açıklarını gidermek ve istasyonun dayanıklılığını artırmak için aşağıdaki yaklaşımların gerekliliğini vurgulamaktadır:

- **Kimlik Doğrulama Yöntemleri:**
  - **Öneri:** Kontrol ile ilgili saldırıları azaltmak için güçlü kimlik doğrulama (authentication) yöntemleri kullanılmalıdır.
  - **Neden:** Sahte komutların sisteme girmesini engellemek için ilk savunma hattıdır.
- **Fizik-Farkındalı Saldırı Tespit Sistemi (Physics-Aware IDS):**

    - **Öneri:** Kimlik doğrulamanın olmadığı veya aşıldığı durumlarda, sistemin fiziksel davranışlarını izleyen bir saldırı tespit sistemi gereklidir.

    - **Neden:** Sistemin beklenen fiziksel tepkileri ile gerçekleşen durum arasındaki tutarsızlıkları (örneğin güneş varken üretimin sıfır görünmesi) tespit etmek için kritiktir.
- **Gözlemci Tabanlı Yöntemler (Observer-Based Methods):**
    - **Öneri:** Ölçüm verilerine yönelik saldırılar için gözlemci tabanlı yöntemler kullanılmalıdır.

    - **Neden:** Ölçüm verilerinin yüksek iletim hızı nedeniyle şifreleme her zaman pratik değildir; bu yöntemler verideki anormallikleri matematiksel olarak saptayabilir.

7. SONUÇ

Bu çalışma, şebekeden bağımsız güneş enerjili elektrikli araç şarj istasyonlarının enerji yönetim sistemi ve DC bara voltaj düzenleme mekanizmasına yönelik siber saldırı senaryolarını incelemiştir. Yapılan simülasyonlar, hem sahte kontrol komutlarının (control-related attacks) hem de manipüle edilmiş ölçüm verilerinin (measurement attacks), istasyonu hizmet dışı bırakmak için başarılı bir şekilde kullanılabileceğini göstermiştir.
Sonuçlar, bu tür saldırıların DC bara voltajını normal çalışma limitlerinin dışına iterek koruma sistemlerini tetiklediğini ve istasyonun kapanmasına neden olduğunu kanıtlamıştır. Bu durum, özellikle alternatif şarj imkanlarının kısıtlı olduğu uzak bölgelerde elektrikli ulaşım altyapısı için ciddi bir risk oluşturmaktadır.

8. KAYNAKÇA

Yazdanipour, S., Arani, F.M. ve Jahromi, A.A. (2024). Investigating Cyberattacks Against Off-Grid Solar-Powered Electric Vehicle Charging Stations. 2024 IEEE/PES Transmission and Distribution Conference and Exposition (T&D).