GÜÇ SİSTEMLERİ KONFERANSI IV

Güç Sistemleri Konferansı 2025

cigre Türkiye

USB Ethernet Adaptörü Üzerinden Modbus TCP/IP ile Bağlantılı LFC Sistemine Yönelik Siber Saldırıların XGBoost-SVM ile Tespit Edilmesi

Detection of Cyber Attacks on Modbus TCP/IP-Connected LFC System via USB Ethernet Adapter Using XGBoost-SVM

Feyza Nur ÇAKICI[1], İbrahim EKE[2], Süleyman Sungur Tezcan[1]

[1]Gazi Üniversitesi, Mühendislik Fakültesi, Elektrik-Elektronik Mühendisliği

[2]Kırıkkale Üniversitesi, Mühendislik ve Doğa Bilimleri Fakültesi, Elektrik-Elektronik Mühendisliği

Feyza Nur ÇAKICI

Elektrik-Elektronik Mühendisi/Doktora Öğrencisi

Bildiri ID Numarası: 0133

İÇİNDEKİLER

I. MOTİVASYON

- Bu çalışmanın amacı, SCADA sistemlerinde kullanılan Modbus TCP/IP protokolünün güvenlik açıklarından yararlanılarak yük frekans kontrolüne (Load Frequency Control — LFC) yönelik gerçekleştirilebilecek siber saldırı türlerini yüksek doğrulukla tespit etmektir.
- Modbus TCP/IP ile Ethernet tabanlı ağ bağlantıları, akıllı şebekelerin faaliyetlerini uzaktan izlemek ve kontrol etmek amacıyla SCADA sistemleri tarafından yaygın olarak kullanılmaktadır. Ancak bu ağ bağlantıları, sistemleri siber saldırılara karşı savunmasız bırakmaktadır.
- Bu doğrultuda çalışma, Modbus TCP/IP protokolü üzerinden USB Ethernet Adaptörü ile bağlantı gerçekleştirerek LFC sistemlerine ait ölçüm verilerine siber saldırılar düzenlenmesine odaklanmaktadır.

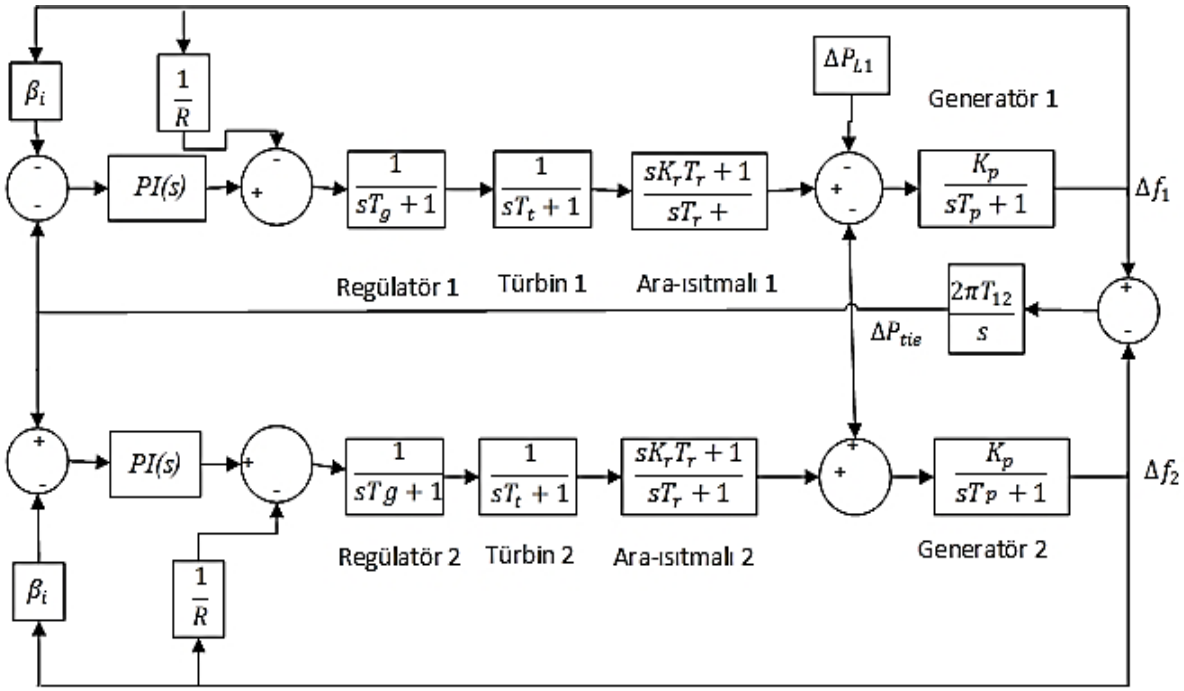
II. GİRİŞ

- LFC sistemlerine yönelik siber saldırılarda saldırganların amaçları; ölçüm verilerini manipüle etmek, SCADA ile cihazlar arasındaki haberleşmeyi engellemek, kontrol birimlerine hatalı veriler göndererek jeneratörlerin işletimini olumsuz etkilemek ve yük birimlerini hedef alarak frekans dalgalanmalarına yol açmaktır. Literatürde bu saldırıların tespitine yönelik çeşitli yapay zekâ tabanlı algoritmalar incelenmektedir.
- Bu çalışmada, Modbus TCP/IP üzerinden USB-Ethernet adaptörü kullanılarak bağlantı kurulmuş; SCADA sistemine gönderilen frekans ile bağlantı hattı güç ölçümlerine FDI (False Data Injection) ve yineleme (Replay) saldırıları uygulanmıştır. Gerçekleştirilen saldırıların türlerini tespit etmek amacıyla XGBoost–SVM hibrit makine öğrenmesi modeli kullanılmıştır.

III. SİSTEMİN MODELLENMESİ VE SİBER SALDIRILAR

A. İki Bölgeli Ara-Isıtmalı LFC Modeli

LFC sistemleri, üretilen ve tüketilen gücün dengelenmesinde ve güç sisteminin kararlılığının sağlanmasında kritik bir görev üstlenmektedir. Şekil 1'de iki bölgeli ara-ısıtmalı termal türbinlerin bulunduğu lineerleştirilmiş LFC modeli gösterilmektedir.



Şekil 1

III. SİSTEMİN MODELLENMESİ VE SİBER SALDIRILAR

B. Modbus TCP/IP Protokolü

Modbus TCP (Transmission Control Protocol)/IP (Ethernet Protocol) protokolü, Modbus/RTU'nun bir versiyonu olarak tasarlanmakta ve bu protokol aracılığıyla aynı ağda yer alan cihazlar, IP adresleri üzerinden Ethernet bağlantısı ile veri alış verişi gerçekleştirmektedir.

III. SİSTEMİN MODELLENMESİ VE SİBER SALDIRILAR

C. Sahte Veri Enjeksiyon Saldırısı (False Data Injection-FDI)

Çok bölgeli enterkonnekte sistemlerinde, açık ağ bağlantısının kullanımından kaynaklı güvenlik açıkları meydana gelmekte ve bu da saldırganların kontrol merkezi ile ölçüm birimleri arasındaki iletişim kanallarını kullanarak siber saldırı düzenlemesine neden olmaktadır. Saldırıların matematiksel eşitlikleri sırasıyla denklem 1 ve denklem 2'de gösterilmektedir.

$$\Delta f_{saldırı} = \Delta f_i + a_i \cdot sin(b_i \cdot t) \quad (1)$$

$$\Delta f_{saldırı} = \Delta f_i + c_i \cdot t \quad (2)$$

III. SİSTEMİN MODELLENMESİ VE SİBER SALDIRILAR

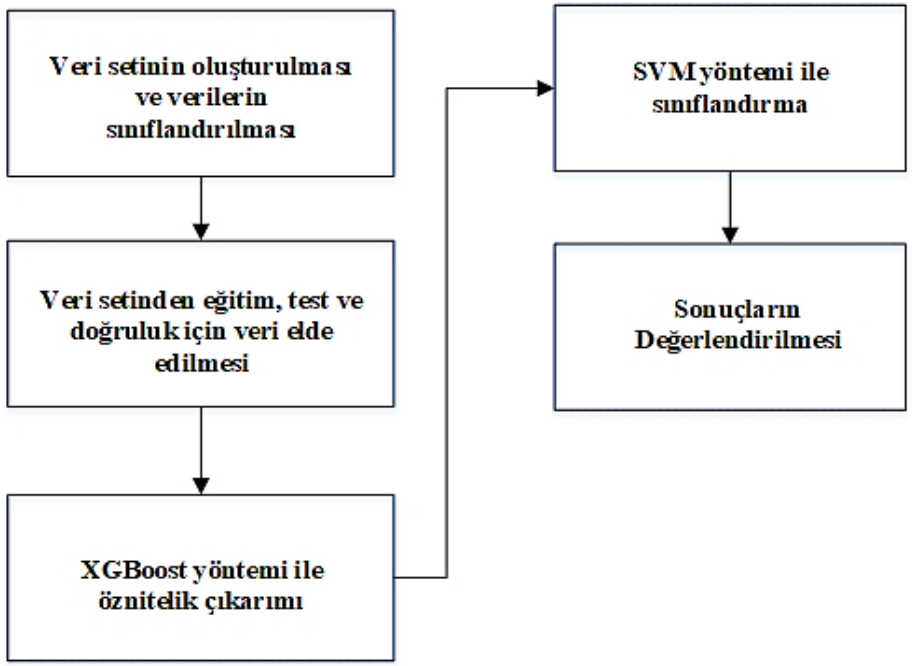
D. Yineleme saldırısı

Yineleme saldırısında (Replay Attack), veri bütünlüğünü hedef alarak ölçüm ve kontrol sinyallerin kaydedildiği iletişim kanallarına saldırılar düzenlenmektedir. Saldırı iki aşamada gerçekleşmekte: birinci aşamada, veri toplama cihazlarından toplanan veriler saklanmakta ve ikinci aşamada ise gerçek verilerin değerleri saklanan verilerin değerleri ile değiştirilmektedir.

III. SİSTEMİN MODELLENMESİ VE SİBER SALDIRILAR

E. Siber Saldırı Tespit Sistemi

Siber saldırıların tespitinde kullanılan modelin akış diyagramı Şekil 2'de gösterilmektedir.



Şekil 2

III. SİSTEMİN MODELLENMESİ VE SİBER SALDIRILAR

F. Veri Setinin Elde Edilmesi

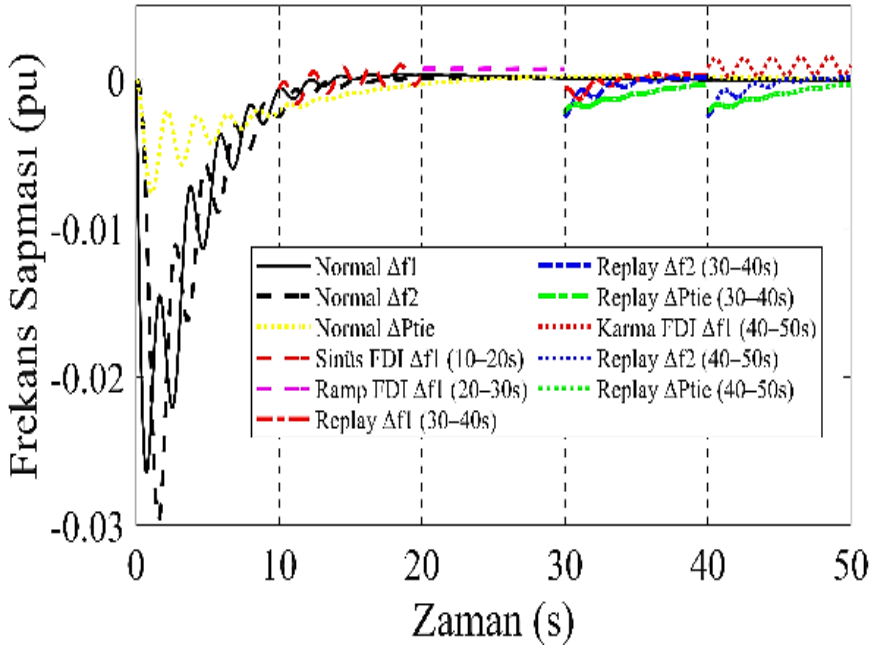
- Makalede saldırının gerçekleştirildiği birinci ve ikinci bölgelerin frekans sapma değerleri ile bağlantı hattı güç değeri, Matlab/Simulink programında simüle edilen iki bölgeli ara-ısıtmalı LFC sisteminden üretilmiştir. Simülasyonda, 50 saniye boyunca elde edilen değerler 100 Hz örnekleme frekansı ile ölçeklendirilerek toplam 5000 veri elde edilmiştir.

- ModbusPal 1.6c simülatörü ile USB Ethernet Adaptörünün IP adresi ve 502 numaralı port üzerinden Modbus TCP/IP bağlantısı sağlanmıştır. Böylece Modbus sunucu görevini ModbusPal 1.6c simülatörü ve Modbus istemci görevini ise Simulink programı üstlenmiştir.

III. SİSTEMİN MODELLENMESİ VE SİBER SALDIRILAR

F. Veri Setinin Elde Edilmesi

•Şekil 3'te LFC sistemine yönelik siber saldılar gösterilmektedir. Simülasyonda, ilk 10 saniye herhangi bir saldırı gerçekleştirilmemiştir. Sinüs saldırısının genlik değeri 0.006, frekans değeri 0.5 ve rampa saldırısı için eğim değeri 0.00002 olarak belirlenmiştir.



Şekil 3

•**10–20 saniye:** Birinci bölgenin frekans sapmasına **sinüs saldırısı** uygulanmıştır.

•**20–30 saniye:** Birinci bölgenin frekans sapmasına **rampa saldırısı** uygulanmıştır.

•**30–40 saniye:** Tüm verilere **yineleme saldırısı** uygulanmış; bu saldırıya **%1** oranında gürültü eklenmiştir.

•**40–50 saniye:** Birinci bölgenin frekans bağlantı hattı güç değerine **yineleme saldırısı** gerçekleştirilmiştir.

III. SİSTEMİN MODELLENMESİ VE SİBER SALDIRILAR

G. XGBoost-SVM Modeli

Destek vektör makine algoritması (Support Vector Machine-SVM), iki kategorili sınıflandırmaya ait problemlerin çözümünde kullanılmaktadır. Gelişmiş gradyan artırma (Extreme Gradient Boosting-XGBoost) algoritması, karar ağaç makine öğrenmesi yöntemine dayanmakta ve bu model birçok karar ağacının bir araya getirilmesiyle meydana gelmektedir.

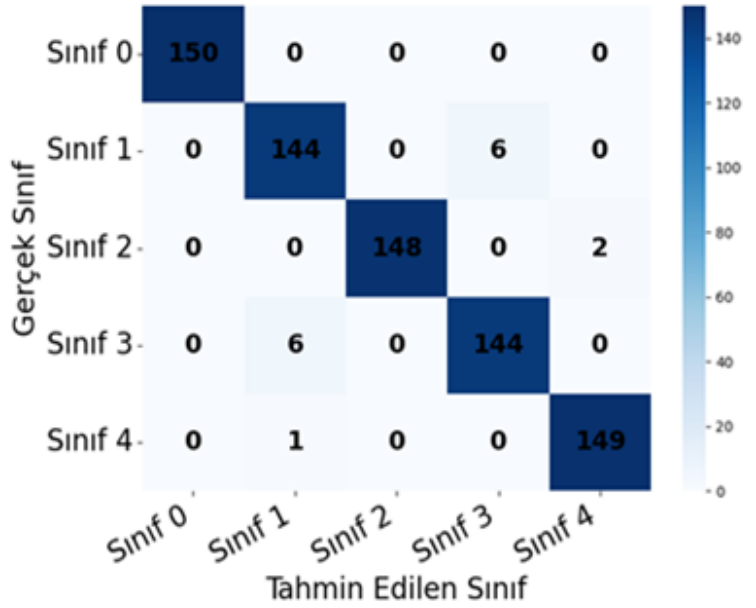
IV. SİMÜLASYON SONUÇLARI

- İki bölgeli LFC sisteminden elde edilen toplam 5000 veri, eğitim, doğrulama ve test için sırasıyla %70, %15 ve %15 oranlarında bölünmüştür.
- Veri setimizde birinci ve ikinci bölgeye ait frekans sapması ile bağlantı hat güç verisinden oluşan toplam 3 özellik bulunmaktadır. XGBoost yöntemi ile yüksek boyutlu özellikler üretilmiş ve veri setimizin özellik sayısı arttırılmıştır.
- XGBoost-SVM modelinin genel başarı değerlendirmesinde test doğruluk değeri %98.00 ve doğruluma değeri ise %97.33 olarak elde edilmiştir. Sonuçlara bakıldığında bu iki değerin birbirine çok yakın olması, modelde aşırı öğrenmenin (overfitting) gerçekleşmediği sonucuna varılmaktadır.

IV. SİMÜLASYON SONUÇLARI

Sınıf No	Doğruluk Değeri (%)
0 (Normal)	%100
1 (Sinüs Saldırısı)	%98.27
2 (Rampa Saldırısı)	%99.73
3 (Yineleme Saldırısı)	%98.40
4 (Karma Saldırı)	%99.60

Tablo 1



Şekil 4

Tablo 1'de XGBoost-SVM modeline ait her bir sınıfın doğruluk değeri ve Şekil 4'te ise XGBoost-SVM modeline ait karşılık matrisi gösterilmektedir.

IV. SONUÇLAR

- Çalışmada, SCADA sisteminde yaygın olarak kullanılan Modbus TCP/IP protokolünü hedef alan siber saldırılardan FDI ve yineleme saldırıları uygulanmıştır. Fiziksel ağ bağlantısını gerçekleştirmek amacıyla USB Ethernet Adaptörü kullanılmış ve Modbus TCP/IP tabanlı gerçek zamanlı veri akışının gerçekleştirilmesi sağlanmıştır.
- Simüle edilen LFC sisteminin ölçüm verilerine yönelik dört farklı siber saldırı senaryosu farklı zaman aralıklarında gerçekleştirilmiş ve kapsamlı bir veri seti elde edilmiştir.
- Veri setindeki dört ayrı sınıfı tespit etmek amacıyla geliştirilen XGBoost-SVM hibrit modeli hem sınıfları ayırt etmede hem de genelde yüksek bir başarı gösterdiği sonucuna varılmaktadır.
- Bundan dolayı iletişim protokollerine yönelik fiziksel olarak gerçekleşebilecek saldırılara karşı bilimsel çalışmaların yapılması önemlidir.

TEŞEKKÜRLER