İSTANBUL TEKNİK ÜNİVERSİTESİ ★ LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

OTOMATİK ÜRETİM KONTROLÜ SİSTEMLERİNE YAPILAN YANLIŞ VERİ ENJEKSİYON SALDIRILARININ TORBALAMA AĞAÇLARI ALGORİTMASI İLE TESPİTİ

YÜKSEK LİSANS TEZİ

Atakan ÖZTÜRK

Elektrik Mühendisliği Anabilim Dalı

Elektrik Mühendisliği Programı

ARALIK 2023

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

OTOMATİK ÜRETİM KONTROLÜ SİSTEMLERİNE YAPILAN YANLIŞ VERİ ENJEKSİYON SALDIRILARININ TORBALAMA AĞAÇLARI ALGORİTMASI İLE TESPİTİ

YÜKSEK LİSANS TEZİ

Atakan ÖZTÜRK

(504191059)

Elektrik Mühendisliği Anabilim Dalı

Elektrik Mühendisliği Programı

Tez Danışmanı: Prof. Dr. Veysel Murat İstemihan GENÇ

ARALIK 2023

ISTANBUL TECHNICAL UNIVERSITY ★ GRADUATE SCHOOL

DETECTION OF FALSE DATA INJECTION ATTACKS ON AUTOMATIC GENERATION CONTROL SYSTEMS WITH BAGGED TREES ALGORITHM

M.Sc. THESIS

Atakan OZTURK

(504191059)

Department of Electrical Engineering

Electrical Engineering Programme

Thesis Advisor: Prof. Veysel Murat Istemihan GENC

DECEMBER 2023

İTÜ, Lisansüstü Eğitim Enstitüsü'nün 504191059 numaralı Yüksek Lisans Öğrencisi Atakan ÖZTÜRK, ilgili yönetmeliklerin belirlediği gerekli tüm şartları yerine getirdikten sonra hazırladığı "OTOMATİK ÜRETİM KONTROLÜ SİSTEMLERİNE YAPILAN YANLIŞ VERİ ENJEKSİYON SALDIRILARININ TORBALAMA AĞAÇLARI ALGORİTMASI İLE TESPİTİ" başlıklı tezini aşağıda imzaları olan jüri önünde başarı ile sunmuştur.

Tez Danışmanı : **Prof. Dr. Veysel Murat İstemihan GENÇ** .....
İstanbul Teknik Üniversitesi

Jüri Üyeleri : **Prof. Dr. Emine AYAZ** .....
İstanbul Teknik Üniversitesi

Dr. Öğr. Üyesi Oben DAĞ .....
İstanbul Arel Üniversitesi

Teslim Tarihi : 27 Kasım 2023
Savunma Tarihi : 26 Aralık 2023

Aileme,

ÖNSÖZ

Öncelikle, yüksek lisans öğrenimim boyunca verdiği desteklerinden ve kattığı vizyondan ötürü, geleceğe daha emin adımlarla ilerlememi sağlayan değerli danışmanım Prof. Dr. V. M. İstemihan GENÇ'e teşekkürlerimi sunarım.

Ayrıca siber güvenlik alanındaki uzmanlığı ve bu uzmanlığını benimle paylaşarak çalışmanın ilerlemesine verdiği katkılarından dolayı Dr. Mohammadpourfard'a çok teşekkür ediyorum.

Hayatımın her anında beni destekleyen ve motive eden sevgili eşim Ceren'e, aynı zamanda hep yanımda olan aileme sonsuz teşekkür ediyorum.

Aralık 2023

Atakan Öztürk

(Elektrik-Elektronik Mühendisi)

İÇİNDEKİLER

Sayfa

KISALTMALAR

ACE	**:** Alan Kontrol Hatası
BT	**:** Torbalama Ağaçları
CART	**:** Sınıflandırma ve Regresyon Ağaçları
CDBN	**:** Koşullu Derin İnanç Ağı
DNP3	**:** Dağıtılmış Ağ Protokolü
FDI	**:** Yanlış Veri Enjeksiyonu
FFNN	**:** İleri Beslemeli Sinir Ağları
FN	**:** Yanlış Negatif
FÖB	**:** Fazör Ölçüm Birimi
FP	**:** Yanlış Pozitif
GDB	**:** Regülatör Ölü Bandı
GPS	**:** Küresel Konumlama Sistemi
GRC	**:** Üretim Oranı Kısıtlamaları
ICCP	**:** Kontrol Merkezleri Arası İletişim Protokolü
IED	**:** Akıllı Elektronik Cihaz
KA	**:** Karar Ağaçları
k-NN	**:** k-En Yakın Komşular
LSTM	**:** Uzun-Kısa Süreli Bellek
MITMA	**:** Ortadaki Adam Saldırısı
MLP	**:** Çok Katmanlı Algılayıcılar
OFGS	**:** Aşırı Frekans Üretim Atma
OÜK	**:** Otomatik Üretim Kontrolü
PCA	**:** Temel Bileşenler Analizi
PI	**:** Oransal İntegral
RBM	**:** Kısıtlı Botzman Makineleri
RED	**:** Rüzgar Enerjisi Dönüştürme
RES	**:** Rüzgar Enerjisi Sistemleri
RNN	**:** Tekrarlayan Sinir Ağı

ROCOF : Frekans Değişim Oranı
RTU **:** Uzak Terminal Birimi
SCADA **:** Merkezi Kontrol ve Veri Toplama Sistemi
SE **:** Durum Tahmini
SVM **:** Destek Vektör Makineleri
TD **:** Zaman Gecikmesi
TN **:** Doğru Negatif
TP **:** Doğru Pozitif
UFLS **:** Düşük Frekans Yük Atma
YSA **:** Yapay Sinir Ağları

SEMBOLLER

$\mathbf{T_R}$: Transdüser zaman sabiti

$\mathbf{T_A}$: AVR zaman sabiti

$\mathbf{T_E}$: Uyartım zaman sabiti

$\mathbf{T_F}$: Geri besleme zaman sabiti

$\mathbf{K_A}$: AVR kazanç sabiti

$\mathbf{K_E}$: Uyartım kazanç sabiti

$\mathbf{K_F}$: Geri besleme kazanç sabiti

$\mathbf{\Delta f}$: Frekans sapması

$\mathbf{\Delta P_m}$: Mekanik güç değişimi

$\mathbf{H}$: Atalet sabiti

$\mathbf{D}$: Yük sönümleme katsayısı

$\mathbf{\Delta P_V}$: Buhar valfi konum değişimi

$\mathbf{\Delta P_{ref}}$: Ayarlı referans güç

$\mathbf{\Delta P_g}$: Karşılaştırıcı çıkışı

$\boldsymbol{\tau_g}$: Regülatör zaman sabiti

$\boldsymbol{\tau_t}$: Türbin zaman sabiti

$\boldsymbol{\delta}$: Güç açısı

$\mathbf{X}$: Hat reaktansı

$\mathbf{V}$: Gerilim

$\mathbf{P_s}$: Senkronize tork katsayısı

$\mathbf{y}$: Toplam kontrol alanı sayısı

$\mathbf{K}$: Oransal integral sabiti

$\mathbf{V_L}$: Valf açma-kapama alt sınırı

$\mathbf{V_U}$: Valf açma-kapama üst sınırı

$\mathbf{e^{-st}}$: Üstel zaman gecikme fonksiyonu

$\mathbf{\Delta t}$: Gecikme süresi

$\mathbf{T_1}$: Aktarma noktası zaman sabiti

$\mathbf{T_2}$: İkinci ara ısıtıcı zaman sabiti

$\mathbf{T_3}$: İlk ara ısıtıcı zaman sabiti

$\mathbf{T_4}$: Buhar hanesi zaman sabiti

$\mathbf{K_1}$: Düşük basınç türbini güç yüzdesi

$\mathbf{K_2}$: Orta basınç türbini güç yüzdesi

$\mathbf{K_3}$: Yüksek basınç türbini güç yüzdesi

$\mathbf{K_4}$: Çok yüksek basınç türbini güç yüzdesi

$\mathbf{K_p}$: Regülatör kazancı

$\mathbf{D_z}$: Ölü band

$\mathbf{T_{sr}}$: Hız rölesi zaman sabiti

$\mathbf{T_{sm}}$: Servo motor zaman sabiti

$\mathbf{v_g}$: Kapakçık açılma hızı

$\mathbf{g}$: Kapakçık açılma limiti

$\mathbf{P_{m0}}$: Türbin başlangıç gücü

$\mathbf{T_r}$: Alçak geçiren filtre zaman sabiti

$\mathbf{V_{T0}}$: Terminal gerilimi başlangıç değeri

$\mathbf{V_{F0}}$: Alan gerilimi başlangıç değeri

$\mathbf{X_l}$: Sızıntı reaktansı

$\mathbf{R_s}$: Stator direnci

$\mathbf{X_d}$: Senkron boyuna reaktans

$\mathbf{X'_d}$: Geçici boyuna reaktans

$\mathbf{X''_d}$: Hızlı geçici boyuna reaktans

$\mathbf{X_q}$: Senkron enine reaktans

$\mathbf{X'_q}$: Geçici enine reaktans

$\mathbf{X''_q}$: Hızlı geçici enine reaktans

$\mathbf{T'_{d0}}$: Boyuna eksenin açık devre geçici zaman sabiti

$\mathbf{T''_{d0}}$: Boyuna eksenin açık devre hızlı geçici zaman sabiti

$\mathbf{T'_{q0}}$: Enine eksenin açık devre geçici zaman sabiti

$\mathbf{T''_{q0}}$: Enine eksenin açık devre hızlı geçici zaman sabiti

$\mathbf{R}$: Rüzgar türbini kanat uzunluğu

$\mathbf{p}$: Hava yoğunluğu

v_w : Rüzgar hızı

$\mathbf{C_p}$	: Kanat güç katsayısı
$\mathbf{B}$	: Kanat açısı
$\boldsymbol{\lambda}$	: Uç hız oranı
$\mathbf{k_{tg}}$	: Aktarma organı mil sertlik değeri
$\mathbf{c_{tg}}$	: Aktarma organı sönümleme katsayısı
$\boldsymbol{\omega_{elB}}$	: Elektriksel baz hız
$\mathbf{T}$	: Tork
$\boldsymbol{\omega}$	: Dönme hızı
$\boldsymbol{\theta_{tg}}$	: Şaft burulma açısı
$\boldsymbol{\lambda_s}$	: Ölçekleme saldırısı parametresi
$\boldsymbol{\lambda_r}$	: Rampa saldırısı parametresi
$\boldsymbol{\beta}$	: Frekans bias değeri
$\boldsymbol{\Delta P_{tie}}$	: Bağlantı hattı güç akışı sapması
$\boldsymbol{\psi}$	: ACE sinyali maksimum eğimi
$\mathbf{z}$	: Ölçüm vektörü
$\mathbf{z_a}$	: Saldırılmış ölçüm vektörü
$\mathbf{w}$	: Ağırlık vektörü
$\boldsymbol{\gamma}$	: Öğrenme oranı
$\mathbf{b}$	: Bias değeri
$\boldsymbol{\zeta}$	: Ayarlanabilir regülirizasyon parametresi
$\boldsymbol{\xi_i}$	: Ayrılabilen nonlineer eğitim seti için gevşek değişken
$\mathbf{M_{Tr}}$	: Özellik vektörü
$\mathbf{y_i}$	: Tahmin edilen sınıf etiketi
$\mathbf{k}$	: En yakın komşu sayısı

ÇİZELGE LİSTESİ

Sayfa

ŞEKİL LİSTESİ

Sayfa

OTOMATİK ÜRETİM KONTROLÜ SİSTEMLERİNE YAPILAN YANLIŞ VERİ ENJEKSİYON SALDIRILARININ TORBALAMA AĞAÇLARI ALGORİTMASI İLE TESPİTİ

ÖZET

Yükselen dünya nüfusu nedeniyle enerji talebi de giderek artmaktadır. Ayrıca fosil yakıt rezervlerinin azalması, enerji kaynaklarının çeşitlendirilmesi ve verimliliğinin arttırılması gerekliliğini ortaya çıkarmaktadır. Enerji üretiminin talep tarafı da dikkate alınarak planlanması ve kontrol edilmesi, verimliliğinin arttırılması açısından gereklidir. Otomatik Üretim Kontrolü (OÜK), güç üretimi ve tüketimi arasındaki dengeyi koruyarak güç sistemi frekansını belirli sınırlar arasında tutar. Bu sayede enerji verimliliğinin arttırılmasına katkıda bulunur. Öte yandan enerji kaynaklarını çeşitlendirmek için yenilenebilir enerji kaynaklarına doğru yapılan kademeli geçiş, güç sistemi dinamiklerini etkilemekte; kontrol, işletme ve siber güvenlik açısından bir kısım zorlukları beraberinde getirmektedir. İşletme koşullarına getirdikleri belirsizlikler, işletme planlaması ve kontrolü açısından yeni yaklaşım ve yöntemlere olan ihtiyacı arttırmaktadır. Yenilenebilir enerji kaynaklarının sistemin eylemsizliğini azaltması ve değişkenlik katması da bu ihtiyacı arttırmaktadır. Öte yandan akıllı şebeke kavramıyla birlikte artan haberleşme ağları nedeniyle şebeke siber saldırılara karşı savunmasız kalmaktadır. Ek olarak şebekeye olan bağlantı sayısının artması, değişken üretim nedeniyle kestirim, talep tarafı yönetim, daha ileri kontrol ve izleme ihtiyacının olması dolayısıyla güç sistemlerinin siber güvenlik ihtiyacı artmaktadır.

OÜK sistem davranışının büyük sapmalar için doğru olarak değerlendirilmesi ve tasarımların buna göre yapılabilmesi için OÜK sistemi bileşenlerindeki doğrusal dışılığının dikkate alınması gerekir. Diğer bozucu etkiler için olduğu gibi Yanlış Veri Enjeksiyon (FDI) saldırılarının gerçek sistem davranışına etkisinin değerlendirilmesi için modellerimizde lineer olmayan durumlar hesaba katılmaktadır. Daha önceki çalışmalarda fazla dikkat edilmeyen Üretim Oranı Kısıtlamaları (GRC), Regülatör Ölü Bandı (GDB) ve Zaman Gecikmeleri (TD) gibi OÜK sistemindeki lineer olmayan durumların etkileri incelenmiştir. Bu çalışmada ilk olarak OÜK'nin siber güvenliği incelenmekte ve doğrusal olmama durumlarının ihmal edilemeyeceği gösterilmektedir.

Elektrik güç sistemindeki iletim hatlarının ölçülen frekans ve güç akış değerleri, jeneratör çıkışını ayarlamak için kullanılan Alan Kontrol Hatası (ACE) değerinin hesaplanması için kontrol merkezine gönderilmektedir. İletişim sistemlerine olan bu bağımlılık, OÜK'yi siber-fiziksel saldırılara karşı savunmasız bırakmaktadır. Veri iletişimi için kullanılan Kontrol Merkezleri Arası İletişim Protokolü'nde (ICCP) güvenlik açıkları bulunmaktadır. Saldırganlar, sisteme siber saldırılar başlatmak için bu güvenlik açıklarından yararlanabilmektedir. FDI saldırıları, davranışını manipüle etmek için, kontrol sistemine yanlış sensör ölçümleri enjekte etmeyi içermektedir.

İkinci olarak, bu yazıda çoklu siber saldırıların saldırı modeli ve etkisi incelenmektedir. Çoklu FDI saldırıları, aynı anda birden fazla sensöre yanlış ölçümler enjekte etmeyi içerirken, tekli FDI saldırıları, tek bir sensöre yanlış ölçümler enjekte etmeyi içermektedir. Çoklu FDI saldırıları, sistemi daha hızlı yük atma sıklığına yönlendirebildikleri ve saldırı parametrelerinin seçim aralığı daha geniş olduğu için, saldırının ciddiyeti ve tespit edilebilirliği açısından tekli FDI saldırılarından daha etkili olmaktadırlar. Başka bir katkı olarak, bu tez, güç sisteminde bulunan Rüzgar Enerjisi Sistemleri (RES) oranına göre çoklu saldırı sınıflandırmasında dört farklı algoritmanın karşılaştırılmasını içermektedir. Sonuç olarak bir siber saldırının etkisi RES oranı arttıkça daha da ağırlaşmaktadır.

Üçüncü olarak, bu tehditlere karşı korunmak için Torbalama Ağaçları (BT) algoritmasına dayalı bir tespit şeması önerilmektedir. Önerilen bu algoritma veri tabanlı olmakla birlikte, bu sayede OÜK'nin doğrusal dışılığı ile parametre belirsizliklerinden, geleneksel tespit şemalarına göre daha az etkilenmesini sağlamaktadır. Bu çalışma önemlidir, çünkü diğer çalışmalarda üzerine fazla düşülmeyen OÜK doğrusal dışılıklarının sisteme dahil edilmesi ve RES entegresi ile daha gerçekçi bir model oluşturulmaktadır. Ayrıca çoğu siber saldırı tespit algoritmalarının yaptığı saldırı var veya yok gibi ikili sınıflandırma yapmak yerine, saldırının yapıldığı OÜK ölçüm biriminin tespit edilmesini de sağlayan çoklu bir sınıflandırma algoritması ile farklılık oluşturmaktadır.

BT algoritması, OÜK sistemindeki FDI saldırılarını sınıflandırmada daha önce kullanılmamıştır. Bu nedenle FDI saldırılarının çoklu sınıflandırma işleminde BT algoritmasının kullanılması farklı bir bakış açısı oluşturmaktadır. Tüm çalışmalar, MATLAB/Simulink ortamında iki alanlı test sistemi kullanılarak oluşturulan OÜK sistemi üzerinde test edilmektedir. Bu tezden elde edilen sonuçlar, saldırı tespit modelinin doğruluğunu ve tehdit altındaki ölçümleri algılama yeteneğini doğrulamaktadır. Önerilen algoritma artan RES oranına göre siber saldırıları sınıflandırmada umut verici bir doğruluk elde etmekte, özellikle en tehlikeli yanlış alarm olan saldırı varken yok olarak tahmin edilmesi durumunu en az veren algoritma olmaktadır. BT algoritmasının; artan RES oranına göre en esnek algoritma olması, düşük hesaplama maliyeti, eğitim prosedürünün sağladığı rastlantısallık nedeniyle aşırı öğrenme sorunlarını hafifletmesi ve saldırıları yüksek doğrulukla sınıflandırabilmesi sebebiyle OÜK sistemlerine yapılan FDI saldırılarının tespit edilmesinde kullanılabilecek bir algoritma olduğu kanıtlanmaktadır.

DETECTION OF FALSE DATA INJECTION ATTACKS ON AUTOMATIC GENERATION CONTROL SYSTEMS WITH BAGGED TREES ALGORITHM

SUMMARY

Energy demand is increasing due to the rising world population. In addition, the depletion of fossil fuel reserves necessitates the diversification of energy resources and the need to increase their efficiency. Planning and controlling energy production by taking into account the demand side is necessary to increase its efficiency. Automatic Generation Control (AGC) keeps the power system frequency within certain limits by maintaining the balance between power generation and consumption. In this way, it contributes to increasing energy efficiency. On the other hand, the gradual transition towards renewable energy sources to diversify energy sources affects power system dynamics and brings some challenges in terms of control, operation and cyber security. The uncertainties they bring to operating conditions increase the need for new approaches and methods for operational planning and control. The fact that renewable energy sources reduce the inertia of the system and add variability also increases this need. On the other hand, due to the increasing number of communication networks with the smart grid concept, the grid is vulnerable to cyber-attacks. In addition, the need for cyber security of power systems increases due to the increasing number of connections to the grid, the need for forecasting, demand-side management, more advanced control and monitoring due to variable generation.

In order to accurately assess the AGC system behavior for large deviations and to design accordingly, the nonlinearity of the AGC system components must be taken into account. As for other disturbances, we account for nonlinearities in our models to evaluate the impact of False Data Injection (FDI) attacks on the actual system behavior. We investigate the effects of nonlinearities such as Generation Rate Constraints (GRC), Governor Dead Band (GDB) and Time Delays (TD) in the AGC system, which have not received much attention in previous studies. In this paper, we first analyze the cybersecurity of AGC and show that nonlinearities cannot be neglected.

The measured frequency and power flow values of the transmission lines in the electric power system are sent to the control center for the calculation of the Area Control Error (ACE) value used to adjust the generator output. This dependence on communication systems leaves the AGC vulnerable to cyber-physical attacks. There are vulnerabilities in the Inter-Control Center Communication Protocol (ICCP) used for data communication. Attackers can exploit these vulnerabilities to launch cyber attacks on the system. FDI attacks involve injecting false sensor measurements into the control system to manipulate its behavior. Multiple FDI attacks involve injecting false measurements into multiple sensors simultaneously, while single FDI attacks involve injecting false measurements into a single sensor.

Secondly, in this paper, we study the attack model and impact of multiple cyber attacks. It is also shown that nonlinearities in the AGC system can lead to slower response times and larger frequency deviations in the presence of FDI attacks. Multiple FDI attacks are more effective than single FDI attacks in terms of attack severity and detectability, as they can drive the system to faster load shedding frequency and the selection range of attack parameters is wider. As another contribution, this thesis compares four different algorithms, namely Decision Trees (DT), k-Nearest Neighbors (k-NN), Artificial Neural Networks (ANN) and Bagging Trees (BT) algorithms, for multiple attack classification based on the proportion of Wind Energy Systems (WES) in the power system. In order to increase the realism of the RES system, the wind speed is generated to fluctuate randomly instead of a constant value. As a result, the impact of a cyber attack becomes more severe as the RES rate increases.

Third, a detection scheme based on the BT algorithm is proposed to protect against FDI attacks targeting the AGC system. This proposed algorithm is data-driven and ensures that the AGC is not affected by nonlinearities and parameter uncertainties. This study is important because it provides a more realistic model with the inclusion of the nonlinearities of the AGC and the integration of the WES, which has not been emphasized in other studies. In addition, instead of the binary classification such as attack or no attack that most cyber intrusion detection algorithms do, it has created a difference with a multiple classification algorithm that also enables the detection of the AGC measurement unit where the attack is made. In this way, it is aimed to fill the gaps in the literature. In order to develop data-driven detection algorithms, the data set and this data must be labeled. For the cyber-attack detection algorithms generally used, a binary classification problem is considered as class 1 if there is an attack and class 0 if there is no attack. In this thesis, four different classes are identified and labeled accordingly: attack on area 1 frequency, attack on area 2 frequency, attack on tie-line power and no attack. The learning dataset is a set of measurements and a collection of data where each sample is represented by a label. For this problem, various unpredictable scenarios about the system should be included in the dataset, such as the operating conditions before the attack and the uncertainties involved in the contingency. In other words, scenarios such as load of the power system under normal operating conditions, the renewable energy source integration rate, and in case of an attack; the attack parameter size, duration, and the measurement of the attack should be included in the dataset. For this reason, while creating the data set, situations that do not involve cyber-attacks are divided into three as load change within the area, load change in the neighboring area, load change in both areas. In addition, four different attack patterns, namely ramp attack, scaling attack, constant value attack and flip attack, were applied to the system with different parameter values.

In this thesis, it is proved that each attack can target different measurement and control points and each attack has a different impact on the system. For this reason, a multi-classification algorithm is proposed in this study that not only detects the presence of an attack, but also the value of the attacked measurement. As a result, a data set was created with 100 different scenarios and 98565 samples. Under the same conditions, WES were added to the two-area power system with 10% and 20% of the total power. Two more data sets were created according to this increased WES ratio. With these three data sets, it is aimed to examine the effect of increasing WES ratio on the performance of intrusion detection algorithms. In this way, it is aimed to fill another gap in the literature.

The classifier structure of the proposed BT algorithm is built by combining multiple decision trees. First, the dataset is resampled with random samples. Each bag is randomly selected from the dataset. A separate decision tree is created for each dataset. The decision trees use the features f_1, f_2, ACE_1, ACE_2 and p_{tie} in the dataset to classify the data. Each classifier runs independently on the sampling data used in the classifier training. The classification results of all decision trees are combined and the final decision is made by majority voting. That is, the class labels given by each classifier are counted and the most predicted class label is selected as the class label predicted by the Bagging Trees. Bagging Trees combine multiple decision trees to form an ensemble model. Each decision tree is trained with different data samples, thus providing diversity. This contributes to more reliable results for the detection of attacks and normal situations. In addition, the proposed algorithm works in parallel. This means that each decision tree works independently, which speeds up the training and prediction process. Due to the structure of ensemble learning algorithms, if one decision tree makes a mistake, the other decision trees compensate for this result, reducing the risk of error. For the training of the proposed Bagging Trees, the decision tree was selected as the learner type and the number of learners was set to 30.

The Bagging Trees algorithm has not been used before to classify FDI attacks in the AGC system. Therefore, the use of the BT algorithm in the multi-classification process of FDI attacks constitutes a different perspective. All the work was tested on the AGC system built using a two-area test system in MATLAB/Simulink environment. The results obtained from this thesis confirm the accuracy of the intrusion detection model and its ability to detect threatened measurements. The intrusion detection rates of all algorithms decreased as the WES integrated into the system increased. The ANN algorithm and the BT algorithm are the two most successful algorithms according to the increasing WES ratio. The most difficult attack to detect for this AGC system was the attack on the power of the tie-line. All four algorithms mostly misclassified the attacks on this point. The proposed BT algorithm for the detection of cyber-attacks on AGC systems achieved a good performance with an accuracy of 0.920-0.871-0.855 at 0-10-20% WES rates, respectively. The ANN, on the other hand, has an accuracy rate of 0.924-0.889-0.814 at 0-10-20% RES rates, respectively. The ANN, which has the most dangerous false alarm, the rate of predicting no attack when there is an attack, which is 0.7-0.7-1.8% when there is 0% WES integration, increased to higher rates as the WES rate increased. For the BT algorithm, the increase in WES increased this false alarm to a relatively small extent. Even at 20% WES, the most dangerous false alarm rate of the BT algorithm was 2.0-2.4-2.8%.

As a result, the proposed BT algorithm was the most successful in the most dangerous false alarm case. The BT algorithm is faster than ANN because the decision trees work independently and parallel computations are performed. This facilitates real-time detection of attacks on the AGC system. As a result, the proposed methodology can be justified as a viable option for multiple classification of FDI attacks on AGC systems. The proposed algorithm achieved a promising accuracy in classifying cyber-attacks with increasing WES, especially in the most dangerous false alarm case of predicting no attack when there is one. The BT algorithm is proved to be the most flexible algorithm for detecting FDI attacks on AGC systems as it is the most flexible algorithm for increasing WES, has low computational cost, mitigates overfitting problems due to the randomness of the training procedure, and can classify attacks with high accuracy.

1. GİRİŞ

Bir elektrik güç sisteminde enerji üretiminin planlanması ve kontrolü şebekenin günlük çalışmasındaki en önemli bileşenlerden biridir. Üretim ve tüketim arasında meydana gelen bir dengesizlik güç sistemini kararsız duruma sürükleyebilir. Bu tür bir olay güç sistemi frekans kontrolü sorunu olarak düşünülmelidir. Frekans sapmasının kalıcı olması durumunda ekipmanlar zarar görebilir, yük performansı düşebilir, iletim hatları aşırı yüklenebilir ve koruma cihazları tetiklenebilir. Bunların sonucunda ise güç sisteminin çalışması doğrudan etkilenir.

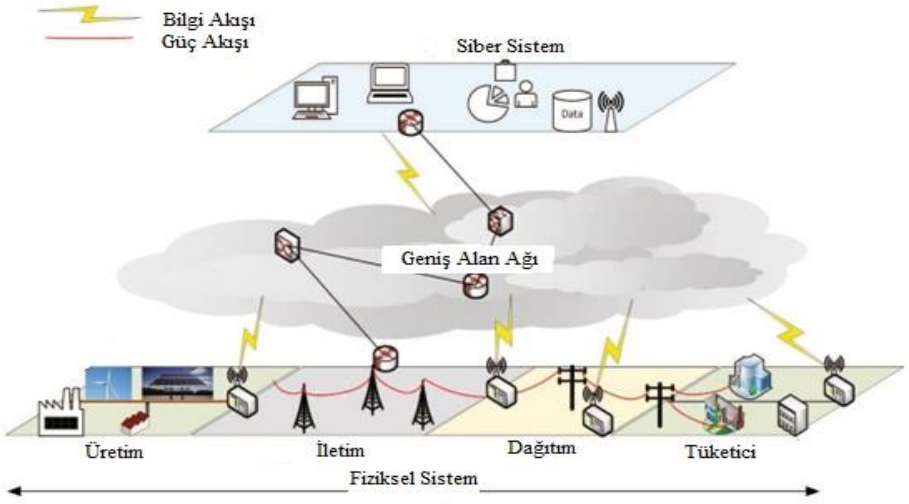
Elektrik güç sistemleri ekonomik ve güvenilir çalışmayı sağlamak için birbirleri ile bağlantılıdır. Bu enterkonnekte yapı, her biri kendi içinde hedefleri ve çalışma koşulları olan bir veya iki elektrik şirketinin yer aldığı kontrol alanlarına bölünür. Çok alanlı bir güç sistemi yüksek gerilim iletim hatları veya bağlantı hatları ile birbirine bağlanan alanları içerir. Bu kontrol alanlarının sorumluluklarından biri kendi alanındaki tüketicilerin yük talebini karşılayacak şekilde gerekli üretimi sağlamak veya diğer kontrol alanlarından tedarik etmektir. Elektrik şebekesinde üretilen frekans, jeneratörün dönüş hızı ile orantılı olduğundan enterkonnekte bir sistemin frekansında değişiklik olduğu zaman sistemdeki tüm jeneratörler hız regülatör kontrolü aracılığıyla frekanstaki değişikliklere yanıt verir. Çok alanlı bir güç sisteminin herhangi bir alanında yükün artması durumunda, türbin jeneratörlerinin dönen kütlelerinde depolanan kinetik enerji ilk anda bu yükü karşılar. Fakat daha sonra şebeke frekansında oluşan düşüş tüm enterkonnekte sistem boyunca gözlenir. Jeneratörler üretimi ayarlayarak frekansın yeni kararlı duruma gelmesini sağlarlar bu sayede tüm sistemdeki toplam üretim ve toplam tüketim arasında tekrar denge kurulur.

Güç sistemleri, Merkezi Kontrol ve Veri Toplama Sistemi (SCADA) tarafından izlenir ve kontrol edilir. Güç sistemlerinin ve SCADA sistemlerinin siber-fiziksel etkileşimi güvenlik sorunlarını arttırır. Bu açıklıklardan faydalanan siber saldırganlar durum tahmincisi (SE) işlemini aldatacak yanlış verileri güç sistemine enjekte edebilir.

Otomatik Üretim Kontrolü (OÜK) algoritması, tamamen otomatik olan tek geniş alanlı kontrol uygulamasıdır, yani kontrol kararları vermek için döngüde insan kararı yoktur. Bu nedenle, saldırganlar yanlış bilgi enjekte ederek ölçümlerin bozulmasını ve ACE sinyalinin yanlış hesaplanması sonucu gereksiz eylemlerin oluşmasını sağlar.

1.1 Güç Sistemlerinin Mimarisi

Şekil 1.1 siber-fiziksel güç sisteminin çalışması ve kontrolü hakkında genel bir bakış sunar. Güç Sistemi, (i) Üretim sistemi (ii) İletim sistemi (iii) Dağıtım sistemi olmak üzere üç ana bileşenden oluşur. Geleneksel güç sistemi, tüketicilerin ihtiyaç duyduğu elektriğin üretildiği ve kullanıcıların tüketebileceği gerilime ayarlanarak dağıtım hatları aracılığıyla tüketicilere sunulduğu bir sistem olarak özetlenebilir. Üretim sistemi, gerekli gücü şebekeye enjekte eden kömür, nükleer ve hidro gibi enerji santrallerini içerir. İletim sistemi, üretilen gücü kaynaktan dağıtım ağlarına taşıyan iletim hatlarını ve kapasitör bankları gibi kararlılıkla ilgili diğer elemanları içerir. Tipik olarak radyal olan ve 33 kV ve altındaki voltajlarda çalışan dağıtım şebekesi, son müşterilere bireysel ve endüstriyel yükler şeklinde güç sağlamaktan sorumludur. İletim hatları, iletim sürecindeki güç kaybının azaltılması ve gücü üretim istasyonundan dağıtım trafo merkezlerine daha yüksek voltajlarda taşımak için kullanılır. Daha sonra güç, dağıtım trafo merkezlerinden basitçe dağıtım sistemi olarak adlandırılan son kullanıcılara aktarılır.



Şekil 1.1: Akıllı şebeke siber-fiziksel sistem[1].

1.1.1 Geleneksel güç sistemleri

Günümüz standartlarına göre geleneksel güç sistemi eski kalmıştır ve yeniden yapılandırılması gerekmektedir. Ayrıca, nüfus yoğunluğunun artması beraberinde yükselen bir enerji talebi sorununu ortaya çıkarmaktadır. Artan enerji talebi ve eskiyen ekipman nedeniyle zorlanan elektrik güç sistemi, kesintilere daha yatkın hale gelmektedir. Bu nedenle, enerji sistemimizin modernizasyonuna ihtiyaç duyulmaktadır. Artan talepleri karşılamak için iletim-dağıtım sistemine yapılan yetersiz yatırımlar ve enerjiyi kesikli olarak üreten yenilenebilir enerji sistemlerinin şebekeye eklenmesi, geleneksel güç sistemini büyük kırılganlıklarla karşı karşıya bırakmaktadır.

Geleneksel güç üretim tesisleri topluluklar etrafında kümelenmiş ve inşa edilmiştir, bu nedenle elektriği uzak bölgelere ulaştırabilmek, dağıtım altyapısının (iletim ve dağıtım hatları) kapasitesi için gelecekteki ihtiyaçları tahmin etme yeteneğimizi zorlamaktadır. Kurulan şebeke elemanları çoğu durumda mevcut talepten ziyade geçmişteki enerji taleplerini karşılamak için tasarlanmıştır. Ek olarak gün içerisinde dalgalanan güç talebi en yüksek değerine ulaşması, mevcut şebeke altyapısı için zorlayıcı olabilmektedir.

Geleneksel elektrik güç sistemlerinde enerji ve iletişimin yönü üretim kaynağından tüketiciye olmak üzere tek yönlüdür. Bunun sonucunda ise, geleneksel elektrik şebekesinin artan enerji taleplerine uyum sağlayamayacağı, şebeke arızalarını tespit etmede zorluklarla karşılaşabileceği, elektriği kendiliğinden yeniden yönlendiremeyeceği ve elektrik hatlarının potansiyel olarak aşırı ısınmasıyla (yine enerji kaybı veya israfı) karşı karşıya kalabileceği anlamına gelmektedir. Ayrıca elektrik akışının izlenmesi manuel olarak yapılmak zorundadır. Bu sorunların çözülebilmesi için mevcut elektrik şebekesinin daha akıllı ve uyarlanabilir olacak şekilde güncellenmesi önem arz etmektedir. Bu nedenle akıllı şebeke kavramı ortaya çıkmıştır ve akıllı şebekelerin yaygınlaşması ile birlikte bu sorunların çözüme kavuşacağı düşünülmektedir.

1.1.2 Modern güç sistemleri

Nüfusun artması ile birlikte elektrik talebi de giderek artmaktadır. Geleneksel güç sistemleri ve kurulu ekipmanlarının yetersiz gelmesi nedeniyle ilk amaç, talep tarafındaki yönetimin iyileştirilmesidir. İkinci amaç ise, geleneksel güç sistemlerinin

kullandığı fosil yakıt rezervlerinin azalması ve bu fosil yakıtların yanması sonucu ortaya çıkan sera gazı emisyonlarının çevreye verdiği zarar nedeniyle, fosil enerji kaynakları yerine yenilenebilir enerji kaynaklarına geçilerek enerji verimliliği çalışmalarının hızlandırılmasıdır. Son olarak doğal afetler ve siber saldırganlara karşı daha güçlü, güvenli, kendi kendine düzelebilen bir elektrik şebekesi oluşturulması amaçlanmaktadır. Öte yandan modern şebeke terimi, bir anda geleneksel şebekenin tamamen ortadan kaldırılıp yerine yeni teknoloji ve ekipmanların getirilmesi fikri yerine akıllı şebekenin geleneksel şebekeye bir güncelleme ve iyileştirme getirmesi fikrini taşımaktadır. Akıllı şebeke kavramı kademeli olarak devreye alınabilen önemli iyileştirmeler sunmaktadır. Ekipman ve teknolojinin değişimi kademeli olarak ilerlese bile enerji kullanımımızda zamanla bazı büyük değişiklikler olacağı düşünülmektedir.

Sonuç olarak akıllı şebekeler, mevcut teknolojilerin güncelleştirilmiş ve geliştirilmiş olan akıllı versiyonlarını içerecektir. Modern şebekeler geleneksel şebekelere dayanacak fakat içerisinde "Geniş Alan İzleme ve Koruma", "Mikro Şebekeler", "Akıllı Ölçüm Cihazları" ve "Sanal Enerji Santralleri" gibi yeni sistemler de yer alacaktır. Fakat temel güç üretim sistemleri üretimde önemli bir rol oynayacaktır. Bunlarla birlikte tüketicilerin de enerji üretimi yapabileceği gibi sistemin üretimi, iletimi, dağıtımı ve işletiminde çok daha fazla aktör olacaktır.

1.2 SCADA Sistemlerinin Mimarisi

SCADA farklı kaynaklardan veri toplayan, bunları işleyen, farklı kullanıcılar ve uygulamalar tarafından erişilebilen bir veritabanında bu bilgileri saklayan bir sistemdir. SCADA, günümüzün güç sisteminin işletimi ve kontrolü için çok önemlidir. Ek olarak kontrol merkezleri ve saha cihazları arasında izlenme ve kontrolün sağlanmasından da sorumludur.

Güç sisteminin fiziksel bileşenleri Akıllı Elektronik Cihazlara (IED) bağlıdır ve bu cihazlar sensörler ile eyleyicilerin yaptığı işlemleri yerine getirebilirler. IED'ler programlanabildikleri için sistem operatörlerinin cihaz düzeyinde otomasyon ve mantıksal işlemleri yapmasına olanak tanırlar. Ayrıca IED'ler ilişkili oldukları Uzak Terminal Birimi'ni (RTU) güç sisteminin değişkenlerinin durumu hakkında bilgilendirirler. RTU'ların görevi IED'lerden gelen bilginin toplanmasıdır. RTU birimleri ise bu bilgileri kontrol merkezindeki SCADA sunucularına iletir. Son olarak

sistem operatörü uygulama sunucularında işlenmiş olarak karşısına gelen bilgi sonrasında uygun kontrol eylemini belirler. Bu kontrol mesajı daha sonra uygun RTU aracılığıyla IED'lerdeki eyleyicilere iletilir. Uygulamada, yardımcı programlar, bakım ve yükseltme amaçları için satıcılara uzaktan erişim yetenekleri sağlar ve piyasa operasyonları için enerji kuruluşlarının şirket ofislerine de benzer erişim yetenekleri sağlanır. Yukarıda anlatılan bu bağlantılar potansiyel olarak kötü niyetli siber saldırganlar tarafından SCADA altyapısına erişim elde etmek ve bu sayede güç sisteminin güvenilirliğini tehlikeye atmak için kullanılır.

1.3 Problemin Belirlenmesi ve Literatür Taraması

Elektriğin tüketicilere iletimi ve dağıtımı dünya çapında sürdürülebilir kalkınma ve refah için temel bir gerekliliktir. İletilen elektriğin kaliteli ve güvenilir bir şekilde sağlanması ve güç sisteminin kararlı çalışması için çeşitli kontrol teknikleri gereklidir. Güç sisteminin kararlı olarak çalışmasını sürdürebilmesi için frekans, rotor açısı ve gerilim değerleri kontrol edilmelidir. Gerilim kontrolü, gerilimi ve reaktif gücü belirli sınırlar içinde tutarak güç sistemlerinin verimliliğini arttırır. Frekans kontrolünün amacı ise aktif güç ile frekansın belirli değerler içerisinde tutulmasıdır.

Öte yandan enerji sektörü, büyüyen elektrik şebekesi nedeniyle bağlantı sayısının artması, haberleşme ağlarının genişlemesi ve akıllı cihaz sayısının artması ile birlikte siber saldırılara daha açık hale gelmektedir. Elektrik şebekesinin siber saldırılara daha açık hale gelmesine, 23 Aralık 2015 tarihinde birkaç saat elektrik kesintisiyle sonuçlanan Ukrayna elektrik şebekesine yapılan saldırı örnek olarak verilebilir. Saldırı, temel olarak üçüncü şahısların Ukraynalı bölgesel bir elektrik şirketi olan Kyivoblenergo'nun SCADA sistemleri ve bilgisayarlarına girmesiyle gerçekleştirilmiştir. Başlangıçta 80.000 tüketicinin etkilendiği düşünülse de daha sonra saldırının eş zamanlı olarak 3 farklı enerji dağıtım şirketine yapıldığı ve çeşitli alanlarda elektriğe erişimi kesilen 225.000 tüketicinin etkilendiği ortaya çıkmıştır [2].

Yanlış Veri Enjeksiyon (FDI) saldırıları, güç sisteminin çalışmasını bozmak için yanlış verilerin sisteme aktarılması veya verilerin değiştirilmesi yoluyla yapılan siber saldırılardır. Bu saldırıların tespit edilmesi, güç sisteminin operasyonel güvenilirliğinin sağlanması için önemlidir. Saldırıların tespit edilmesi için farklı yöntemler önerilmiştir. FDI saldırılarının tespiti için genellikle sayaç ölçümlerinin

izlenmesi ve Durum Tahmincisi (SE) kullanılır [3]. OÜK sisteminde kullanılan tespit şemaları, elde edilen ölçümlerin kabul edilebilir aralıklarda olup olmadıklarını kontrol eden algoritmaları kullanır [4]. ISO/RTO seviyesinde her 5 dakikada bir çalışan SE gibi mevcut ölçüm değerlendirme teknikleri her 5 saniyede bir kontrol komutu vermesi gereken OÜK sistemi için kullanılamaz [5]. Aslında modern güç sistemleri, durum tahmini algoritmalarını daha hızlı çalıştıracak bilgi işlem ve veri toplama birimleri ile donatılmıştır. Bu sayede modern güç sistemlerinde kullanılan bu algoritmalar OÜK'ye gönderilecek verilerin güvenilirliğini arttırabilir [6]. Fakat durum tahmini algoritmalarını atlatacak yanlış veri enjeksiyon saldırıları da uygulanabilir. Bu saldırılar durum tahmini algoritmalarının ölçüm hatalarına karşı olan toleransından faydalanır [7]. Başarılı bir FDI saldırısı, durum tahmincisini atlatıp sistem operatörlerinin yanlış kararlar almasına, sistem cevabının tahmin edilemez ve kararsız olmasına neden olur. Bunların sonucu olarak da güç sisteminin ekonomik çalışmasını ve kararlılığını etkiler. Bu saldırılardan güç sistemini korumak oldukça önemlidir.

Bu saldırılara karşı önlemler korumaya yönelik yaklaşımlar ve tespite dayalı yaklaşımlar olarak ayrılmaktadır [8]. Terminal birimlerinin savunmasız olması güç sistemini bütünlük saldırılarına daha yatkın hale getirmektedir [9]. Bu nedenle bazı temel ölçüm birimlerinin korunması FDI saldırılarına karşı yapılabilecek savunma yöntemlerinden biri olarak gösterilmektedir. Liu ve arkadaşları, eğer saldırgan H sistem matrisini bilirse ve $k \geq m - n + 1$ tane sayaca müdahale edebilirse, z zararlı vektörünü sisteme tespit edilmeden enjekte edebileceğini göstermektedir [3]. Burada n durum değişkenleri m ise sayaçların sayısıdır. Bu nedenle bazı ölçüm setlerini korumak kritiktir. Güç sisteminde çok sayıda sayaç ve bunları korumak için kısıtlı bir bütçe olduğundan yazarlar minimum sayaç koruyarak optimum sonuç almak için çeşitli yaklaşımlar önerilmektedir [10-13]. Minimum sayaç koruması yönteminde saldırganlar eğer sistem hakkında tam bilgiye sahiplerse, maksimum güvenlik açığı ile minimum sayaç/sensör sayısının belirlenmesi için optimizasyon problemi çözerek ihlalde bulunabilmektedirler.

Fazör Ölçüm Birimi (FÖB) elektrik şebekesinde gerilim, akım ve faz açısını anlık olarak takip etmek için kullanılan Küresel Konumlama Sistemi (GPS) tabanlı bir cihazdır. GPS'ler ölçümlere zaman damgası vurarak saldırganlar tarafından ele geçirilmesini engeller. FÖB'ler FDI'lara karşı başarılıdır fakat FÖB'lerin kurulumu

maliyetlidir. Bu nedenle FÖB'lerin yaygın kullanımı zorlaşmaktadır. Ayrıca saldırganlar GPS sinyalini taklit ederek FÖB veri zaman damgalarını geçersiz kılabilecek saldırı vektörleri oluşturabilmektedirler [14].

Bir diğer koruma yöntemi ise oyun teorisi yöntemidir. Oyun teorisini kullanan yaklaşımlar açısından Wei ve arkadaşları saldırılardan korunma için stokastik tabanlı bir yaklaşım önerdiler [15]. Burada yazarlar optimum yük atma algoritmaları tasarlamışlardır. Yazarlar bu yaklaşımın FDI'lere karşı korumada etkinliğini kanıtladılar.

FDI saldırılarından koruma açısından başka oyun teorisi yöntemleri de önerilmiştir [16,17]. Bu yaklaşımların saldırılara karşı etkinlikleri kanıtlansa da oyun teorisi modeli, saldırganlar ve savunanlar arasındaki etkileşimi nedensel olaylar zinciri olarak modellediği için gerçekçi değildir [18].

Güç sistemini FDI'lardan korumak için şifreleme tabanlı iletişim koruma yöntemleri de kullanılmaktadır. Sun ve arkadaşları güç sistemi verilerinin güvenliğini korumak için, çalışmada verilen yöntemler ile gönderici tarafında dinamik olarak ölçüm verilerini şifrelemektedir [19]. Burada yazarlar, verileri iletmek için yeniden iletim protokolünü kullanmaktadır. Bu protokol ile ölçüm verileri düz metin olarak gönderilmek yerine stenografi ile gizlenerek gönderilmektedir. Şifreleme tabanlı yöntemlerin uygulamaya geçebilmesi için yüksek bütçeler gerektiğinden büyük sistemlere uygulanması oldukça zordur. Güç sistemlerindeki FDI saldırılarını tespit etme mekanizmalarına ilişkin daha fazla ayrıntı [20-22]'da verilmektedir. Yukarıda anlatılan tespit yöntemlerinin negatif yönlerinden dolayı farklı yaklaşımların araştırılması gerekmektedir.

Güç sistemini FDI saldırılarından korumak için diğer bir savunma aracı veriye dayalı makine öğrenmesi yöntemleridir. Bu yöntemlerin başlıca iki önemli avantajı bulunmaktadır:

1) Veriye dayalı tespit yöntemleri ağ topolojisine bağlı değildir ve

2) Bu yaklaşım siber-fiziksel sistemlerin mekansal ilişkisine dayalı olarak oluşturulan gizli FDI saldırılarını tespit etmede çok etkili olabilen zaman-varyans ölçümüne duyarlıdır [23].

Ozay ve arkadaşları [24] anomali tespit problemini çözmek için makine öğrenmesi yöntemlerinin uygulanmasına öncülük etmişlerdir. Çalışmada seyrek lojistik regresyon (Sparse Logistic Regression), k-en yakın komşu (k-nn), Çok Katmanlı Algılayıcılar (MLP), AdaBoost ve Destek Vektör Makineleri (SVM) yöntemleri de dahil olmak üzere makine öğrenmesi algoritmalarının bir bölümü test edilmiştir. Simülasyon için MATPOWER kullanılmıştır [25]. Saldırılarının seyrekliğinin bir fonksiyonu olarak modellerin performansını değerlendirmişlerdir ve AdaBoost'un %100 kesinliğe ulaşabileceği kanıtlanmıştır.

Foroutan ve arkadaşları FDI'ları tespit etmek için MLP kullanmıştır ve bunları yaygın makine öğrenmesi yöntemleriyle karşılaştırmışlardır [26]. Burada ağ, bir giriş katmanı, bir gizli katman ve bir çıkış katmanından oluşmuştur aynı zamanda aktivasyon fonksiyonu olarak tanh kullanılmıştır.

Ganjkhani güç sistemlerinin ölçümleri ve durum değişkenleri arasındaki korelasyonu dikkate alan ve "Nonlinear Autoregressive Exogenous" konfigürasyonundan yararlanan yeni bir MLP algoritması geliştirmiştir [27].

[28]'da FDI saldırılarının davranışını ortaya çıkarmak için Koşullu Derin İnanç Ağı (CDBN) önerilmiştir. Yazarlar kullandıkları CDBN için, ilk gizli katmanda Koşullu Gaussian-Bernoulli Kısıtlı Botzman Makinelerini diğer tüm gizli katmanlar için geleneksel Kısıtlı Botzman Makineleri (RBM) kullanmışlardır. %98,10 ile en yüksek doğruluk değeri, 5 gizli katmana sahip bir CDBN tarafından elde edilmiştir.

Eşrefuzzaman ve arkadaşları [29] bir güç sisteminin durum tahminini atlatabilen yanlış veri enjeksiyon saldırılarını tespit edebilmek için İleri Beslemeli Sinir Ağları (FFNN) tabanlı bir yöntem önermişlerdir. Derin öğrenme, Gradyan Artış Makineleri, Genelleştirilmiş Doğrusal Modeller ve Dağıtılmış Rastgele Ormanlar ile karşılaştırılmıştır.

Mohammadpourfard ve arkadaşları [30], gizli FDI'ları tespit etmek için mevcut denetimli öğrenme yöntemlerinin performansını arttırmak üzere kavram kayması fikrini kullanmışlardır. Özellik azaltmak için Temel Bileşenler Analizi (PCA) ile k-nn kullanmışlardır. Standart IEEE-14 baralı test sistemi kullanılarak tespit algoritmasının performansı ölçülmüştür.

Niu ve arkadaşları [31] bir sinir ağına dayanan akıllı şebeke anomali tespit şeması oluşturmuşlardır. Uzun-Kısa Süreli Bellek (LSTM) hücresine sahip bir Tekrarlayan Sinir Ağı (RNN) ile güç sistemlerinin dinamik davranışını yakalamak için bir model geliştirmişlerdir. Yakalanan davranışa göre ölçümler tahmin edilmiş ve gözlemlenen ölçümler ile karşılaştırılmıştır. Bu ölçümler arasındaki kalıntı (treshold) belirlenen eşik değerinden büyükse saldırı olduğu sonucuna ulaşılmıştır.

Mohammadpourfard ve arkadaşları [32]'da, güç sistemleri üzerindeki siber saldırıları RNN tabanlı bir LSTM kullanarak tanımlamıştır. Zaman serisi veri durumunu modelleme yeteneğine dayanan bu teknolojinin, güç ve enerji sistemlerindeki sorunları tahmin etme konusunda özel bir uygulamaya sahip olmuştur. Ayrıca önerilen teknik %90'dan fazla bir doğruluk sağlamıştır.

Başka bir çalışmada ise farklı Buluşsal Özellik Seçimi Teknikleri ile üç sınıflandırma tekniği test edilmiştir [33]. Yazarlar SVM ve k-nn algoritmalarının yapay sinir ağından daha doğru bir sonuç ürettiği sonucuna varmışlardır, fakat bu yöntemler büyük sistemler için uygulanabilir değildir.

Yük-Frekans Kontrolünü tam anlamıyla sağlayabilmek için güç sistemi dinamiklerini etkileyen fiziksel kısıtlamaları ve doğal gereklilikleri hesaba katmak önemlidir. Uygulamada termal birimler tarafından elde edilecek aktif güç değişimi oranının üst bir sınırı vardır [34] ve bu Üretim Oranı Kısıtlamaları (GRC) olarak adlandırılır. GRC, OÜK sistemlerinde üretimin değişim oranını sınırlayan fiziksel bir kısıtlamadır. GRC sisteme entegre edildiğinde, üretim hızı değişikliği kısıtlanır ve ACE değerlerinde büyük sapmalara neden olur. Sistemin kontrol performansını arttırmak için GRC frekans kontrol şemasına eklenmelidir [35].

Ayrıca GRC'nin sisteme yaptığı bu etki Hız Regülatörü Ölü Band (GDB) kısıtlamasıyla birleşince daha da kötü hale gelmektedir. Röle ayar süreleri tarafından belirlenen bir zamana kadar, frekans nominal değerine geri dönemez. Bu durum sistemin kararsız hale gelmesine neden olmaktadır [36]. GRC ve GDB varlığında sistem en küçük bozucu etkilere bile çok büyük tepkiler vermektedir, bu nedenle gerçek bir güç sistemindeki kontrolörün performansı büyük ölçüde düşmektedir [36].

OÜK sistemlerindeki gecikmeler, mekanik sistemin yanıtındaki gecikmenin yanı sıra haberleşme sistemindeki gecikmelerden de kaynaklanmaktadır [36]. OÜK sistemlerindeki zaman gecikmesini, transdüserlerdeki gecikmeler, ayrık Fourier

dönüşümünün boyutu, işlem süresi, çoğullama ve geçişler, sensör çıkışının veri boyutu ve kullanılan iletişim bağlantılarının türü oluşturmaktadır. Bu faktörler ayrıntılı olarak [37] ve [38]'da açıklanmaktadır.

Yukarıda açıklanan nedenlerden dolayı bir siber saldırı sırasında, OÜK'nin davranışını gerçek bir güç sisteminde görebilmek için bu kısıtlamaların sisteme dahil edilmesi gerekmektedir. Bu kısıtlamaları dikkate alan ve FDI saldırılarının tespitini içeren bazı çalışmalar yapılmıştır [39-41].

Öte yandan karbon salınımının azaltılması isteği ve enerji kaynaklarının tükenmeye yakın olması nedeniyle elektrik şebekesine yenilenebilir enerji sistemlerinin entegresi zamanla artmaktadır. Elektrik şebekesine yüksek miktarda Rüzgar Enerjisi Sistemi (RES) entegre edilmesi, kesintili bir üretim sağladığından, güç kalitesini ve sistem güvenilirliğini etkilemektedir [42]. Yenilenebilir enerji kaynaklarından elde edilen enerjinin invertör/konvertör ile kullanılabilecek forma dönüştürülmesi gerekmektedir. İnvertör/konvertör bağlantılı kaynaklar nedeniyle güç sisteminin dönme ataleti azalmaktadır [43-45]. Bu durum sonucunda daha hızlı bir Frekans Değişim Oranı (ROCOF) ve daha az kararlı frekans dinamiği oluşmaktadır [44]. Enterkonnekte güç sistemine yüksek oranda RES entegresyonu sonucunda bağlantı hatları aşırı yüklenmektedir ve sonuç olarak frekans kararlılığı bozulmaktadır. Yüksek RES entegresyonu durumunda frekans daha hızlı değişeceği için OÜK sistemlerine yapılan siber saldırının etkisi daha büyük olacaktır [46]. Bu nedenle güç sistemlerine yapılacak saldırıların analizini daha gerçekçi yapabilmek adına, güç sistemine RES ilave edilmesi önemli bir yer tutmaktadır.

RES sistemlerinin ilave edildiği çalışmalara örnek olarak [47]'da, çeşitli FDI saldırı şablonları tanımlanmış ve çok alanlı OÜK üzerinde analiz edilmiştir. Saldırıları tespit etmek için bulanık mantık ve sinir ağlarından oluşan veriye dayalı bir yöntem sunulmuştur. OÜK sistemine büyük oranlı yenilenebilir enerji kaynakları entegre edilerek yenilenebilir enerji üretimi olan ve olmayan duruma göre üç simülasyon senaryosu oluşturulup FDI'ları tespit etme performansı doğrulanmıştır. Sonuç olarak çoğu durumda çeşitli FDI'ların tespit edilmesinde Fuzzy Lojik ve Sinir Ağları karşılaştırılan diğer algoritmalara göre daha yüksek bir doğruluk göstermiştir. Fakat bu çalışmada gizli saldırılar incelenmemiş olup GDB, GRC ve zaman gecikmesi gibi OÜK nonlineerlikleri dahil edilmemiştir.

Bir diğer RES ilave edilen çalışmada [46], OÜK sisteminin çalışması hakkında bir siber saldırı-savunma analizi sunulmuştur. OÜK çalışmasına farklı koşullar altında rampa saldırısı gerçekleştirilmiştir ve farklı oranlarda değişen yenilenebilir enerji kaynakları sisteme entegre edilmiştir. Yazarlar yenilenebilir enerji oranının artması ile birlikte sistem frekansının daha hızlı düştüğünü gözlemlemişlerdir. Ayrıca sistem savunmasını geliştirmek ve sistemin verimli çalışmasını sürdürmek için iki aşamalı bir siber saldırı azaltma stratejisi uygulanmıştır. Saldırı azaltma nedeniyle OÜK performansı üzerinde üretilen Yanlış Pozitifler (FP) için de analiz yapılmış ve tatmin edici performans elde edilmiştir. Deneyler sonucunda saldırının verdiği zarar büyük ölçüde önlenmiştir. Deneyler Iowa Devlet Üniversitesi'ndeki CPS güvenlik test ortamı kullanılarak gerçekleştirilmiştir. Bu çalışmada çoklu saldırı stratejileri ele alınmamıştır ve etkileri gözlenmemiştir.

OÜK sistemlerine yapılan siber saldırılar için literatürde yapılan çalışmalar yukarıda verilmiştir. OÜK sistemlerine yapılan siber saldırılar pek çok çalışmada incelenmiştir fakat yenilenebilir enerji kaynaklarının entegre edildiği çalışmaların yetersiz olduğu gözlemlenmiştir. Ek olarak güç sisteminin performansını büyük ölçüde etkileyen OÜK doğrusalsızlıkları da yeteri kadar incelenmemiştir.

Bu çalışmada frekans ve ACE değerleri, doğrusallaştırmanın bensimsendiği veya benimsenmediği durumuna göre ayrı ayrı incelenmiştir. OÜK doğrusalsızlıklarının sistemin davranışında önemli bir etkiye neden oldukları simülasyon sonuçları ile doğrulanmıştır. Ek olarak sisteme farklı koşullarda ve oranda yenilenebilir enerji kaynakları entegre edilmiş ve sonuçlar analiz edilmiştir. Ayrıca farklı siber saldırı şablonları OÜK sistemine uygulanmıştır. Bu saldırıların etkisinin arttırılması amacıyla çeşitli saldırı şablonları birleştirilerek farklı hibrit saldırı senaryoları oluşturulmuştur. Son olarak verilen bu dinamikler altında siber saldırıların çoklu sınıflandırması için k-nn, karar ağaçları, sinir ağları ve torbalama ağaçları algoritmaları kullanılmıştır. Farklı RES entegresyon oranı altında çeşitli saldırı modelleri uygulanmıştır. Önerilen torbalama ağaçları algoritmasının, OÜK sistemlerine yapılan FDI saldırılarının çok sınıflı sınıflandırmasında kullanılabileceği kanıtlanmıştır.

2. OTOMATİK ÜRETİM KONTROLÜ (OÜK)

2.1 Güç Sistemlerinin Kontrolü

Güç sisteminin kontrolü işlemi otomasyon ve insan faktörü kullanılarak fiziksel bir bozulma sonrası sistemi normal çalışmasına geri döndürme işlemidir [48]. Güç sistemi kontrolü terimi, normal veya anormal işlemler sırasında güç sistemlerinin performansını iyileştirmek için kontrol teorisi ile teknolojisinin optimizasyon metodolojilerinin ve akıllı sistemlerin uygulanmasını tanımlamak için kullanılır [49].

2.1.1 Gerilim kontrolü

Bir dağıtım sistemi için gerilimlerin belirli sınırlar içinde tutulması gerekmektedir. Yani gerilim çok düşük olduğunda yükseltmek, çok yüksek olduğunda ise düşürmekten sorumlu araçlar bulunmalıdır. Dağıtım sisteminin genel gerilim düzenlemesini iyileştirmek için çok sayıda yöntem vardır. Lokay [50] bunun için aşağıda verilen listeyi hazırlamıştır:

1) Birincil fiderdeki yüklerin dengelenmesi

2) Dağıtım trafo merkezinde kapasitör kurulumu

3) Dağıtım trafo merkezinde gerilim düzenleyici ekipmanların bulunması

4) Yüklerin yeni fiderlere aktarılması

5) Jeneratör voltaj regülatörlerinin kullanımı

6) Fider iletken boyutunun arttırılması

7) Şönt kapasitörlerin birincil fiderlere bağlanması

8) Seri kapasitörlerin birincil fiderlere bağlanması

9) Yeni trafo merkezlerinin ve birincil fiderlerin kurulumu

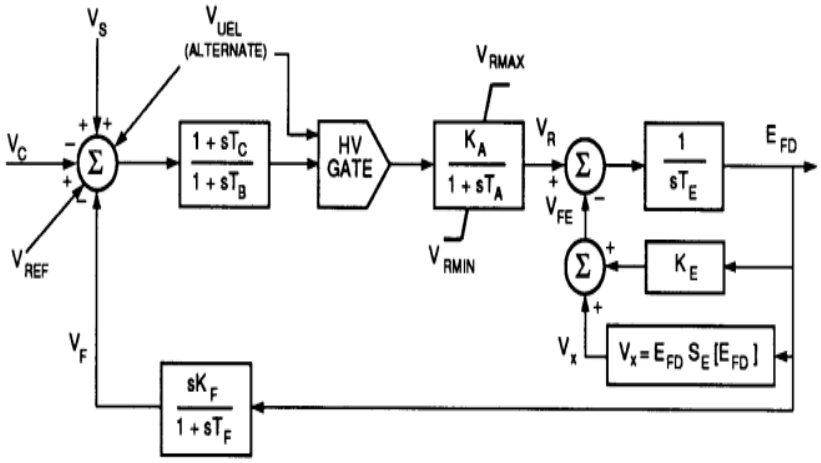
10) Birincil gerilim seviyesinin artması

11) Fider bölümlerinin tek fazdan çok faza değiştirilmesi

12) Birincil fiderlerde gerilim regülatörlerinin uygulanması.

Yukarıda verilen bir tekniğin veya birden çok tekniğin seçimi, belirli sistem gereksinimlerine bağlıdır ve bununla birlikte birçok kamu hizmeti kuruluşu gerilimi belirli limitler içerisinde tutmanın en ekonomik yolunun kademeli gerilim regülatörleri ile şönt kapasitörleri birlikte uygulamak olduğunu belirlemiştir [51]. Bir güç sisteminde çok sayıda yük ve jeneratör bulunur ve bunlar çoğu zaman geniş bir alana yayılmışlardır. Geniş bir alana yayılan ve çok sayıda yük-üretim birimi bulunan bir güç sistemi için gerilimi düzenleme işlemi oldukça zordur.

Bir bölgedeki yük değiştiği zaman sistemin reaktif güç ihtiyacı da değişir ve reaktif gücün uzun mesafelere iletimi çok zor olduğundan gerilim kontrolünün özel ekipmanlar ile yapılması büyük önem arz etmektedir. Gerilimin kontrol edilebilmesi için ekipman seçimi ve koordinasyonu güç sistemi mühendisliğindeki en büyük zorluklardan biridir. Güç sistemlerinde gerilim kontrolü için senkron jeneratörler, iletim hatları, statik VAR kompanzatörleri, şönt kapasitörler, şönt reaktörler vb. ekipmanlar kullanılmaktadır. Şekil 2.1'de IEEE tarafından tanımlanan standart gerilim kontrol döngüsü gösterilmektedir.



Şekil 2.1: Type DC1A – DC komütatör uyartım [52].

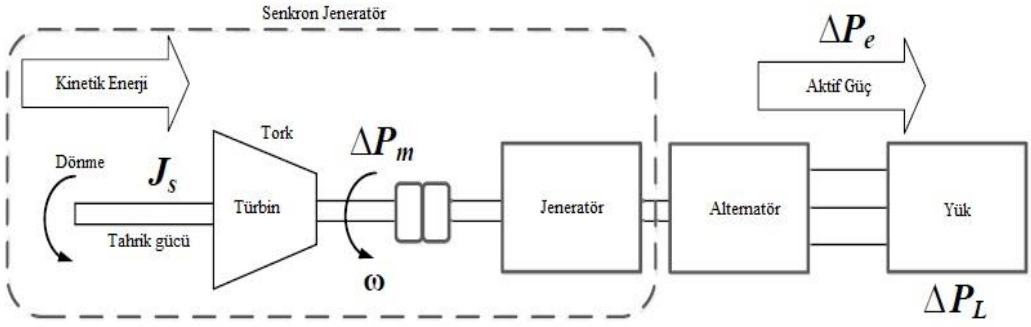
Burada T_R Transdüser, T_A AVR, T_E Uyartım, T_F Geri Besleme zaman sabitleri K_A AVR, K_E Uyartım, K_F ise Geri Besleme kazanç sabitleridir.

2.1.2 Frekans kontrolü

Bir güç sisteminin frekansı belirlenen çalışma limitleri içerisinde kalmazsa bu güç sisteminde frekans kararsızlığı oluşur. Frekans kararsızlığı, bir güç sisteminin, sistem frekansını belirtilen çalışma limitleri içinde tutamamasıdır. Genel olarak, frekans kararsızlığı, yük ve üretim arasındaki önemli bir dengesizliğin sonucudur ve kontrol-koruma ekipmanının zayıf koordinasyonu, yetersiz üretim ve ekipman yanıtlarındaki yetersizlikler ile ilişkilidir [53,54]. Üretilen güç ve tüketilen güç arasında büyük bir dengesizlik olduğu zaman güç sisteminin performansı ciddi şekilde düşer.

OÜK ana görevi olan yük-frekans kontrolü elektrik güç sisteminin tasarımı ve işletimi için önemli kontrol parametrelerinden biridir. Frekansın normal olmadığı durumlarda güç sisteminin çalışması ve güvenilirliği doğrudan etkilenir [48]. Oluşan büyük bir frekans sapması ekipmanlara zarar verebilir, yük performansını düşürebilir, iletim hatlarının aşırı yüklenmesine neden olabilir ve sonuç olarak güç sisteminin kararlılığı olumsuz etkilenir [55].

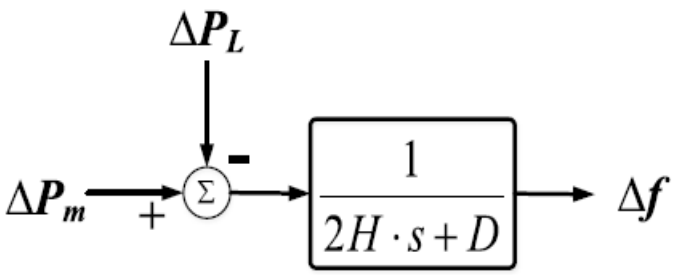
Üretim tipine göre, bir jeneratör tarafından sağlanan aktif güç, buhar türbini, gaz türbini, hidro-türbin veya dizel gibi bir tahrik sisteminin mekanik güç çıkışı tarafından kontrol edilir. Bir buhar veya hidro-türbin söz konusu olduğunda, mekanik güç, türbine buhar veya su akışının girişini düzenleyen valflerin açılıp kapanmasıyla kontrol edilir. Birincil frekans kontrolüne ek olarak, çoğu büyük senkron jeneratör, ek bir frekans kontrol döngüsü ile donatılır. Şekil 2.2'de izole bir yükü besleyen bir generatör ve hız regülatörü sistemi temel blok diyagramı yer alır.



Şekil 2.2: İzole yükü besleyen senkron makinenin blok diyagramı.

Yükte bir değişiklik olduğu zaman generatörün elektriksel tork çıkışında da değişiklik olur. Bunun sonucunda mekanik tork ve elektriksel tork arasında hareket denklemleri

tarafından belirlenen bir eşitsizlik oluşur. Şekil 2.3'de mekanik güç ile torkun bir fonksiyonu olarak frekans değişimi gösterilir.



Şekil 2.3: Frekans kontrolü için yük-jeneratör modelinin blok diyagramı.

Yük-frekans kontrolünde, yukarıda verilen tork ilişkisi yerine mekanik ve elektriksel güç cinsinden verilmesi tercih edilir.

Genel jeneratör mekanik gücü ve yük arasındaki ilişki (ΔP_m-ΔP_L) ile frekans sapması (Δf) arasındaki dinamik ilişki şu şekilde ifade edilebilir:

$$\Delta \mathrm{P_m(t)} - \Delta \mathrm{P_L(t)} = 2\mathrm{H}\frac{\mathrm{d}\Delta \mathrm{f(t)}}{\mathrm{dt}} + \mathrm{D}\,\Delta \mathrm{f(t)} \tag{2.1}$$

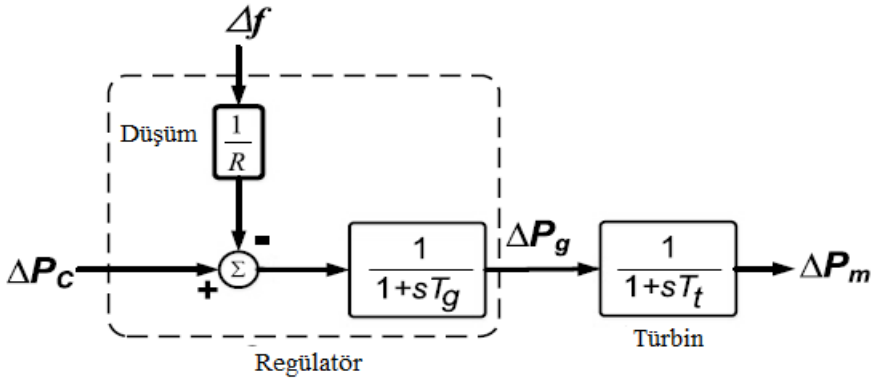
burada Δf frekans sapmasıdır, ΔP_m mekanik güç değişimidir, ΔP_L yük değişimidir, H atalet sabitidir ve D yük sönümleme katsayısıdır. Laplace dönüşümü kullanılarak denklem 2.1 aşağıdaki gibi yazılabilir:

$$\Delta \mathrm{P_m(s)} - \Delta \mathrm{P_L(s)} = 2\mathrm{Hs}\Delta \mathrm{f\,(s)} + \mathrm{D}\Delta \mathrm{f\,(s)} \tag{2.2}$$

Türbin modeli mekanik güç çıkışındaki (ΔP_m) değişiklikleri buhar valfi konumundaki (ΔP_V) değişikliklerle ilişkilendirilir. Farklı türbin türleri tek zaman sabiti τ_T ile aşağıdaki transfer fonksiyonu ile yaklaşık olarak indirgenebilir.

$$G_T(s) = \frac{\Delta P_m(s)}{\Delta P_g(s)} = \frac{1}{1 + \tau_T(s)} \tag{2.3}$$

Basit bir türbin için blok diyagramı Şekil 2.4'de gösterilmektedir.



Şekil 2.4: Ara-ısıtıcısız buhar türbin-regülatör kontrol blok diyagramı.

Elektriksel yük ani olarak arttığında elektriksel güç mekanik güç girdisini aşar. Bu güç eksikliği dönen sistemlerde depolanan kinetik enerji ile karşılanır. Kinetik enerjinin azalması, türbin dönüş hızının azalmasına ve sonuç olarak jeneratör frekansının düşmesine neden olur. Hızdaki değişiklik türbin regülatörü tarafından algılanır. Ayrıca hızı tekrar kararlı duruma getirmek için türbin regülatörü, mekanik güç çıkışını türbin giriş valfini ayarlayarak düzenler. Regülatörler sistemdeki yük arttıkça hızın düşmesini sağlayacak şekilde tasarlanır. Ayrıca regülatörler, tipik olarak sıfırdan tam yüke %5-6 olacak şekilde bir hız regülasyon oranına sahiptir [56]. Hız regülatörü mekanizması aşağıdaki denklemde verilen şekilde ayarlı referans güç ΔP_{ref} ile $\frac{1}{R}\Delta\omega$ arasındaki fark olan bir karşılaştırıcı görevi görür. Bu karşılaştırıcının çıkışı ise ΔP_g'dir.

$$\Delta P_g = \Delta P_{ref} - \frac{1}{R}\Delta\omega \tag{2.4}$$

$$R = \frac{\Delta\omega}{\Delta P} \tag{2.5}$$

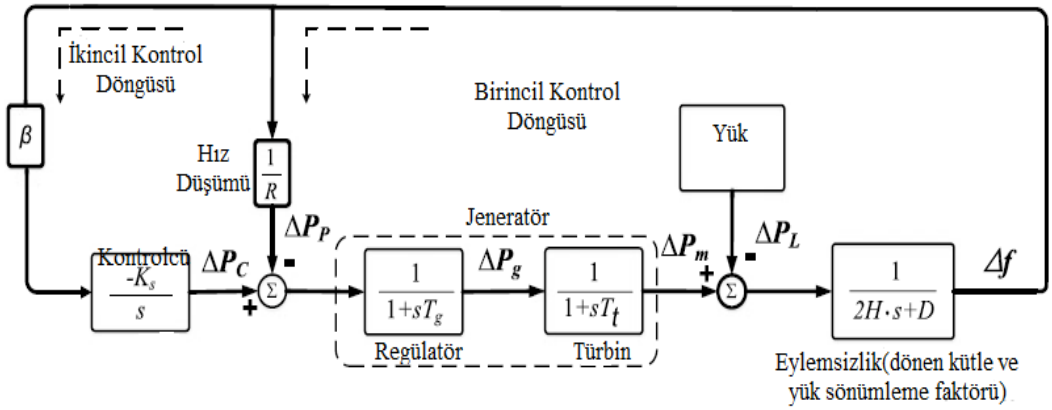
Denklem 2.4'ü s-domeninde yazarsak,

$$\Delta P_g(s) = \Delta P_{ref}(s) - \frac{1}{R}\Delta\Omega(s) \tag{2.6}$$

elde edilir. ΔP_g komutu, hidrolik yükseltici aracılığıyla buhar valfi konum komutu olan ΔP_V'ye dönüştürülür. Doğrusal bir ilişki olduğu düşünüldüğünde τ_g zaman sabiti eşliğinde aşağıdaki ilişki elde edilir.

$$\Delta P_V(s) = \frac{1}{1 + \tau_g} \Delta P_g(s) \tag{2.7}$$

Tek alanlı bir güç sistemi için frekans kararlılığı çalışması ve analizinde, Şekil 2.5'de gösterilen eşdeğer bir jeneratör modeli kullanarak çok jeneratörlü bir dinamik davranışı modellemek yaygındır. Ardından Şekil 2.5'de oluşturulan birleştirilmiş model, tek alanlı bir güç sisteminin tüm jeneratörleri için bir eşdeğer frekans analiz modeli olarak kullanılmaktadır.



Şekil 2.5: Birincil ve ikincil kontrol döngüleriyle ara-ısıtıcısız bir buhar jeneratörünün dinamik modeli.

Eşdeğer modelde sistem yükleri, jeneratörleri ve bunların sönümleme etkileri tek bir sabit ile temsil edilmektedir. Eşdeğer atalet sabitinin, tüm jeneratörlerin atalet sabitinin toplamı olduğu kabul edilmektedir. Sadece birincil kontrol döngüsü sistem kararlılığını sağlamakta yetersiz kalmaktadır. Bu nedenle ikincil kontrolünü sisteme entegre ederek sistem frekansının birkaç saniye içinde eski değerine geri dönmesi sağlanmaktadır.

2.2 Enterkonnekte Bir Güç Sisteminde Frekans Kontrolü

İzole bir güç sisteminde frekans analizi yapılırken çok makineli bir dinamik davranışı eşdeğer tek bir makineyle modellemek yaygındır. Bu modelin, tüm güç sistemi eşdeğer frekans cevabı modeli olarak kullanılması düşünülebilir. Oluşturulan eşdeğer modelde, sistem yükleri ve jeneratörlerin etkileri tek bir sönümleme katsayısında toplanmaktadır. Eşdeğer atalet sabitinin, tüm jeneratörlerin atalet sabitinin toplamı olduğu düşünülmektedir. Ek olarak kontrol döngüleri ile türbin ve jeneratörlerin aynı

parametrelere sahip olduğu varsayılmaktadır. Bu modelin oluşturulma amacı, frekans cevabı analizinin basitleştirilmesini sağlamaktır. Çok alanlı bir güç sistemi, yüksek voltajlı iletim hatları ile birbirine bağlanan alanlardan meydana gelmektedir. Enterkonntekte bir güç sisteminin her bir kontrol alanındaki frekans kontrol sistemi, o alandaki frekansın yanı sıra diğer alanlarla olan güç alışverişini de kontrol etmelidir. Bu nedenle verilen izole güç sistemi modeli bağlantı hattı gücü de dikkate alınarak tekrar oluşturulmalıdır.

Alan 1'den Alan 2'ye doğru bağlantı hattındaki güç akışı

$$\mathrm{P}_{tie,12} = \frac{V_1 V_2}{X_{12}} \sin\left(\delta_1 - \delta_2\right) \tag{2.8}$$

burada X_{12} alan 1 ve alan 2 arasındaki bağlantı hattı reaktansı; δ_1, δ_2 alan 1 ve alan 2'nin eşdeğer makinelerinin güç açısı ve V_1, V_2 ise alan 1 ve alan 2'nin gerilimleridir. Denklem 2.8'i (δ_1^0, δ_2^0) denge noktası etrafında lineerleştirilirse;

$$\mathrm{P}_{tie,12} = T_{12}(\Delta\delta_1 - \Delta\delta_2) \tag{2.9}$$

olur. Burada T_{12} senkronize tork katsayısıdır ve denklem 2.10'da verilmektedir:

$$T_{12} = \frac{|V_1||V_2|}{X_{12}} \cos\left(\delta_1^0 - \delta_2^0\right) \tag{2.10}$$

Alan güç açısı ile frekans arasındaki matematiksel ilişki dikkate alındığında denklem 2.9 aşağıdaki gibi yazılabilmektedir.

$$\mathrm{P}_{tie,12} = 2\pi T_{12}\left(\int \Delta f_1 - \int \Delta f_2\right) \tag{2.11}$$

Bu denklemde Δf_1 ve Δf_2 sırasıyla alan 1 ve alan 2 frekans sapmalarıdır. Denklem (2.11)'in Laplace dönüşümü alındığında aşağıdaki denklem elde edilmektedir.

$$\mathrm{P}_{tie,12}(s) = \frac{2\pi}{\mathrm{s}} T_{12}\left(\Delta f_1(s) - \Delta f_2(s)\right) \tag{2.12}$$

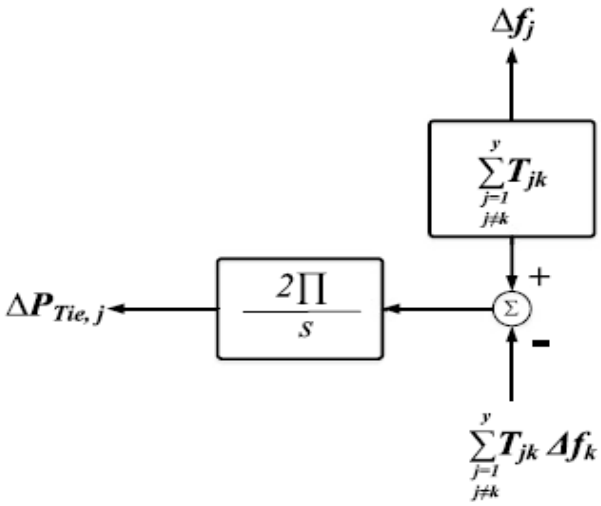
Benzer olarak, j-kontrol alanı için, alan-1 ile diğer alanlar arasındaki toplam bağlantı hattı güç alışverişi aşağıdaki gibi elde edilebilmektedir [49]:

$$\Delta P_{Tie,j} = \sum_{\substack{j=1 \\ j\neq k}}^{y} \Delta P_{Tie,jk}(s) = \frac{2\pi}{s}\left[\sum_{\substack{j=1 \\ j\neq k}}^{y} T_{jk\Delta f_j} - \sum_{\substack{j=1 \\ j\neq k}}^{y} T_{jk\Delta f_k}\right] \quad (2.13)$$

Burada y toplam kontrol alanı sayısıdır. Denklem 2.13 Şekil 2.6'daki gibi gösterilebilmektedir. OÜK sisteminin diğer komşu alanlar ile frekans ve güç alışverişini planlanan değerlerde sürdürmesi gerekmektedir. Bu değerlere, bir kontrol hatası sinyali olan ACE ölçülerek ulaşılmaktadır. Herhangi bir "i" alanı için ACE sinyali;

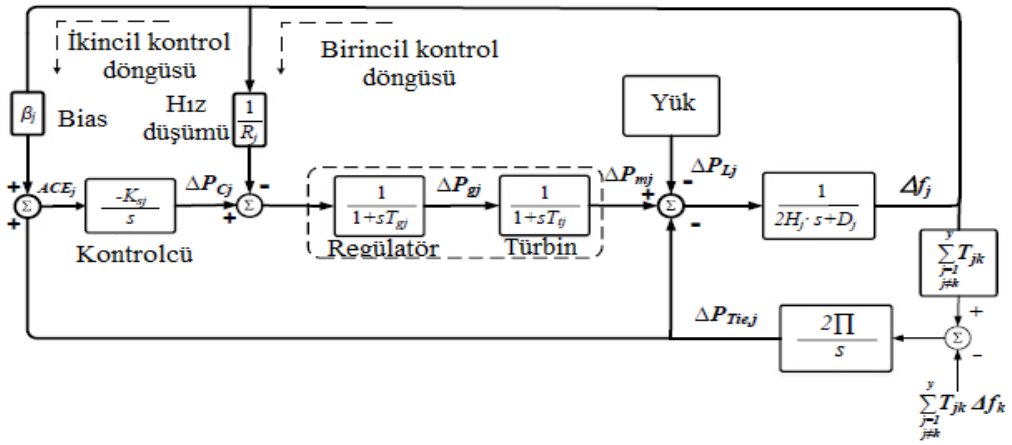
$$ACE_i = \sum_{j=1}^{n} \Delta P_{ij} + K_i \, \Delta w \quad (2.14)$$

olarak hesaplanmaktadır.



Şekil 2.6: j kontrol alanı için bağlantı hattı güç değişimi bloğu.

Böylece, $\Delta P_{Tie,j}$ mekanik (üretilen) güç değişimine ve alan yükü değişimine eklenmiş olmaktadır. Şekil 2.5 ile Şekil 2.6 birleştirilince enterkonnekte bir sistemin blok diyagramı modeli Şekil 2.7'de gösterildiği gibi olmaktadır. Enterkonnekte bir güç sisteminde, ikincil kontrol döngüsü, alan frekansını programlanan değerlere ayarlamakta ve birbirine bağlı tüm alanlarda güç alışverişini düzenlemektedir.



Şekil 2.7: İkincil kontrol ile j kontrol alanı için dinamik model.

İntegral sabiti K_i, komşu alanlardaki bir bozulma sırasındaki etkileşim miktarını belirlemektedir. K_i, o alanın frekans cevap karakteristiğine eşit seçildiğinde genel olarak iyi bir performans elde edilmektedir. Bir başka deyişle, $B_i = \frac{1}{R_i} + D_i$. Böylece 2 alanlı bir sistem için ACE aşağıdaki gibi verilmektedir.

$$ACE_1 = \Delta P_{12} + B_1 \Delta w_1 \tag{2.15}$$

$$ACE_2 = \Delta P_{21} + B_2 \Delta w_2 \tag{2.16}$$

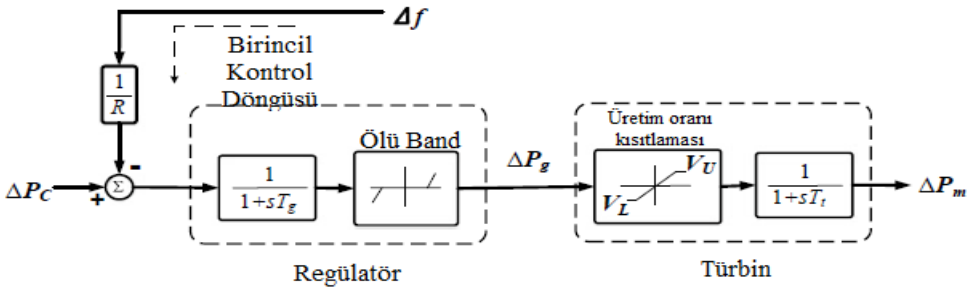
ACE sinyali filtrelendikten sonra, genellikle Oransal İntegral (PI) kontrolcüsü için bir giriş kontrol sinyali olarak kullanılmaktadır. Ardından kontrolcü tarafından çıkan kontrol sinyali, belirli tesislerin ayar noktalarını uygun kontrol komutları ile düzeltmek üzere katılım faktörleri de dikkate alınarak OÜK bulunan jeneratör üniteleri arasında dağıtılmaktadır. Enterkonnokte güç sistemlerinin artan boyutu, karmaşıklığı ve değişen yapısı nedeniyle frekans kontrolü gün geçtikçe önemini arttırmaktadır. Güç sisteminin daha verimli ve güvenilir kullanımıyla birlikte göz önünde bulundurulan ekonomik baskılar, güç sisteminin frekansını ve bağlantı hattı güç akışlarını planlanan değerlere mümkün olduğunca yakın değerde tutulmasını zorunlu kılmaktadır.

2.3 Otomatik Üretim Kontrolü Doğrusalsızlıkları

OÜK doğrusalsızlıkları, sistemin gerçek davranışını beklenen davranışından saptırmasını ifade etmektedir. Bu çalışma, aşağıda yer alan üç farklı OÜK doğrusalsızlığının sisteme dahil edilmesini içermektedir.

2.3.1 Hız regülatörü ölü bandı (GDB)

OÜK sistemlerinde regülatör, güçteki küçük değişikliklere (yani, küçük bozulmalara) yanıt vermez ve bu nedenle, güç çıkışı mevcut seviyesinde kalır. Bunun nedeni GDB'dir [36] [57]. Ancak frekans sapması ölü bandı aşarsa, regülatör güç çıkışını yük talebine göre yeniden düzenler. GDB, yaklaşık T_0 = 2s [58] doğal periyodunun sürekli sinüzoidal salınımını üretir. Ölü band OÜK sistemleri için önemli bir parametredir. Gereksiz düzenlemeler yapmaktan kaçınarak jeneratörlerin ve kontrol sistemlerinin aşınmasını ve yıpranmasını azaltmaya yardımcı olur. Fakat, ölü band uygun olarak seçilmezse, band içinde kalan frekans sapmaları sitemin kararsız hale gelmesine veya yüksek seviyelerde frekans sapması oluşmasına neden olur. GRC ve GDB, Şekil 2.8'de ara ısıtıcısız bir buhar türbini için gösterildiği gibi histerezis modeli ve sınırlayıcıyı türbin-regülatör yapısına entegre ederek incelenebilir. V_L ve V_U, valf açma ve kapama hızını sınırlayan alt ve üst kısıtlamalardır.



Şekil 2.8: Ara ısıtıcısız bir ünite için ölü bant ve üretim oranı kısıtlamaları konfigürasyonu.

2.3.2 Üretim oranı kısıtlamaları (GRC)

GRC, jeneratörlerin güç çıkışlarının ani olarak değişmesini engelleyen bir sınırlamadır. Bu sınırlama jeneratörlerin fiziksel ve mekanik kısıtlamalarını dikkate alır. GRC'ler sisteme entegre edildiğinde, üretim hızı değişikliği sınırlanır ve ACE değerlerinde büyük sapmalara neden olur. Sonuç olarak, güç iletim süresi, üretim hızının kısıtlanmadığı durumlara kıyasla önemli ölçüde artar [59]. Bu nedenle, GRC'nin OÜK'deki etkisi iyi anlaşılmalı ve göz ardı edilmemelidir.

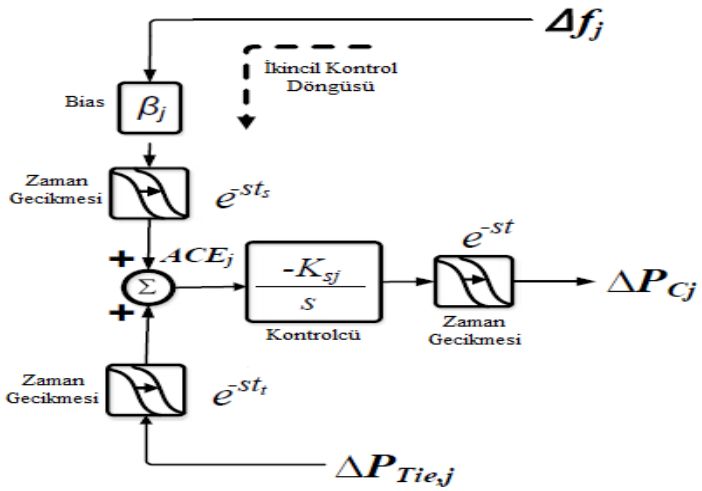
GRC etkisi matematiksel olarak şu şekilde ifade edilebilir:

$$\frac{\Delta P_m}{\Delta t} < \text{GRC} \tag{2.17}$$

burada ΔPm, Δt zaman aralığında türbinin mekanik çıktısındaki değişikliktir.

2.3.3 Zaman gecikmesi (TD)

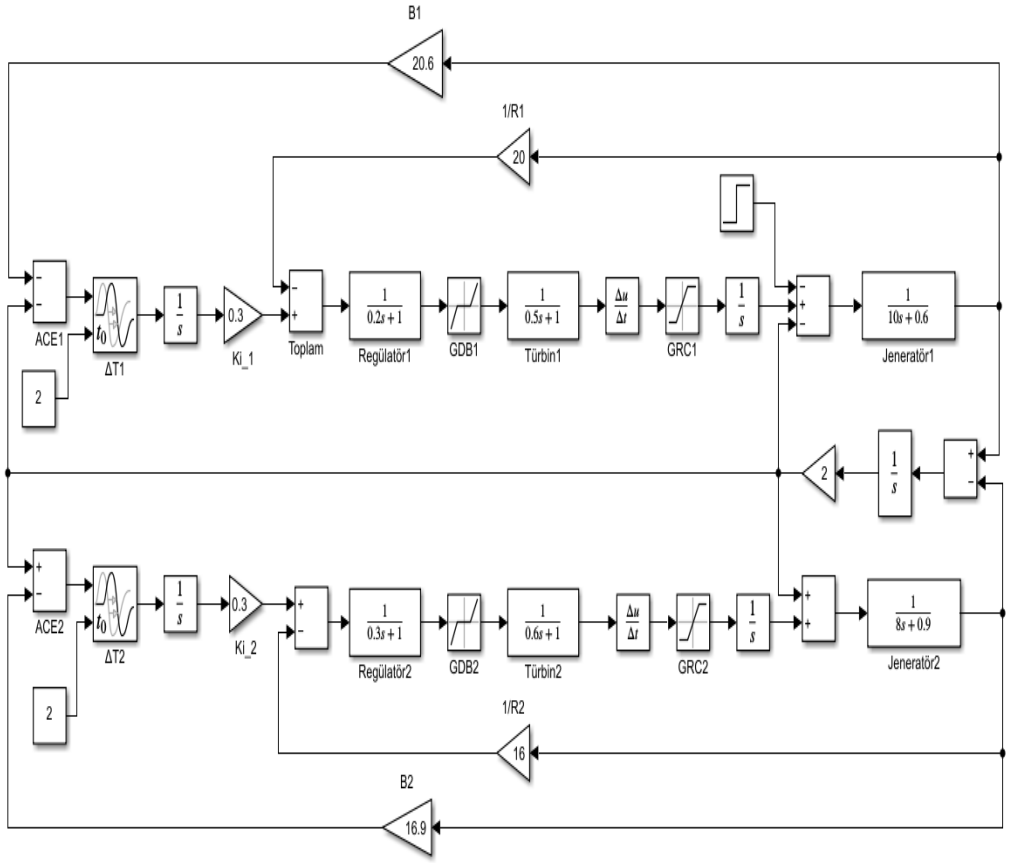
OÜK sistemlerindeki gecikmeler, mekanik sistemin yanıtındaki gecikmenin yanı sıra haberleşme sistemindeki gecikmelerden de kaynaklanmaktadır [36]. OÜK sistemlerindeki zaman gecikmesinin kaynakları, transdüserlerdeki gecikmeleri, ayrık Fourier dönüşümünün boyutunu, işlem süresini, çoğullama ve geçişleri, sensör çıkışının veri boyutunu ve kullanılan iletişim bağlantılarının türünü içermektedir. Bu faktörler ayrıntılı olarak [37,38]'de açıklanmaktadır. İkincil kontroldeki zaman gecikmeleri işletim istasyonları ile kontrol merkezi arasındaki iletişim kanallarında meydana gelmektedir. Özellikle, uzak terminal ünitelerinden (RTU) kontrol merkezine giden bağlantı hattı güç akışı ve frekansının ölçümü ile kontrol merkezinden bağımsız üretim birimlerine giden kontrol sinyalinin ölçümünde gecikmeler mevcuttur. Bu tür gecikmelerin yapısı, Şekil 2.9'da açıklanmaktadır. Gecikme, üstel bir fonksiyon bloğu $e^{-s\tau}$ ile temsil edilmektedir; burada τ veya t, iletişim gecikme süresidir, t_s ve t_t, sırasıyla ikincil kontrol ve bağlantı hattı kontrol birimleri için iletişim gecikme süresidir.



Şekil 2.9: İkincil kontrol döngüsündeki zaman gecikmeleri.

2.3.4 Doğrusalsızlıkların OÜK'nin çalışmasına etkileri

Şekil 2.10'da verilen 2 alanlı OÜK, test sistemi-1 olarak belirlenmektedir. Bu model gerçek bir 2-alanlı güç sisteminin tüm bileşenlerinin ayrı ayrı birer bileşen ile temsil edildiği lineerleştirilmiş modeldir. Bu sayede işlem ve hesap kolaylığı sağlanması amaçlanmaktadır. Ayrıca belirtilen doğrusalsızlıkların sisteme etkisinin daha iyi anlaşılması için iki alanlı OÜK sistemi aynı bozulma şartları altında lineer-nonlineer olarak test edilmektedir.



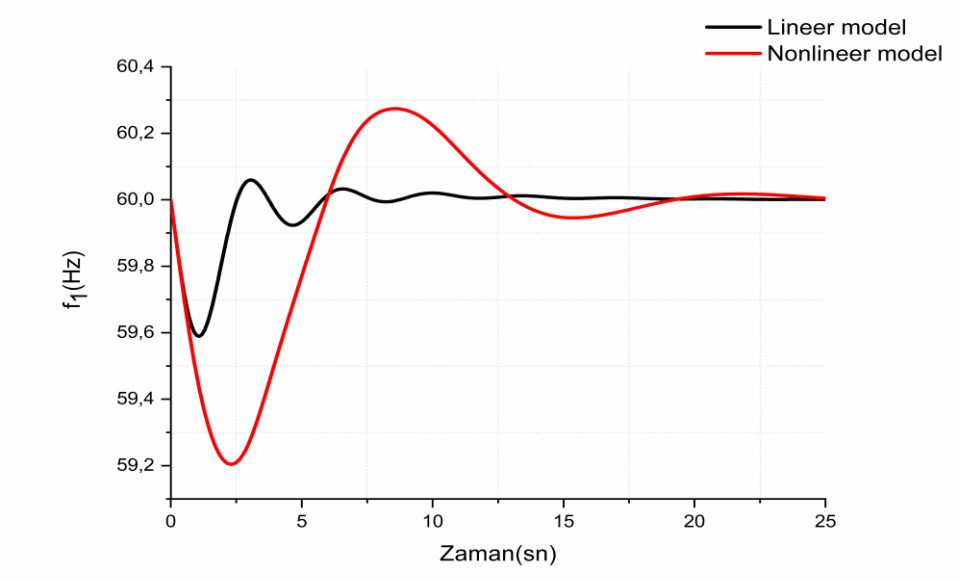
Şekil 2.10: İkincil kontrollü iki alanlı test sisteminin MATLAB/Simulink modeli.

Sistem parametleri için sayısal değerler Çizelge 2.1'de verilmiştir ve bu değerler Saadat'tan [56] alınmıştır. Δt ve GDB ise her iki alan için sırasıyla 2s ve 0.036 Hz olmak üzere Golpira ve Bevrani'den [36] alınmıştır. Alan 1'de t=0 anında 0.1 pu değerinde bir yük artışı olacak şekilde bozucu bir etki meydana gelmiştir.

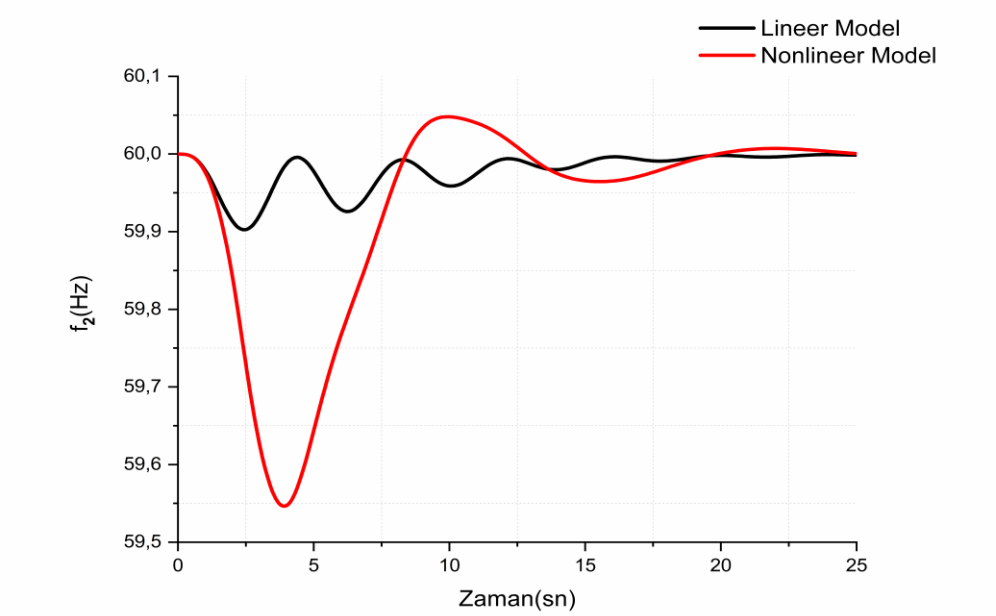
Çizelge 2.1: İki alanlı indirgenmiş güç sistemi parametreleri [56].

Parametreler	Alan 1	Alan 2
D (pu/Hz)	0.6	0.9
H (sn)	5	4
R (Hz/pu)	0.05	0.0625
τ_g (sn)	0.2	0.3
τ_t (sn)	0.5	0.6
B (pu/Hz)	20.6	16.9
ΔP_L (pu)	0.1	0
Baz Güç (MVA)	1000	1000

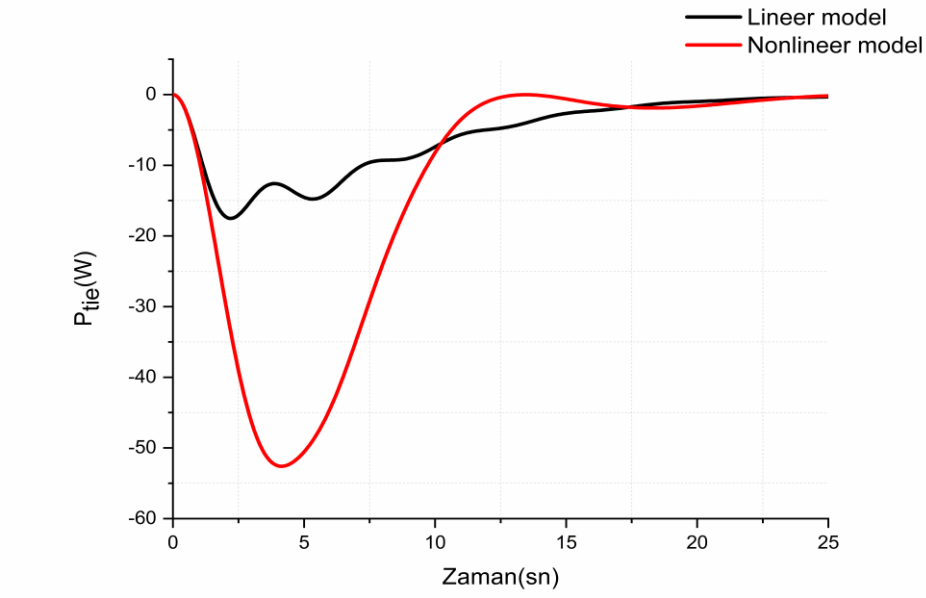
Şekil 2.11-2.12 ve 2.13'den görüldüğü üzere OÜK durum cevabı nonlineer durum için Δf ve ΔP_{tie} değerlerinin lineer durumdan oldukça farklıdır. Bunun oluşma nedeni doğrusalsızlıkların sistemde oluşturduğu etkilerdir. Doğrusalsızlıkları göz ardı edersek, doğrusal model, doğrusal olmayan modele kıyasla sıfıra yakın bir sinyal gönderir ve bu da sistemi optimum çalışma koşullarından saptırır.



Şekil 2.11: Doğrusallık ve doğrusalsızlıklara göre alan-1 frekans cevabı.

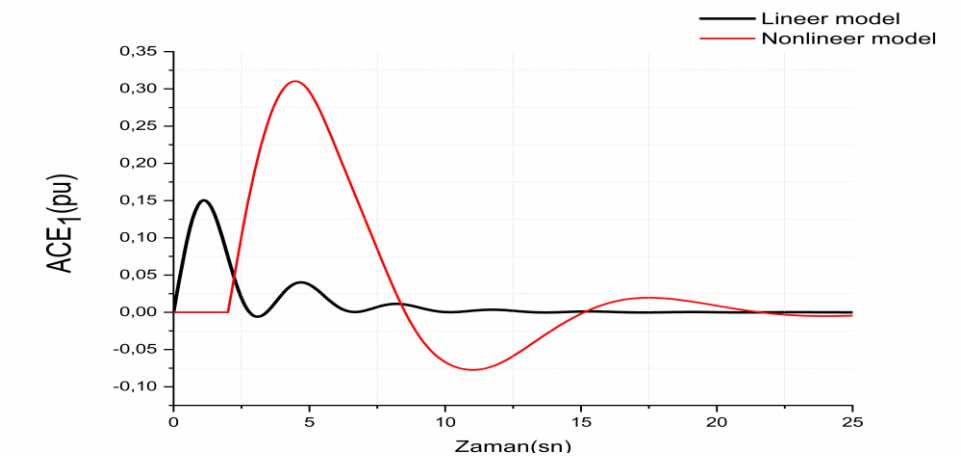


Şekil 2.12: Doğrusallık ve doğrusalsızlıklara göre alan-2 frekans cevabı.

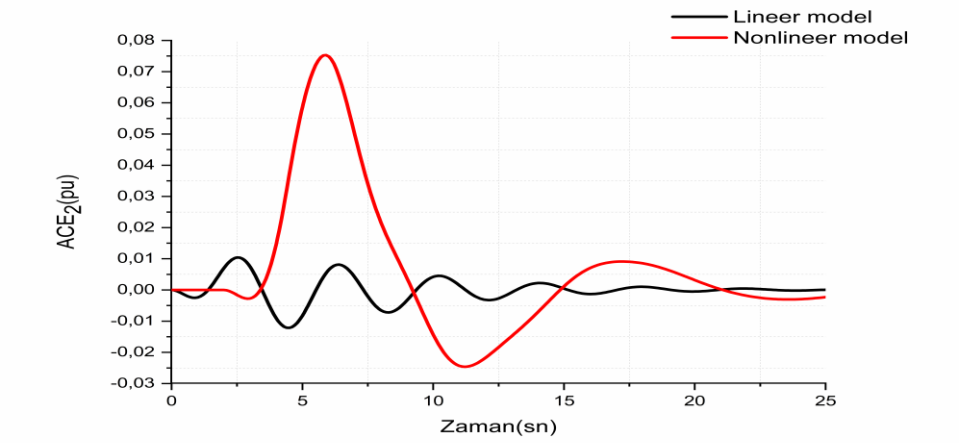


Şekil 2.13: Doğrusallık ve doğrusalsızlıklara göre bağlantı hattı gücü değişimi.

Aynı durumda Şekil 2.14 ve 2.15'den görüldüğü üzere OÜK durum cevabı nonlineer durum için ACE_1 ve ACE_2 değerlerinin lineer durumdan oldukça farklıdır.Doğrusalsızlıkların sistemde oluşturduğu etkiler ACE değerleri üzerinden de gözlenebilmektedir.



Şekil 2.14: Doğrusallık ve doğrusalsızlıklara göre ACE_1 değişimi.



Şekil 2.15: Doğrusallık ve doğrusalsızlıklara göre ACE_2 değişimi.

2 alanlı güç sistemi üzerinde yapılan simülasyonlar sonucunda OÜK doğrusalsızlıklarının sistemin çalışmasında önemli bir etkiye sahip olduğu kanıtlanmıştır. Bundan dolayı kullanılan tüm simülasyonlarda doğrusalsızlıklar sisteme dahil edilmiştir.

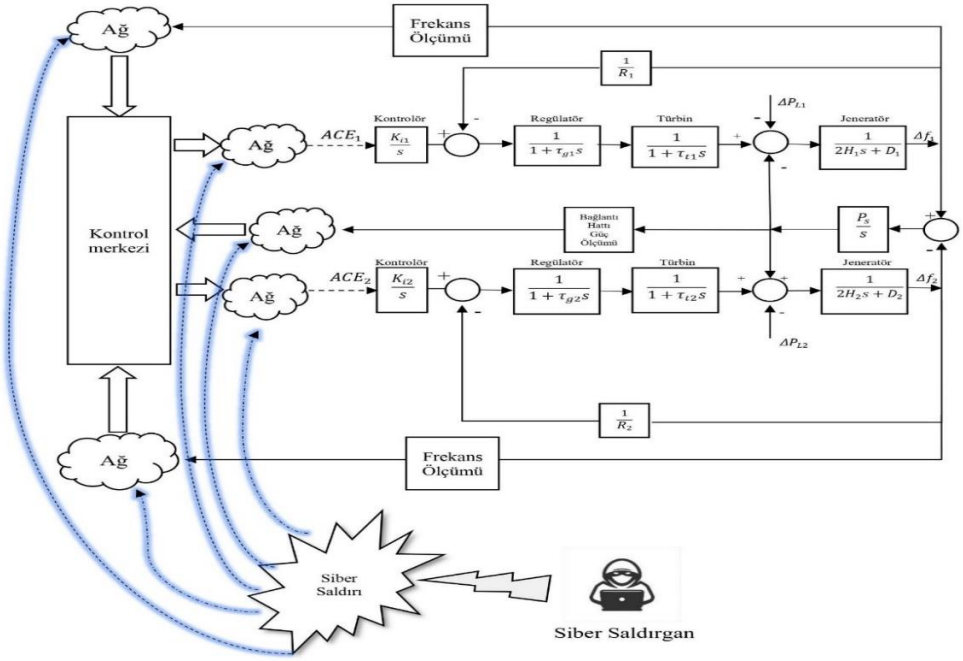
2.4 Otomatik Üretim Kontrolü Siber Zayıflıklar

Yukarıda da açıklandığı gibi OÜK, bir elektrik santralinin hız regülatörlerinin ayar noktalarını düzenleyerek şebeke frekansını istenilen değerde tutmayı sağlamaktadır. Bu ayar noktalarının düzenlenmesi için OÜK, SCADA sistemi tarafından sağlanan bağlantı hattı ve frekans ölçümlerini kullanmaktadır. Her alanda bulunan kontrol

merkezi, Dağıtılmış Ağ Protokolü (DNP3) aracılığıyla sensörler tarafından ölçülen bağlantı hattı ve frekans ölçümlerini almaktadır. Fakat DNP3'ün siber saldırılara karşı zaafiyetleri çeşitli çalışmalarda ortaya koyulmaktadır [60-62]. Bu zaafiyetlerden yararlanan kötü amaçlı siber saldırganlar, OÜK sistemine yönelik veri bütünlüğünü veya veri mevcudiyetini siber saldırılar aracılığıyla etkileyebilmektedirler.

Bu çalışmada kullanılan veri bütünlüğü saldırıları, güç sisteminin siber bölümleri arasında iletilen sinyallerin değiştirilmesi veya bozulması yoluyla gerçekleştirilmektedir [63]. Şekil 2.16'da iki alanlı bir OÜK sisteminin blok diyagramı ve muhtemel saldırı noktaları belirtilmektedir. Saldırganlar ölçüm ve kontrol birimleri arasındaki haberleşme kanallarını sabote ederek ölçümlerin doğruluğunu etkilemekte ve kontrol sisteminin yanlış eylemler yapmasına neden olmaktadırlar.

Öte yandan güç sistemine yapılan bir veri bütünlüğü saldırısı, güç sisteminin ilkelerine uymalıdır [64]. Saldırganların eyleyici ve sensör kanallarına enjekte edecekleri veriler [64] numaralı çalışmada belirtilen sınırlar içinde kalmak zorundadır, aksi halde kötü veri tespit şemaları saldırıları kolayca tespit eder ve saldırı başarısız olur. OÜK'ye yönelik bir bütünlük saldırısının sistem frekansı, kararlılığı ve ekonomik çalışması üzerinde doğrudan etkileri olabilir.



Şekil 2.16: İki alanlı OÜK sisteminin saldırı noktaları.

Farklı bir saldırı türü olan DoS türü saldırılar, büyük miktarda veri göndererek iletişim kanallarını bozmayı amaçlar. Bu saldırıların amacı yüksek miktarda ağ bant genişliği tüketerek, iletişimde kesintiler oluşturarak iletişim hızını yavaşlatmaktır. Başka bir saldırı ile desteklenmedikçe DoS saldırıları OÜK üzerinde önemli bir etkiye sahip olmayabilir. Kontrol sistemi hakkında yeterli bilgiye sahip olmayan saldırganlar DoS türü saldırı politikasını benimsemektedir [65]. DoS türü saldırıların tespit edilmesi kolaydır fakat ağ şartlarının kötü olması algılama performansını etkilemektedir [66]. DoS saldırılarının ana hedef noktası RTU/FÖB ile kontrol merkezini birbirine bağlayan iletişim kanalları ile birlikte regülatör ve kontrol merkezi arasındaki iletişim kanallarıdır. DoS saldırıları, ölçüm verilerinin kontrol merkezine aktarılmasını engelleyebilmekte ve kontrol sinyalinin eyleyiciye gönderilmesini geciktirerek güç sisteminin çalışmasını etkileyebilmektedirler [67]. Düşük işlem hızına ve yetersiz belleğe sahip sunucular DoS saldırılarının ana hedef noktasıdır. Bu çalışmada saldırganların sistem hakkında gerekli bilgiye sahip olduğu kabul edildiğinden ve DoS türü saldırıların kolay tespit edilmesinden dolayı [66] DoS saldırıları uygulanmamaktadır.

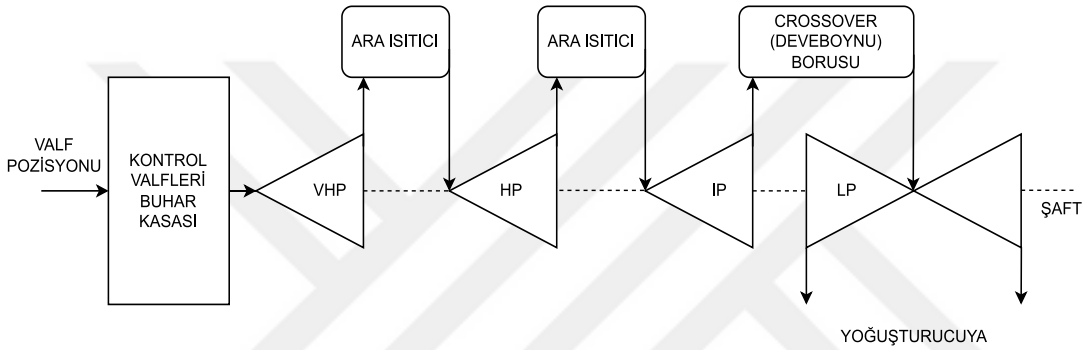
2.5 Test Sistemi-2'nin Modellenmesi

Bu modelde, güç sistemi tipik olarak birbirine bağlı bölgeleri veya şebekeleri temsil eden iki ayrı alana bölünmektedir. Her alanda ikişer jeneratör olmak üzere toplamda dört jeneratör yer almaktadır. Makineler, alanlar arasında elektrik enerjisi alışverişine izin verecek şekilde iletim hatları aracılığıyla birbirine bağlanmaktadır. İki alanlı dört makineli sistemini kullanarak güç sistemlerini modellemenin amacı, sistemin farklı çalışma koşulları ve bozulmalar altındaki dinamik davranışını analiz etmektir. Güç sistemi kararlılığı, kontrolü ve çeşitli faktörlerin sistem performansı üzerindeki etkisi hakkında yapılan analizler için oldukça kullanışlıdır. Alanlar arasındaki etkileşimleri ve bir alandaki bozulmaların diğerini nasıl etkileyebileceğini anlamaya yardımcı olur, böylece kararlılık ve güvenilirliği sürdürmek için etkili kontrol stratejilerinin tasarlanmasını ve uygulanmasını sağlamaktadır.

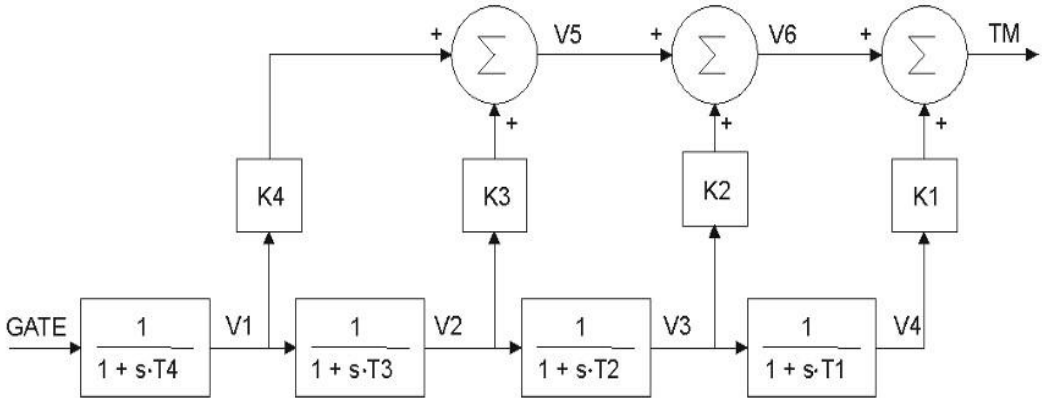
2.5.1 Regülatör ve türbin sistemi

Türbin sistemleri enerji kaynaklarından gelen farklı türdeki enerjiyi mekanik enerjiye dönüştürmektedir. Bu enerji kaynakları su, fosil yakıt, nükleer veya rüzgar olarak

ayrılmaktadır. Bir buhar türbininde, fosil yakıt veya nükleer reaktör kullanan bir kazanda su ısıtılarak buhar oluşturulmaktadır. Buharın oluşturduğu yüksek basınç ve sıcaklık ile rotorun hareket etmesini sağlayan mekanik enerji meydana gelmektedir [68]. Genel olarak buhar türbini, aşırı ısıtılan buhar ile ortaya çıkan ısı ve basınç enerjisini mekanik enerjiye dönüştüren kanat sıralarından oluşmaktadır. Buhar türbinleri için yüksek basınçlı türbin girişlerinde regülatörün kontrol ettiği bir valf bulunmaktadır. Bu valf ile buharın geçişi ayarlanarak şaft hızı kontrol edilmektedir. Şekil 2.17 bu test sisteminde kullanılan buhar türbini konfigürasyonunu göstermektedir. Bu modele karşılık gelen matematiksel model ise Şekil 2.18'de yer almaktadır.



Şekil 2.17: Çift gövdeli çift ara ısıtıcılı buhar türbini konfigürasyonu [69]**.**



Şekil 2.18: Çift gövdeli iki ısıtıcılı buhar türbini yaklaşık lineer modeli [70].

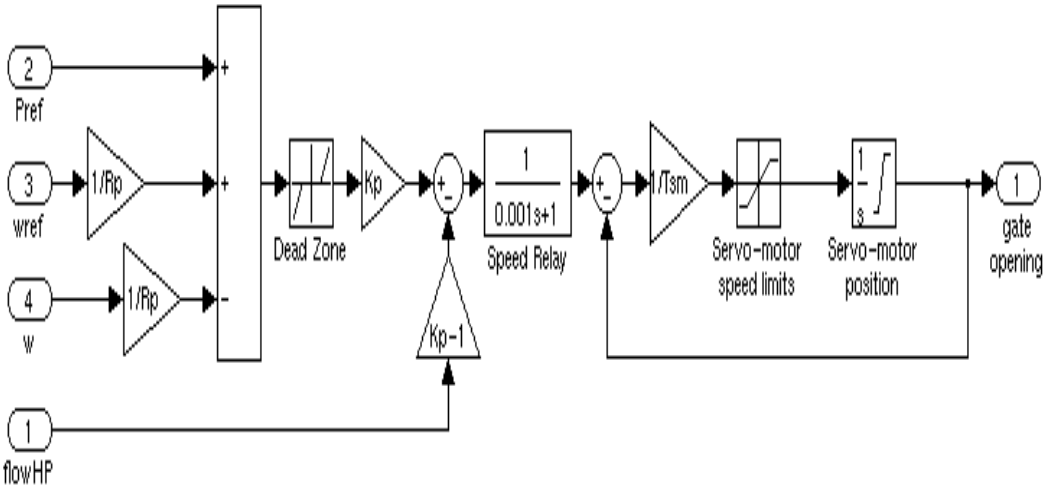
Burada T_4 buhar haznesi zaman sabiti (valften HP'ye doğru(VHP)), T_3 ara ısıtıcı zaman sabiti (HP VHP- IP HP'ye doğru), T_2 ikinci ara ısıtıcı zaman sabiti (HP'den IP'ye doğru) ve T_1 ise aktarma noktası (IP'den LP'ye doğru) zaman sabitidir. K_4 çok

yüksek basınç türbini güç yüzdesi, K_3 yüksek basınç türbini güç yüzdesi, K_2 orta basınç türbini güç yüzdesi ve K_1 ise düşük basınç türbini güç yüzdesidir. Burada K ile temsil edilen terimler türbin tasarımında kullanılır ve türbinlerin güç üretimindeki payını belirtir. K_1, K_2, K_3 ve K_4 toplamı 1'e eşit olmalıdır. Çizelge 2.2'de simülasyonda kullanılan türbin modeli için parametre değerleri yer almaktadır.

Çizelge 2.2: Türbin parametreleri.

T_1 / K_1	T_2 / K_2	T_3 / K_3	T_4 / K_4
0 sn / 0	10 sn / 0.36	3.3 sn / 0.36	0.5 sn / 0.28

Regülatörün ise buhar türbininde üç ana görevi bulunmaktadır. Birinci olarak buhar türbininin hızını kontrol etmektedir. Sürekli olarak değişen enerji taleplerine yanıt vermek için hızlı bir şekilde tepki vererek güç çıkışını ayarlamaktadır. Genel olarak %4-5 aralığında bir hız düşüşü oluşmasını sağlamaktadır. Şekil 2.19'da bir elektro-hidrolik hız kontrol mekanizması görülmektedir.



Şekil 2.19: Buhar türbini hız-regülatör yaklaşık matematiksel modeli [72].

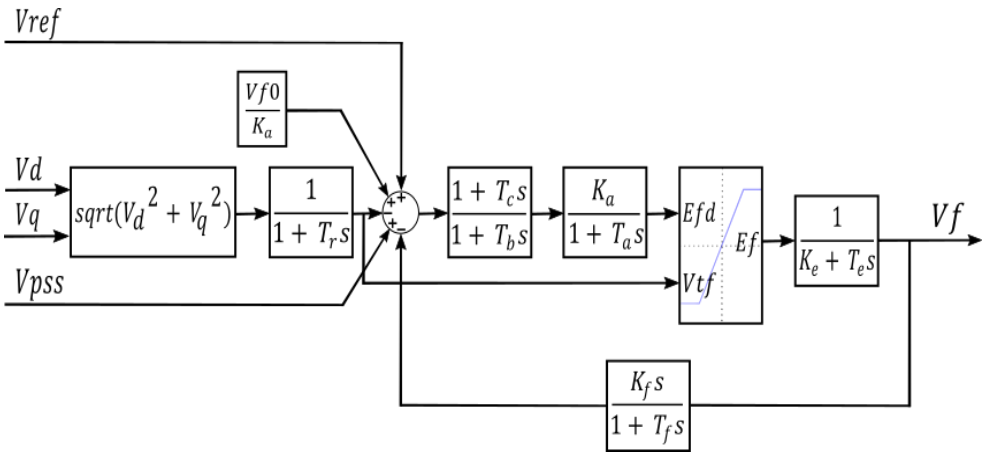
Birinci aşamadaki basınç geri bildirimi (flowHp) ve servo motor geri besleme döngüsü sistemin doğrusallaştırılmasını sağlamaktadır. Simülasyonda kullanılan hız regülatörü için tüm parametre değerleri Çizelge 2.3'de verilmektedir.

Çizelge 2.3: Hız regülatörü parametreleri.

Parametreler	Değerler
K_p (regülatör kazancı)	1
R_p	0.9 pu
D_z (ölü band)	0.036 pu
T_{sr} (hız rölesi zaman sabiti)	0.001 sn
T_{sm} (servo motor zaman sabiti)	0.15 sn
v_{gmin}, v_{gmax} (kapakçık açılma hızları)	[-0.1 0.1] pu/sn
$gmin, gmax$ (kapakçık açılma limitleri)	[0 4.496] pu
P_{m0} (her türbin için başlangıç güçleri)	[0.44494 0.7102 0.44496 0.4451] pu

2.5.2 Uyartım sistemi

Uyartım sistemleri jeneratörlerin alan sargılarına akım sağlamakla görevlidir ve bu sayede gerilim ile reaktif güç akışı kontrolü sağlayarak sistem kararlılığını arttırmaktadır. Yani uyartım sistemi, alan akımını otomatik olarak ayarlayarak terminal gerilimini kontrol etmektedir. Uyartım modeli olarak IEEE Tip 1 seçilmiştir. Şekil 2.20'de simülasyonda kullanılan uyartım blok diyagramı görünmektedir. Ayrıca simülasyonda kullanılan bu model için parametre değerleri Çizelge 2.4'de yer almaktadır. Bu model için MATLAB/Simulink kütüphanesi içinde bulunan uyartım sistemi (Excitation System) bloğu kullanılmıştır. Şekil 2.20'de ise bu bloğun detaylı gösterimi yer almaktadır.



Şekil 2.20: IEEE Tip 1 uyartım blok diyagramı.

Çizelge 2.4: Uyartım devresi parametreleri.

Uyartım Verileri	Değer
Alçak geçiren filtre zaman sabiti (T_r)	0.02 sn
Regülatör kazancı (K_a)	200
Regülatör zaman sabiti (T_a)	0.001 sn
Uyartım sabiti (K_e)	1
Uyartım zaman sabiti (T_e)	0 sn
Sönümleme filtresi kazancı (K_f)	0
Sönümleme filtresi zaman sabiti (T_f)	0 sn
Maksimum regülatör çıkış kazancı (V_{RMAX})	12.3 pu
Minimum regülatör çıkış kazancı ($V_{RMİN}$)	0 pu
Terminal voltajı başlangıç değeri (V_{T0})	1 pu
Alan voltajı başlangıç değeri (V_{F0}) (M_1-M_2-M_3-M_4)	(1.2116-1.5042-1.1476-0.96426) pu
Geçici kazanç azalma öncü zaman sabiti (T_b)	0 sn
Geçici kazanç azalma gecikme zaman sabiti (T_c)	0 sn

2.5.3 Jeneratör modeli

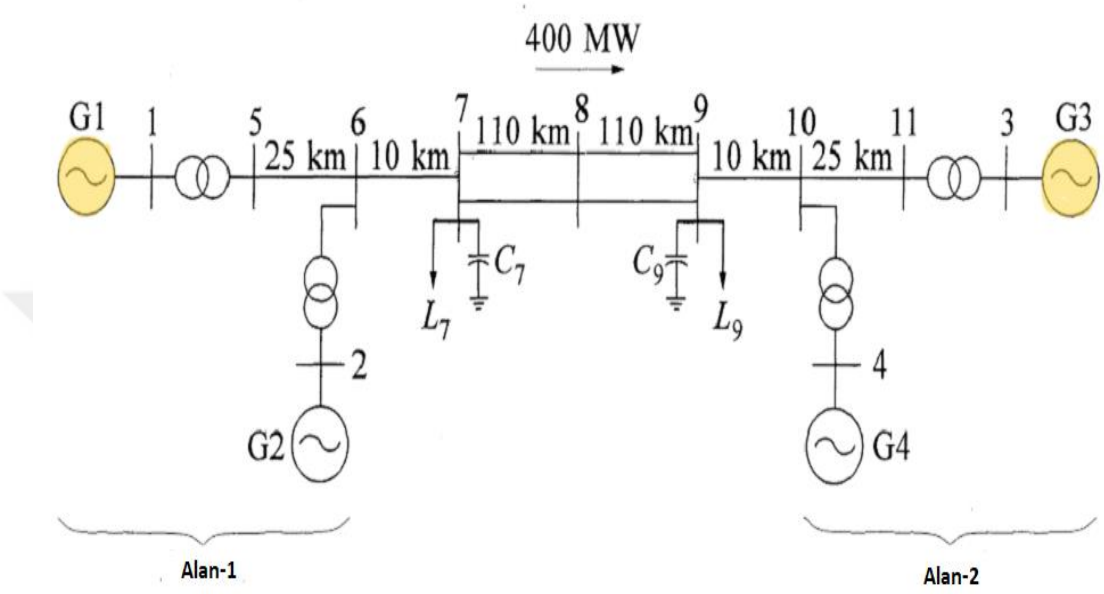
Simülayon için kullanılan jeneratörde mekanik güç ölçümü hız yönetim sisteminden, alan gerilimi ölçümü ise uyartım devresinden alınmaktadır. Ayrıca jeneratörün stator alan gerilimi, rotor hızı, rotor hız sapması, rotor açısı, elektriksel gücü ve yük açısı ölçümleri, kontrol-ölçüm birimlerine gönderilmektedir. Simülasyonda kullanılan jeneratörler için parametre değerleri aşağıda yer alan Çizelge 2.5'de görünmektedir.

Çizelge 2.5: Jeneratör verileri.

Jeneratör verisi	Jeneratör 1	Jeneratör 2	Jeneratör 3	Jeneratör 4
Bara numarası	1	2	3	4
Tipi	PV	Swing	PV	PV
Aktif güç (MW)	700	-	700	700
Voltaj (pu)	1	1	1.03	1.03
Baz güç (MVA)	900	900	900	900
Sızıntı reaktansı X_l (pu)	0.2	0.2	0.2	0.2
Stator rezistansı R_s (pu)	0.0025	0.0025	0.0025	0.0025
Senkron boyuna reaktans X_d(pu)	1.8	1.8	1.8	1.8
Geçici boyuna reaktans X'_d(pu)	0.3	0.3	0.3	0.3
Hızlı geçici boyuna reaktans X''_d (pu)	0.25	0.25	0.25	0.25
Boyuna eksenin açık devre geçici zaman sabiti T'_{d0} (sn)	8	8	8	8
Boyuna eksenin açık devre hızlı geçici zaman sabiti T''_{d0} (sn)	0.03	0.03	0.03	0.03
Senkron enine reaktans X_q(pu)	1.7	1.7	1.7	1.7
Geçici enine reaktans X'_q(pu)	0.55	0.55	0.55	0.55
Hızlı geçici enine reaktans X''_q(pu)	0.25	0.25	0.25	0.25
Enine eksenin açık devre geçici zaman sabiti T'_{q0}(sn)	0.4	0.4	0.4	0.4
Enine eksenin açık devre hızlı geçici zaman sabiti T''_{q0}(sn)	0.05	0.05	0.05	0.05
Eylemsizlik sabiti H(sn)	0.08335	0.08335	0.1085	0.1085

Şekil 2.21'de ise 4-makineli 2-Alanlı test sistemi hat uzunlukları ile birlikte tek hat gösterimi verilmektedir. Burada sarı ile boyanan jeneratörlere OÜK sistemi

eklenmektedir. Diğer jeneratörler birincil kontrol döngüsü ile kontrol edilmektedir. Hat uzunlukları Şekil 2.21'de verildiği gibidir. Hat parametreleri 100 MVA, 230 kV baz değerinde birim başına $r = 0.0001\ \text{pu/km}$, $x_L = 0.001\ \text{pu/km}$, $b_C = 0.00175\ \text{pu/km}$ olarak verilmektedir. Bu model ile siber saldırı modelleri ve tespit algoritmalarının gerçek bir güç sistemi üzerindeki etkinliği araştırılmaktadır.



Şekil 2.21: 2-Alanlı Test Sistemi Tek Hat Gösterimi [68].

İki alanlı test sistemi [68], 220 km uzunluğunda iki 230 KV hat ile birbirine bağlanan büyük ölçüde simetrik iki alandan oluşmaktadır. Her birinin 20KV/900 MVA değerinde iki özdeş yuvarlak rotorlu jeneratörü vardır. Temel durum yük akışı, sistemdeki tüm jeneratörlerin her biri yaklaşık 700 MW üretecek şekildedir. Alan 1 ve 2 yükleri sırasıyla 976 MW ve 1765 MW iken, yüklerin her yerde sabit empedanslı yük modeli olduğu varsayılmaktadır. Gerilim profilini iyileştirmek için her alana 187Mvar kapasitörler eklenmektedir. Ek olarak simülasyonlarda 2-Alanlı test sistemine farklı oranlarda rüzgar üretimi entegre edilmektedir.

2.6 Rüzgar Enerjisi Üretimi

Rüzgar, yenilenebilir temiz enerji kaynaklarından biridir. Rüzgar gücünden üretilen enerji sayesinde karbondioksit, sülfür dioksit ve daha farklı havayı kirleten partiküllerin atmosfere salınımı engellenmektedir. Rüzgar enerjisinin geleneksel enerji kaynaklarına göre farklı avantajları vardır ve dünya çapında en hızlı büyüyen

yenilenebilir enerji kaynağıdır. Enerji talebine olan pozitif etkileri dolayısıyla Rüzgar Enerjisi Sistemlerinin (RES) kurulumu artmaktadır. RES'lerin karakteristikleri güç sistemlerinin çalışmasını ve kararlılığını etkilemektedir. Bu nedenle rüzgar türbinlerinin analizi ve modellenmesi güç sistemleri çalışmaları için oldukça önemlidir.

Bir rüzgar enerjisi dönüştürme (RED) sistemi rüzgarın sahip olduğu kinetik enerjiyi mekanik enerjiye dönüştürmektedir. Bir RED sistemi genellikle rüzgar türbini, dişli kutusu, jeneratör, konvertör, kontrol sistemleri ve kuleden meydana gelmektedir. Bu sistemler uzak yerlerdeki izole kullanıcıların yanı sıra elektrik şebeke sisteminin bir parçası olarak da kurulabilmektedirler. Elektrik enerji sistemlerinde artan RES oranı ile birlikte farklı sorunlar da ortaya çıkmaktadır. RED sistemlerini elektrik şebekesine bağlamak, geleneksel hidrolik veya buhar bazlı santrallere göre çok daha zor bir işlemdir. Anlaşıldığı üzere rüzgar santrallerinin simülasyonu ve geleneksel elektrik şebekelerine entegre edilmesi günümüz modern elektrik şebekelerini yansıtması açısından oldukça önemlidir. Ek olarak rüzgar hızındaki değişiklikler üretilen gücün büyüklüğünü, frekansını ve voltajını etkilemektedir. Simülasyonların gerçekliğini arttırabilmek için sabit bir rüzgar hızı almak yerine değişken olan bir rüzgar hızı modellenmektedir.

2.6.1 Rüzgar türbini modellenmesi

Rüzgâr türbini modeli, rüzgar hızını jeneratör rotor hızı ile ilişkilendirmektedir. Tipik bir türbin konfigürasyonunda, rüzgar enerjisini ile bir jeneratör rotorunu döndüren üç kanat bulunmaktadır. Jeneratör hız gereksinimlerine bağlı olarak türbin ile jeneratör arasına bir dişli kutusu yerleştirilebilmektedir. Türbin modeli bloğu rüzgar hızı ve elektriksel tork girdilerini almakta ve çıkış olarak jeneratör hızı meydana gelmektedir. Türbin modeli iki alt modele ayrılmaktadır. (1) Rüzgar enerjisini mekanik torka dönüştüren bir aerodinamik model ve (2) jeneratör bloğundan gelen elektriksel tork girişi ve jeneratör hız çıkışı ile mekanik torku ilişkilendiren bir aktarma organı modeli. Bu çalışmada, rüzgar hızı standart sapması, rastgele rüzgar gücünü gerçeklemek için MATLAB/Simulink®'teki beyaz gürültü bloğundan iletilen rastgele dalgalanma ile çarpılmaktadır.

2.6.1.1 Rüzgar türbini aerodinamik model

Rüzgar türbini aerodinamik modeli, rüzgar hızını türbinin mekanik çıktısına dönüştürmektedir. Bu modelde rüzgar türbininin $R = 40.06$ m uzunluğunda 3 adet kanadı olduğu kabul edilmektedir. Bu durumda mekanik güç çıkışı denklemi aşağıdaki gibi verilmektedir.

$$P_t = 0.5p\pi R^2 C_p(B, \lambda)v_w^3 \text{ [W]} \tag{2.18}$$

Burada p hava yoğunluğu ve değeri ise 1.225 kg/m^3, $\pi = 3.1416$, v_w rüzgâr hızı olmak üzere birimi m/s ve $C_p(B, \lambda)$ ise kanatların güç katsayısıdır. Teorik olarak $C_p = 0.59$ ile sınırlıdır ve bu Betz limiti olarak adlandırılır. C_p, rüzgâr enerjisinin türbin tarafından çekilebilen enerjisini temsil eder ve bu değer B ile λ olmak üzere iki parametreye bağlıdır. Sahada kullanılacak türbinler için üreticiler genellikle bir performans eğrisi belirler. Fakat akademik çalışmalar için sayısal yaklaşık denklemler kullanılabilir. Mei [69] tarafından verilen (2.19)'daki denklem kullanılmıştır.

$$C_p(B, \lambda) = 0.5176\left(\frac{116}{\lambda+0.08B} - \frac{4.06}{1+B^3} - 0.4\,\beta - 5\right)e^{\left(\frac{-21}{\lambda+0.08B}+\frac{0,735}{1+B^3}\right)}+0.0068\lambda \tag{2.19}$$

Burada B kanat açısı ve λ ise uç hız oranını temsil etmektedir. Türbin kanatları, türbin hızını kontrol etmek için rüzgarın içine ve dışına döndürülebilir. Kanat açısı, kanadın uzunlamasına ekseni üzerindeki dönüş açısını ifade etmektedir. Bu bölümde kullanılan rüzgar türbini verileri için kanat açısı 0 ila 23 derece arasında değişmektedir; kanatlar maksimum enerjiyi çıkaran rüzgara karşı olduğunda kanat açısı sıfır derece olmalıdır.

Verilen türbin parametreleri için, $C_{pmax} = 0.48$ olarak belirlenir bunun için , $B = 0$ ve $\lambda_{opt} = 8.1$ olmalıdır. Denklem 2.18'de $C_p = C_{pmax}$ ve Pt = 5 MW yerine koyulduğunda, $B = 0$'da nominal çıkışı üretmek için gereken rüzgar hızı 15 m/s olarak elde edilir. Bu, türbinin nominal rüzgar hızıdır.

2.6.1.2 Türbin jeneratör mekanik aktarma organı modeli

Rüzgar türbini modeli oluşturulurken ikinci olarak jeneratör bloğundan gelen elektriksel tork girişi ve jeneratör hız çıkışı ile mekanik torku ilişkilendiren bir aktarma organı modeli oluşturulmalıdır. Bu model türbin, dişli kutusu ve jeneratör kütlelerini içerir. Aktarma organı modeli Şekil 2.22'de gösterildiği üzere iki kütle ve onları birleştiren bir şaft ile temsil edilmiştir. Denklem (2.20-2.23) modelin matematiksel

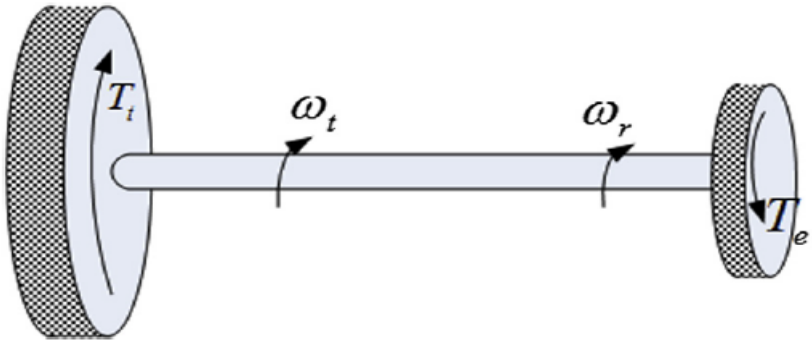
denklemler ile açıklanması için oluşturulur. Parametreler ve değerleri Çizelge 2.6'da listelenmiştir.

$$\frac{d}{dt}\omega_g = \frac{1}{2H_g}(T_s - T_g) \tag{2.20}$$

$$T_s = \mathrm{k}_{tg}\theta_{tg} + \mathrm{c}_{tg}\frac{d}{dt}\theta_{tg} \tag{2.21}$$

$$\frac{d}{dt}\theta_{tg} = \omega_{elB}(\omega_t - \omega_g) \tag{2.22}$$

$$\frac{d}{dt}\omega_t = \frac{1}{2H_t}(T_t - T_s) \tag{2.23}$$



Şekil 2.22: İki kütleli bir rüzgar türbini aktarma modeli.

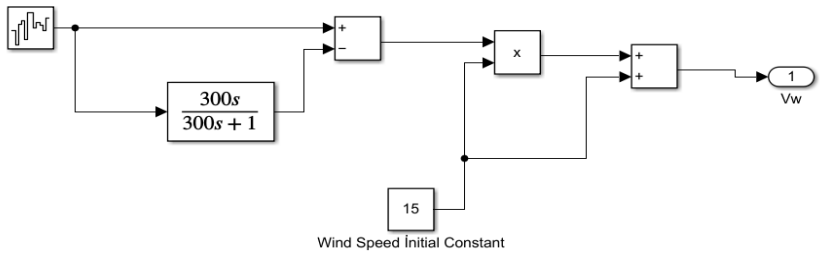
Çizelge 2.6: Rüzgar türbini aktarma organı parametreleri.

Parametre	Sembol	Değer
Türbin Eylemsizlik değeri	H_t	4 sn
Jeneratör Eylemsizlik değeri	H_g	0.4 sn
Aktarma organı mili sertliği	k_{tg}	0.3 pu/el.rad
Aktarma organı sönümleme katsayısı	c_{tg}	0.01 pu.sn/el.rad
Elektriksel baz hız	ω_{elB}	$2\pi 50$ rad/sn

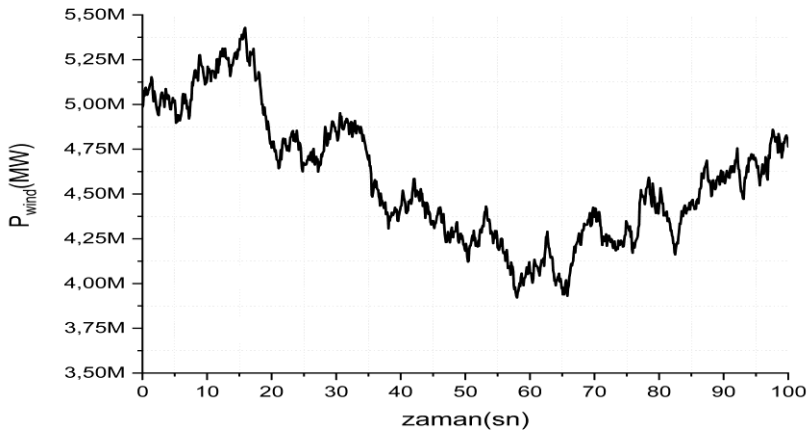
Burada T torku, ω dönme hızını, θ_{tg} ise şaft burulma açısını temsil etmektedir. Alt simge g jeneratörü, s şaftı t ise türbini temsil etmektedir. Türbin mekanik torku T_t ve türbine bağlı jeneratör tarafından üretilen elektriksel tork T_g bu denklem sistemine girdi olarak verilmelidir. Türbin hızı ω_t ve jeneratör hızı ω_g denklemlerden elde edilmektedir. Bu denklemler ile blok diyagramı oluşturulmaktadır. Oluşturulan bu entegre model rüzgar hızını ve jeneratör elektrik torkunu girdi olarak, jeneratör hızını çıktı olarak almaktadır. Değişkenler yüklendikten sonra türbin modeli oluşturulmaktadır.

2.6.2 Rüzgar hızı modellemesi

Şekil 2.23'de görüldüğü üzere rüzgar hızı modellemesi için beyaz gürültü (white noise) bloğundan elde edilen rassal bir hız dalgalanması başlangıç rüzgar hızı ile çarpılmaktadır [70,71]. Sonuç olarak blok çıkışında elde edilen güç çıkışı Şekil 2.24'de gösterilmektedir.



Şekil 2.23: MATLAB/Simulink ile oluşturulan rüzgar hızı modellemesi.



Şekil 2.24: MATLAB/Simulink ile modellenen rüzgar türbini güç çıkışı.

3. YANLIŞ VERİ ENJEKSİYON SALDIRILARININ OTOMATİK ÜRETİM KONTROLÜNE ETKİLERİ

OÜK sistemine yönelik ana saldırı türleri, hizmet reddi saldırıları (verilerin kullanılabilirliğini etkileyen) ve veri bütünlüğü saldırıları (iletilen verilerin bozulması yoluyla sistem bütünlüğünü etkileyen) olmak üzere iki ana başlığa ayrılır. FDI saldırıları OÜK sistemlerinde frekans ve ACE gibi gerçek zamanlı verileri bozabilen bir bütünlük saldırısı türüdür [5]. Bu saldırıda, saldırgan genellikle önceden hazırladığı saldırı şablonlarını takip eder [64]. Saldırganın amacı sistem ölçümlerini değiştirerek ekipman hasarına, son kullanıcıların güç kesintisine veya sistem genelinde elektrik kesintisine neden olmaktır. Saldırgan, önce sistem yapılandırmasını ortaya çıkarmak ve gerçek zamanlı veriler elde edebilmek için sistemin açıklıklarını kullanır. Ardından bu kaynaklar ile sistemin normal çalışmasını etkilemeye çalışır. FDI saldırıları, OÜK sisteminin ölçüm ve kontrol kanallarına, saldırı şablonları veya veri bozma stratejileri ile oluşturulmuş saldırı vektörlerini enjekte etmek üzerine kurulmuştur.

DNP3'ün siber saldırılara karşı zafiyetlerinden dolayı saldırganlar iletilen verilere erişim sağlayabilirler. Ek olarak saldırganların bu zafiyetlerden faydalanarak ölçümlere saldırdığında ACE değeri yani kontrol sinyali yanlış hesaplanır. Bunun sonucunda jeneratör üretimi arttırmak ya da azaltmak gibi yanlış bir konum alır ve şebeke frekansında istenmeyen değişiklikler olur. OÜK her 5 saniyede bir kontrol komutu ürettiği için, ISO/RTO düzeyinde tipik olarak her 5 dakikada bir çalışan mevcut ölçüm değerlendirme tekniklerinden olan durum tahmincisi ile yanlış verilerin tespit edilmesi mümkün değildir [5]. Bu OÜK'yi ölçüm bozulmasını içeren saldırılara karşı savunmasız bırakır.

Saldırganın atak şablonuna uygun ölçümleri enjekte edebilmesi için OÜK'nin çalışmasına ek olarak hedef sistem hakkındaki bilgileri bilmesi gereklidir. Bu bilgiler her iki alan için yük tahminleri, planlanan bağlantı hattı güç akışı, yük frekansı hassasiyet parametresi 'D', droop constant 'R' ve frekans bias 'B' değerlerini içerir.

3.1 Saldırı Şablonları

i, ii ve iii bölümlerinde incelenen saldırı şablonları [72]'den alınmıştır.

3.1.1 Ölçekleme saldırısı

Ölçekleme (scaling) saldırısı, atak parametresi λ_s değerine bağlı olarak doğru ölçümlerin değiştirilmesini sağlar.

$$y^*(t) = \begin{cases} y(t) & t \notin \tau_a \; için \\ (1+\lambda_s) * y(t) & t \in \tau_a \; için \end{cases} \quad (3.1)$$

λ_s saldırı parametresi, t zamanı, τ_a ise saldırı periyodunu temsil etmektedir.

3.1.2 Rampa saldırısı

Rampa saldırısı, zamanla orantılı olarak artan veya azalan bir rampa fonksiyonu olan $\lambda_r * t$'nin doğru ölçümlere eklenmesiyle gerçek ölçümlerin değiştirilmesi işlemidir. λ_r saldırı parametresi, t zamanı, τ_a ise saldırı periyodunu temsil etmektedir.

$$y^*(t) = \begin{cases} y(t) & t \notin \tau_a \; için \\ y(t) + \lambda_r * t & t \in \tau_a \; için \end{cases} \quad (3.2)$$

3.1.3 Rassal (Random) saldırı

Bu saldırı vektörü, gerçek ölçüme rastgele bir pozitif değer eklenerek oluşturulur.

$$y^*(t) = \begin{cases} y(t) & t \notin \tau_a \; için \\ y(t) + rand(a,b) & t \in \tau_a \; için \end{cases} \quad (3.3)$$

3.1.4 Sabit değer (Compensation) saldırısı

Bu şablonda, saldırgan bir Ortadaki Adam Saldırısı (MITMA) başlatarak jeneratörlere gönderilen ACE değerlerini değiştirir. Bu değere göre saldırı farklı sonuçlar doğurabilir ve aynı zamanda farklı türlere ayrılabilir. Bu çalışmada kullanılan saldırı şablonu [73]'dan alınmıştır.

3.1.4.1 Yüksek-düşük sabit değer "over-under compensation" saldırıları

Saldırı sırasında frekans ve bağlantı hattı gücünün nominal değerinden sapma miktarı, kontrol merkezine gönderilmeden önce m katsayısı ile çarpılır. Bu nedenle ACE_i değeri $m_i \; x \; ACE_i$ olarak değişir. Buradaki m_i değerine göre saldırı yüksek veya düşük "over-under" saldırı olarak gerçekleştirilir. Eğer $m_i > 1$ ise yüksek, $0 \leq m_i < 1$ ise

düşük saldırı oluşturulur. Yüksek/düşük sabit değer saldırısı uygulandığında frekans ve ACE sinyallerinin davranışını daha detaylı incelemek adına, N alanlı bir güç sisteminin i alanında üretim ve tüketim arasında oluşan dengesizliğe ΔP_{L_i} ve alan 1'den alan N'e kadar olan frekans biası ise β_i'den β_N'e kadar temsil edilmiştir. Saldırı olmayan duruma göre i alanındaki açısal frekans ve bağlantı hattı güç akışı aşağıdaki gibi olur.

$$\Delta\omega_i = \frac{-\Delta P_{L_i}}{\sum_{j=1}^{N} \beta_j} \tag{3.4a}$$

$$\Delta P_{tie_{i,j}} = \beta_j \Delta\omega_i \qquad j\ \varepsilon\ \delta_i \tag{3.4b}$$

k zaman adımında i alanında ΔP_L büyüklüğünde bir yük değişimi meydana geldiğinde 3.4 numaralı denklemlerdeki $\Delta\omega_i$ ve $\Delta P_{tie_{i,j}}$ değerleri denklem 2.5'de yerine koyulursa i alanı için alan kontrol hatası sinyali $ACE_i = \Delta P_{L_i}$, diğer alanlar için ise sıfır olur [74]. OÜK sistemi ACE değerini sıfır olmaya zorladığından i alanının frekans ve bağlantı hattı gücünün sıfır olabilmesi için k zaman adımında düzeltme sinyali $-ACE_i^k$ olmalıdır. Fakat saldırı olduğu durumda ACE_i^k sinyali kontrol merkezine gönderilmeden önce m_i katsayısı ile çarpıldığı için $ACE_i^k\ x\ m_i = m_i \Delta P_L$ olur ve i alanındaki üretim cevabı $-\Delta P_{L_i}$ olacağına $-m_i \Delta P_L$ olur. Bunun sonucunda üretim ve tüketim arasında $(1 - m_i)\Delta P_{L_i}$ kadar bir eşitsizlik meydana gelir [73].

3.1.4.2 Negatif sabit değer saldırıları

Bu saldırı yüksek/düşük sabit değer saldırısı ile aynıdır fakat bu saldırıda m değeri negatiftir. Negatif m_i değeri OÜK sisteminin çalışması üzerinde pozitif m_i değerine göre ters yönde bir etki yapar. Bu saldırılar saldırının başladığı zamanki ACE_i^k veya ΔP_{L_i} değerine göre sistem frekansını arttırıp azaltabilir. Saldırıda yük atma frekansı olan 59.3 Hz [75] değerini tetikleyecek şekilde frekansın düşmesi amaçlanmıştır.

3.1.5 İşaret (Flip) saldırısı

Bu şablonda saldırgan jeneratörlere gönderilen her ACE değerinin işaretini değiştirir, saldırgan, ölçüm sinyallerini, doğru ölçümler gibi görünecek, ancak zıt işaretli olacak şekilde manipüle eder. OÜK sistemi, jeneratörlerin güç çıkışını artırarak veya

azaltarak frekansı 60 Hz'lik nominal değerine geri getirmeye çalışır. Bununla birlikte, manipüle edilmiş sinyaller, potansiyel olarak yaygın elektrik kesintilerine ve hatta jeneratörlere zarar verecek eylemlerde bulunmasına neden olur. Bu nedenle, işaret saldırısı elektrik şebekesinin güvenilirliği ve istikrarı için ciddi bir tehdit oluşturur ve bunları tespit etmek için önlemlerin alınması önemlidir. Saldırılan bir ACE değerinin hesaplama işleminin değişimi aşağıda açıklanmaktadır. Bu sayede saldırıların etkisinin anlaşılabilmesi amaçlanmaktadır.

i alanı için ACE sinyali denklem 3.5'de verilmektedir.

$$\mathrm{ACE_i} = \sum_{\mathrm{j}\varepsilon\delta_\mathrm{i}} \Delta\,\mathrm{P_{ij}} + \mathrm{B_i}\Delta\omega_\mathrm{i} \tag{3.5}$$

Burada $\Delta \mathrm{P_{ij}}$, planlanan değere göre oluşan bağlantı hattı güç akışı sapmasıdır, $\Delta\omega_i$ nominal açısal frekans değerinden sapmadır. B_i bir bozulma sırasında birbirine bağlı iki alanın karşılıklılığını belirleyen frekans bias faktörüdür. δ_i, i alanının bağlı olduğu alanlar kümesidir. Saldırılmış ACE_i.c ifadesini elde etmek için çeşitli saldırı modelleri ACE açılımına entegre edilebilir.

$$\mathrm{ACE_i.c} = \sum_{\mathrm{j}\varepsilon\delta}(\Delta\mathrm{P_{ij}} + \mathrm{a_{tie}}) + \beta_\mathrm{i}(\pi\omega_\mathrm{i} + \mathrm{a_f}) \tag{3.6}$$

Burada a_{tie} ve a_f sırasıyla bağlantı hattı saldırısı ve frekans saldırısını göstermektedir. Saldırgan herhangi bir ölçüm türünü veya her ikisini birden hedef alabilir.

3.2 Tespit Edilemez Saldırı Şablonu Oluşturulması

Saldırıların amacına ulaşması için tespit edilmemesi oldukça önemlidir. Enerji yönetim sisteminde alarm verilmemesi için maximum ACE değerinin $\pm 0.05\,pu$ olduğu varsayılır. Ayrıca ölçümler kısa bir zaman periyodunda önemli ölçüde değişmemelidir.

$$\left|\frac{\mathrm{ACE_{i,t}} - \mathrm{ACE_{i,t+T}}}{\mathrm{T}}\right| < \psi \tag{3.7}$$

$$\left|\mathrm{ACE_i^A}\right| < \mathrm{ACE_{MAX}} \tag{3.8}$$

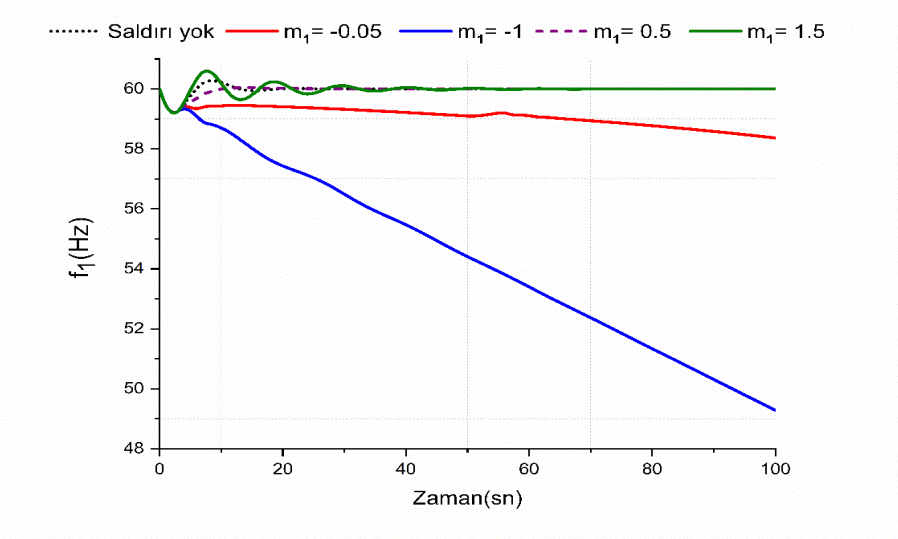
Burada $ACE_{i,t}$, i alanı ve t zamanındaki ACE değerini, T birbiri ardına gelen iki ACE örneğinin ölçüldüğü zamanı ψ ise ACE sinyalinin maksimum eğimini temsil

etmektedir. Bu nedenle bu çalışmada ACE sinyalinin maksimum değerinin $\pm 0.05\ pu$ olmak kaydıyla yavaş etkisini gösterecek şekilde bir saldırı sinyali oluşturulmaktadır. Eğer denklem 3.7 ve denklem 3.8'deki eşitsizlikler dikkate alınmadan saldırı şablonu oluşturulursa kötü veri tespit şemaları sistemde saldırı olduğunu tespit edebilir. Bu eşitsizlikler dikkate alınarak OÜK sistemine yapılacak bir saldırının klasik veri doğrulama yöntemleriyle tespit edilmesi oldukça zordur.

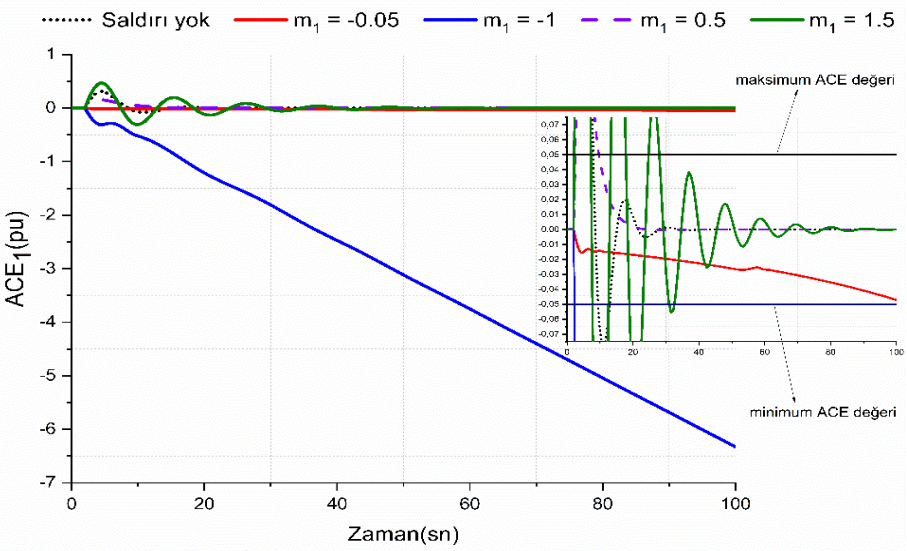
3.2.1 Saldırı parametresi seçimi

3.2.1.1 Sabit değer "Compensation" saldırısı parametre seçimi

Bu bölümde, saldırgan açısından bakıp, sistem frekansını yük atmayı tetikleyecek olan 59.3 Hz değerine düşürmeyi ve aynı zamanda veri kontrol algoritmalarının saldırıyı tespit edemeyeceği şekilde bir saldırı şablonu oluşturulması amaçlanmaktadır. Şekil 3.1'de $m_1 = 0.5, 1.5$ ve 1 (saldırı yok) olarak seçilmektedir. t = 0s'dan t = 100s'e kadar alan-1'e saldırı yapılmaktadır. Bu saldırı sonucunda alan-1 frekans sapması Şekil 3.1'de görülmektedir. Şekil 3.2'de ise Alan-1 ACE sinyali görülmektedir. Burada ACE sinyali generatör aktif gücüne göre normalize edilmekte ve pu cinsinden verilmektedir. Şekil 3.1 ve Şekil 3.2'den görüldüğü gibi düşük parametere değerli FDI'lar OÜK sisteminin çalışmasıyla aynı yönde hareket ettikleri için sistem frekansını ve ACE sinyalini gözle görülür bir şekilde değiştirmemektedirler. Bunlara ters olarak yüksek parametre değerli FDI'lar frekansı önemli ölçüde etkileyebilmelerine rağmen büyük ACE salınımlarına neden olmaktadırlar. Yük değişimi sırasında sisteme yüksek sabit değer saldırısı yapılırsa, generatörlerin ayar noktaları gerektiğinden m kat fazla olacak şekilde değişmekte ve bu da sistem frekans sapmasını olumsuz yönde etkilemektedir. Bu saldırı türü tercih edilmez çünkü büyük ACE salınımlarına neden olduklarından tespit edilmeleri kolaylaşmaktadır.



Şekil 3.1: Sabit değer "compensation" saldırıları sırasında Alan 1 frekansı.

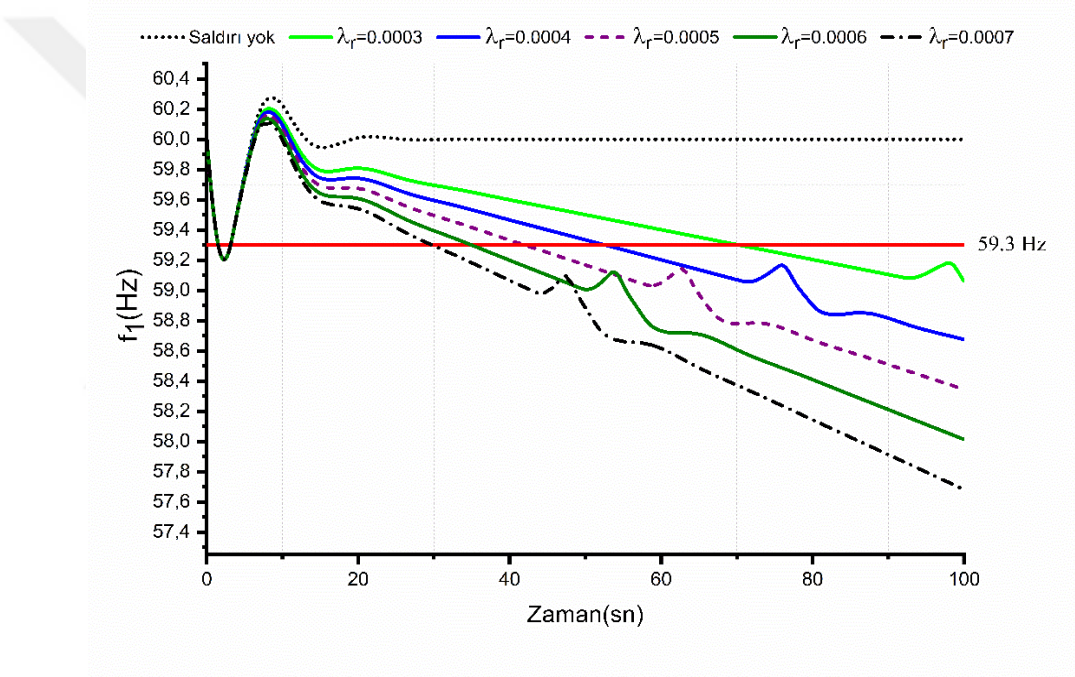


Şekil 3.2: Sabit değer "compensation" saldırıları sırasında ACE_1 değeri.

Şekil 3.1'de $m_1 = -0.05$ ve $m_1 = -1$ olacak şekilde negatif sabit değer saldırısı yapıldığı sırada frekans sapması grafikleri görülmektedir. Bu saldırılar, t = 0 s, alan-1'de 0.1 pu değerinde bir yük artışı olduğu anda yapılmaktadır. Şekil 3.1'den görüleceği üzere negatif sabit değer saldırısı sırasında m_1 değeri küçüldükçe sistem frekansı daha hızlı yük atmaya gitmektedir. Fakat Şekil 3.2'ye bakıldığında negatif sabit değer saldırısı sırasında küçük m_1 değerleri için ACE değerinin belirtilen ± 0.05pu değerini hızlıca geçtiğini ve veri kalitesi alarmlarını tetikleyeceği anlaşılmaktadır. Bu nedenle hem yük atmayı tetikleyecek hem de ACE değerini hata sınırları içinde tutabilecek olan $m_1 = -0.05$ değeri parametre olarak seçilmektedir.

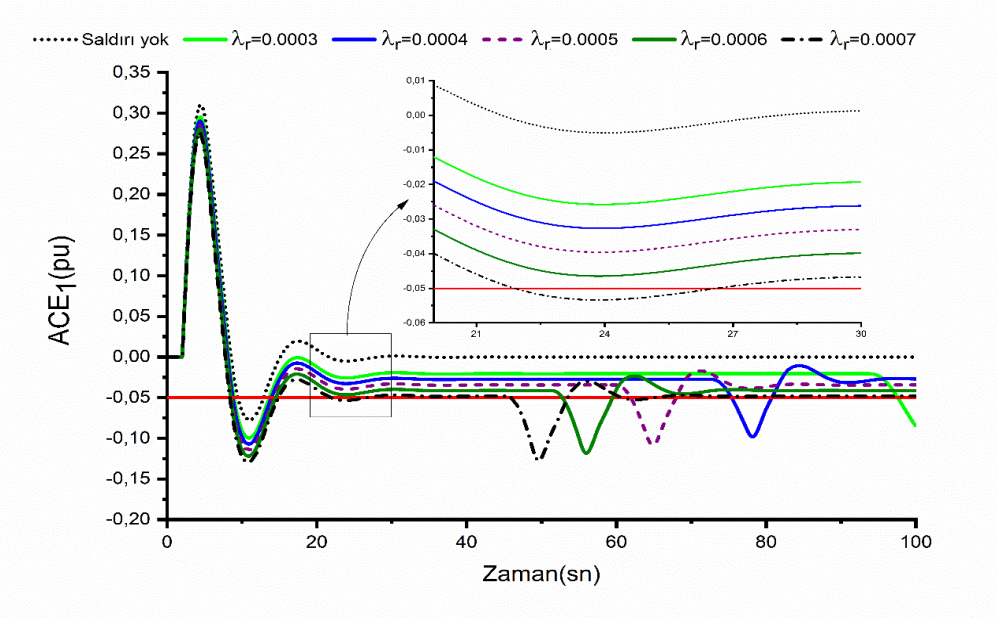
3.2.1.2 Rampa saldırısı parametre seçimi

Buradaki saldırı modeli [72]'de incelenen saldırı modelini sunmaktadır. Rampa saldırısı, zamanla orantılı olarak artan veya azalan bir rampa fonksiyonu olan $\lambda_r * t$'nin doğru ölçümlere eklenmesiyle gerçek ölçümlerin değiştirilmesi işlemidir. Saldırgan açısından λ_r parametresinin seçimi çok önemlidir. Parametre seçimi sonucunda hem amacına ulaşmalı hem de sistemde veri kalitesi alarmı verdirmemelidir. Şekil 3.3'de farklı λ_r saldırı parametreleri sonucunda bir rampa saldırısının Alan-1 frekansına olan etkileri gösterilmektedir. Görüldüğü üzere $\lambda_r = 0.0007$ değerinde frekans en hızlı şekilde yük atma frekansı olan 59.3 Hz değerine ulaşmaktadır.



Şekil 3.3: Farklı saldırı parametreleri ile rampa saldırısı sırasında f_1 değişimleri.

Fakat $ACE_1 \pm 0.05$ (pu) değerlerine ulaşırsa alarmlar tetiklenecek ve sisteme siber saldırı olduğu anlaşılacaktır. Bu kısıt dikkate alındığında $\lambda_r = 0.0006$ olarak seçilmektedir. Şekil 3.4'e bakıldığında farklı saldırı parametre değerleri sonucunda ACE değerinde oluşan hata dinamikleri detaylı olarak gösterilmektedir.

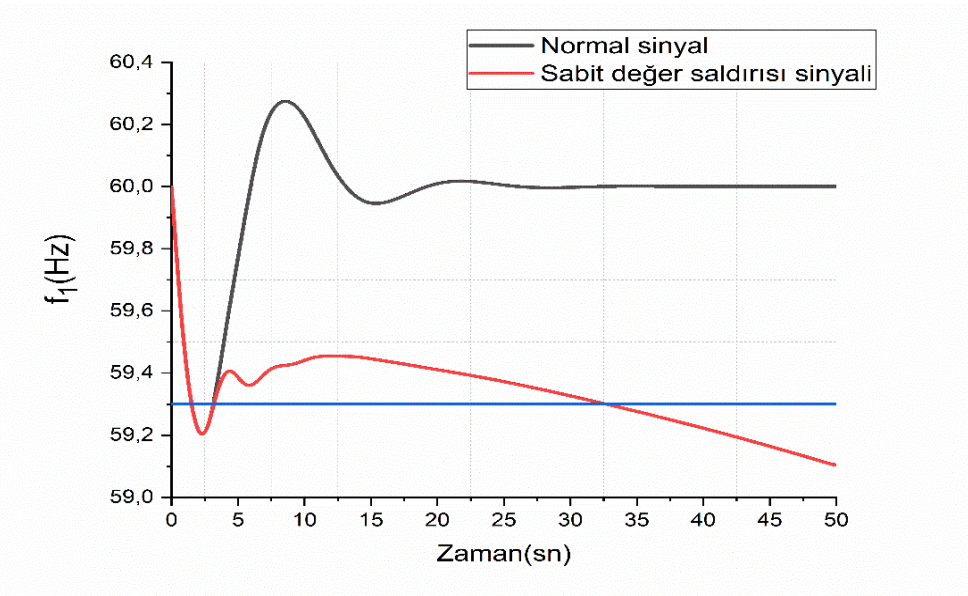


Şekil 3.4: Farklı saldırı parametreleri ile rampa saldırısı sırasında ACE_1 değişimleri.

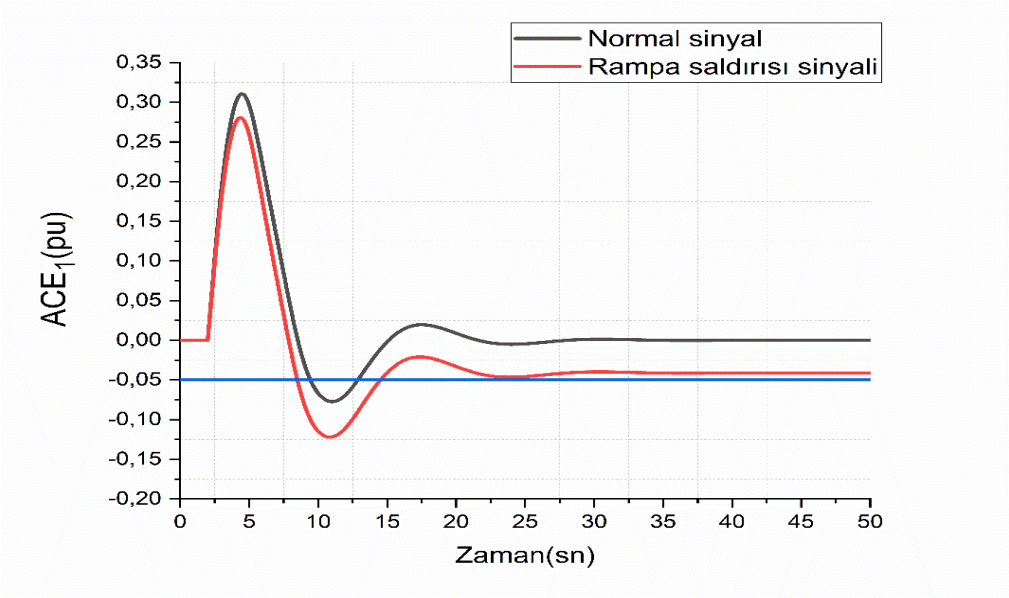
3.3 FDI Saldırılarının Sistem Kararlılığına Etkisi

OÜK Sistemlerine yapılan siber saldırıların en büyük amaçlarından biri sistem kararlılığını etkileyerek potansiyel yük atma şablonlarına yönlendirmek veya elektrik kesintileri oluşturmaktır. Buna 2015 yılında Ukrayna'da meydana gelen elektrik kesintisi örnek verilebilmektedir [76]. Alanlar arasında iletilen gücün salınımlarını sönümleyerek ve sistemin frekansını koruyarak ana görevini yerine getiren OÜK sisteminin frekans okumaları veya güç ölçümleri saldırgan tarafından manipüle edilirse OÜK düzgün çalışamaz ve şebekede kararsız durumlar oluşur. Sonuç olarak Düşük Frekans Yük Atma (UFLS) veya Aşırı Frekans Üretim Atma (OFGS) gibi eylemler uygulanır. Bu da tam bir elektrik kesintisi ile sonuçlanır. Saldırıların OÜK'ye etkisinin incelenebilmesi için Şekil 2.10'da verilen test sistemi-1 kullanılmaktadır. OÜK sistemindeki doğrusalsızlıkların etkisinin, göz ardı edilmemesi gerektiği bölüm 2.3.1'de verilen simülasyon sonuçları ile kanıtlanmaktadır. Bu nedenle yapılan tüm simülasyonlar, OÜK sistemine doğrusalsızlıklar eklenerek gerçekleştirilmektedir.

Senaryo 1: Saldırı parametre değeri "$m = -0.05$" olan negatif sabit değer saldırısı ACE_1 değerini hedef alacak şekilde uygulanmaktadır. ACE_1 grafiği ise Şekil 3.6'da gösterilmektedir. Şekil 3.5'de Alan 1 frekansının yük atma frekansı olan 59.3 Hz değerine düştüğü yaklaşık zaman değeri 32,5s olarak gösterilmektedir.

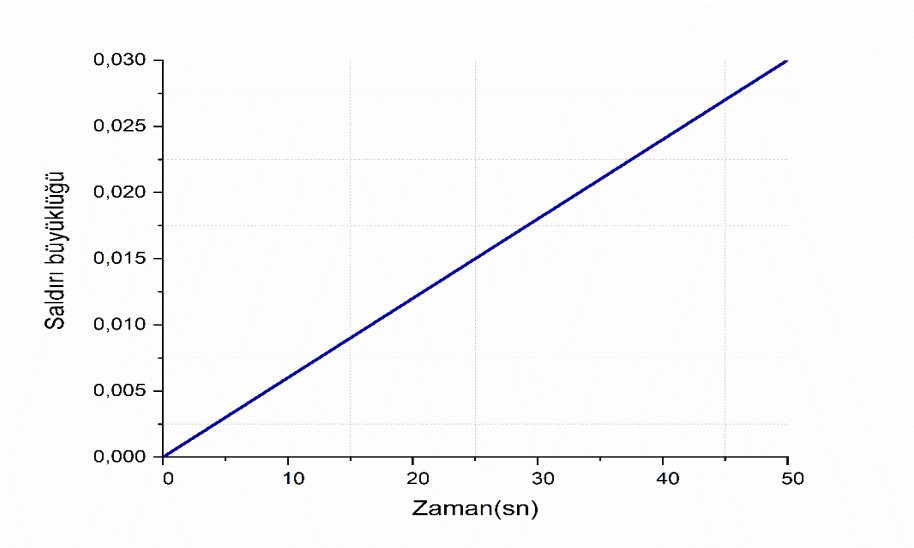


Şekil 3.5: Sabit değer "compensation" saldırısı sırasında Alan-1 frekans değişimi.



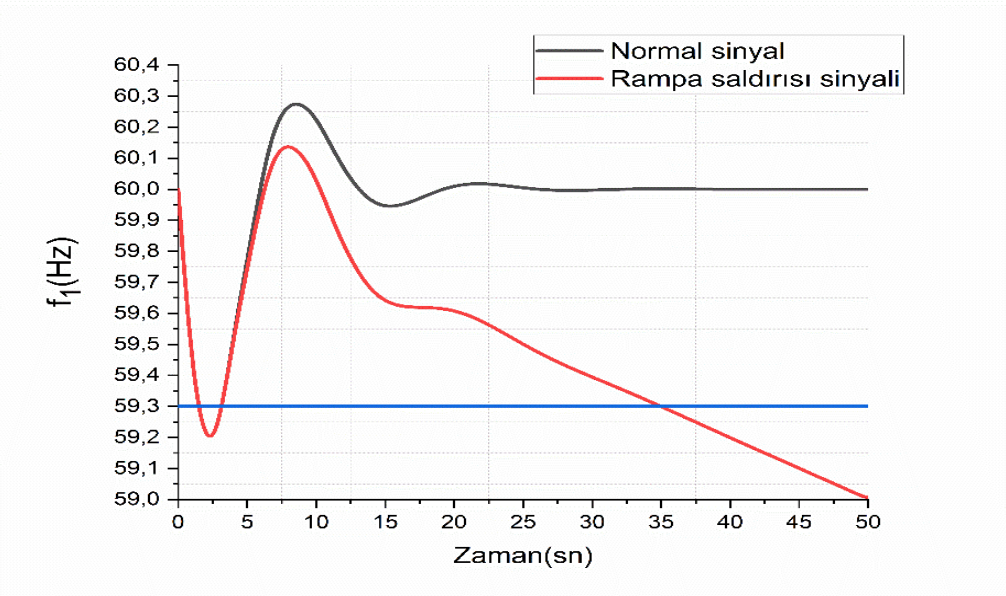
Şekil 3.6: Sabit değer saldırısı sırasında ACE_1 değişimi.

Senaryo 2: Rampa faktörü 0,0006 olan bir rampa saldırısı Alan-1 frekansını hedef almaktadır. Saldırı büyüklüğü Şekil 3.7'de gösterilmektedir. Şekil 3.8, Alan-1 frekansının yük atma frekansı olan 59.3 Hz değerine düştüğü yaklaşık zaman değeri 35s olarak gösterilmektedir. Şekil 3.9'da ise rampa saldırısı sırasında ACE_1 değişimi görülmektedir.

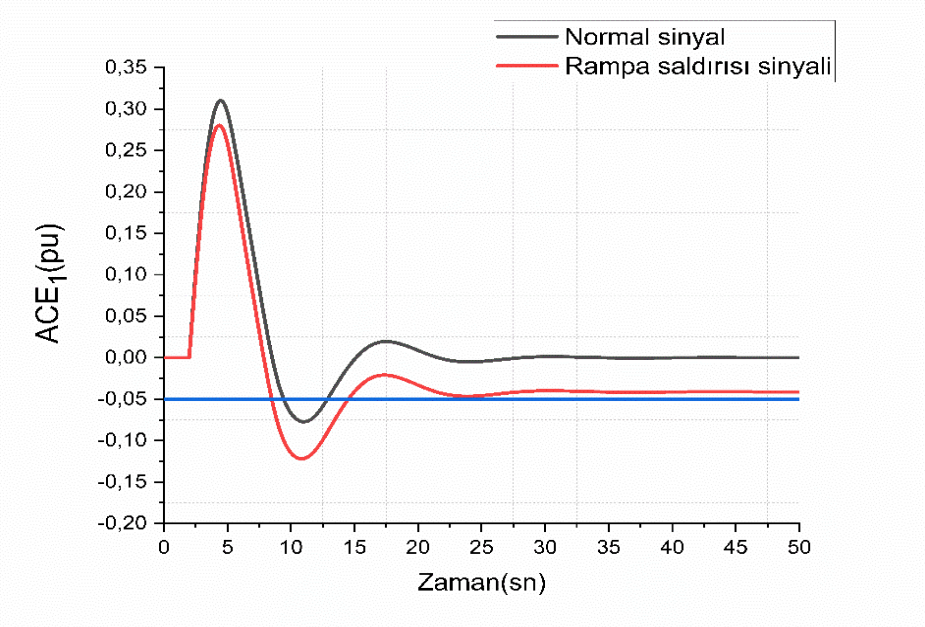


Şekil 3.7: Rampa saldırısı büyüklüğü.

Görüldüğü gibi rampa saldırısı sabit değer saldırısına göre daha geç yük atmayı tetiklemektedir. Bunun nedeni rampa saldırısında enjekte edilen yanlış verilerinin etkisinin zamanla kademeli olarak artmasıdır, dolayısıyla çok daha uzun zaman sonra etkisini göstermeye başlamaktadır.

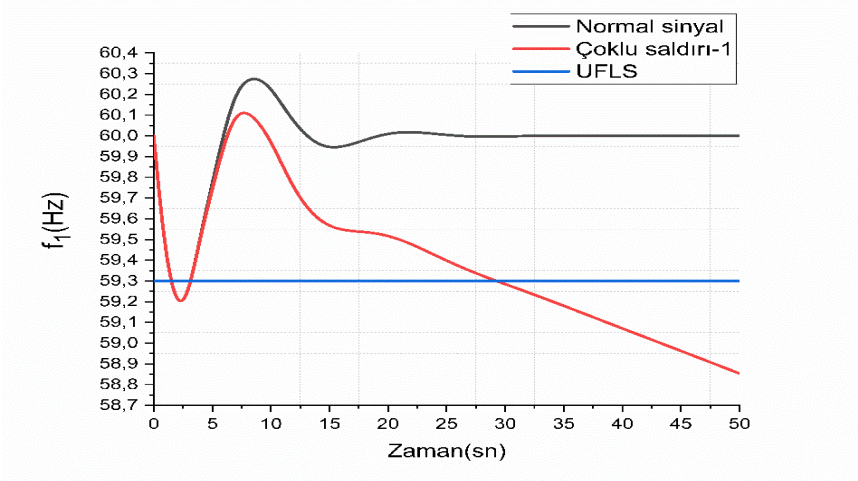


Şekil 3.8: Rampa saldırısı sırasında Alan-1 frekans değişimi.

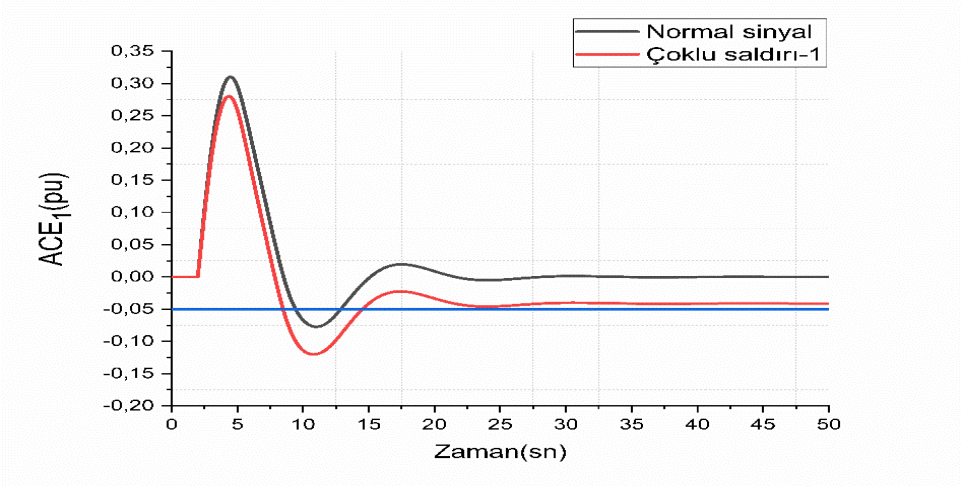


Şekil 3.9: Rampa saldırısı sırasında ACE_1 değişimi.

Senaryo 3: Bu senaryoda ise Alan 1 frekans ölçümlerini hedef alan ve rampa faktörü 0,0006 olan rampa saldırısı ile ACE_2 değerini hedef alan ve saldırı parametresi değeri "$m = -0.05$" olan negatif sabit değer saldırısı birlikte uygulanmaktadır. Tekli saldırılarda kullanılan parametre değerlerinin aynısı ile sisteme çoklu saldırı yapıldığında Alan-1 frekansının yük atma frekansı olan 59.3 Hz değerine düştüğü yaklaşık zaman değeri Şekil 3.10'dan 29 sn olarak görülmektedir. Bu zaman değeri her iki tekli saldırının yük atmayı tetiklediği zamandan daha kısadır. Şekil 3.11'de ise çoklu saldırı senaryosu-1 sırasında ACE_1 değişimi görülmektedir.

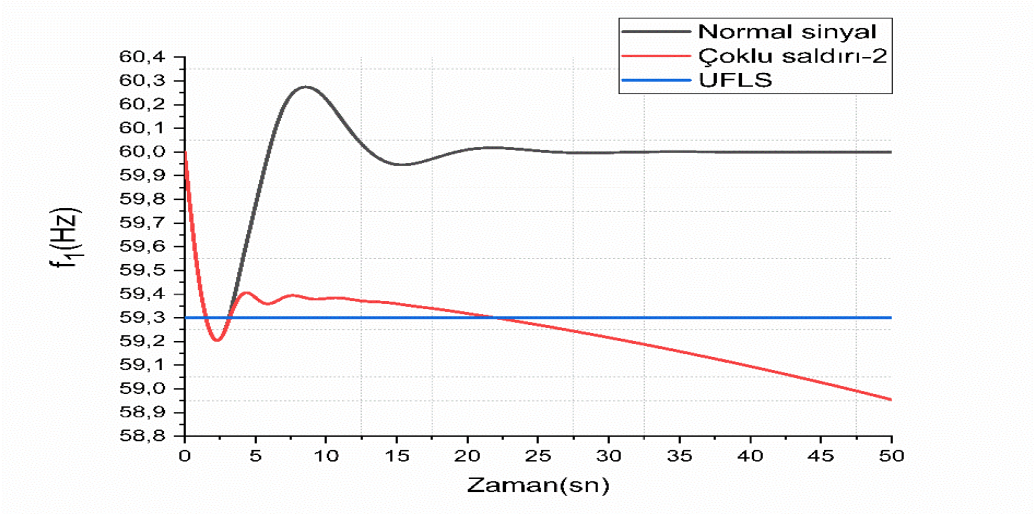


Şekil 3.10: Çoklu saldırı senaryosu-1 sırasında f_1 değişimi.

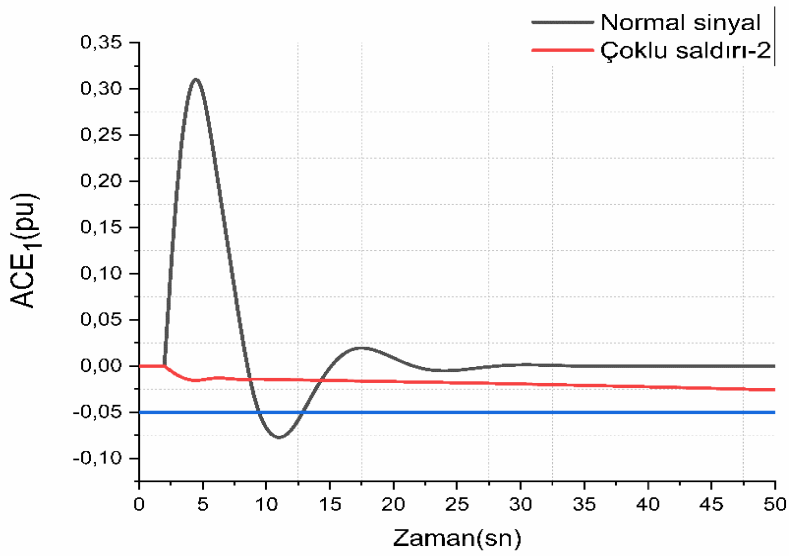


Şekil 3.11: Çoklu saldırı senaryosu-1 sırasında ACE_1 değişimi.

Senaryo 4: ACE_1 ve ACE_2 değerlerini hedef alan ve saldırı parametre değerleri "$m = -0.05$" olan çoklu negatif sabit değer saldırısı bu senaryoda uygulanmaktadır. Son olarak aynı parametre değerleri ile sisteme çoklu saldırı yapıldığında Alan 1 frekansının yük atma frekansı olan 59.3 Hz değerine düştüğü yaklaşık zaman değeri Şekil 3.12'den 22sn olarak ölçülmektedir. Şekil 3.13'de ise çoklu saldırı senaryosu-2 sırasında ACE_1 değişimi görülmektedir. Bu zaman değeri her iki tekli saldırıdan ve Senaryo 3'deki atak şablonundan daha kısa bir sürede sistemin yük atmasını sağlamaktadır.



Şekil 3.12: Çoklu saldırı senaryosu-2 sırasında f_1 değişimi.



Şekil 3.13: Çoklu saldırı senaryosu-2 sırasında ACE_1 değişimi.

Son olarak aynı parametre değerleri ile sisteme çoklu saldırı yapıldığında Alan 1 frekansının yük atma frekansı olan 59.3 Hz değerine düştüğü yaklaşık zaman değeri 22sn olarak ölçülmektedir. Bu zaman değeri her iki tekli saldırıdan ve Senaryo 3'deki atak şablonundan daha kısa bir sürede sistemin yük atmasını sağlamaktadır. Çizelge 3.1 saldırı şablonlarının parametre sınırlarını göstermektedir. Burada çoklu saldırıların parametre sınırlarının tekli saldırılara göre daha geniş olduğunu vurgulanmaktadır. Çoklu saldırılarda parametre sınırlarının geniş olması nedeniyle saldırganlar aynı parametre değerleri ile sisteme daha fazla zarar vermektedirler.

Çizelge 3.1: Tekli ve çoklu saldırı parametrelerinin karşılaştırması.

Saldırı Tipi	Parametreler	Alt Sınır	Üst Sınır
Rampa Saldırısı	λ_r	0.000425	0.000625
Sabit Değer Saldırısı	m	-0.0775	-0.0325
Çoklu saldırı 1	λ_r	0.00036	0.000659
	m	-0.157	-0.019

Bu saldırıların tespit edilmesi elektrik şebekesinin kararlılığı ve çalışması için önemlidir. Bu nedenle beşinci bölümde önerilen saldırı tespit tahmin algoritması ile saldırıların tehlikeye düşürdüğü ölçümlerin nereye ait olduğu belirlenmekte ve gerekli önlemlerin hızlıca alınması sağlanmaktadır.

4. YANLIŞ VERİ ENJEKSİYON (FDI) SALDIRILARININ TESPİTİ İÇİN MAKİNE ÖĞRENMESİ

Makine öğrenmesi, bilgisayar sistemlerinin verilerden öğrenmesini sağlayan, algoritmalar kullanarak bilgi ve tecrübe seviyesini arttıran bir yapay zeka dalıdır. Makine öğrenmesi ile birçok farklı veri tipi analiz edilebilir, desenler ve ilişkiler arasındaki modeller ortaya çıkarılabilir, karar-öneri sistemleri oluşturulabilir. Veri setleri ile makine öğrenmesi algoritmaları eğitilir ve modeller oluşturulur. Bu modeller daha sonra yeni verilere uygulanabilir ve çıkarımlar yapılabilir. Spam filtreleme, görüntü tanıma, konuşma tanıma, otomatik sürüş, hedef pazarlama, finansal tahminler ve tıbbi teşhisler gibi daha birçok alanda makine öğrenmesi teknikleri kullanılır. FDI'ların tespit edilmesi için araştırmacılar tarafından farklı makine öğrenmesi algoritmaları önerilmektedir.

4.1 Performans Metrikleri

Çok sayıda ölçüm tespit yöntemlerinin performansını değerlendirmek için benimsenmektedir. Doğruluk, kesinlik, duyarlılık, F1 skoru ve ROC eğrisi gibi metrikler en yaygın olanlarındandır. Bir ölçümün gerçek değeri ve onun tahmin edilen değeriyle; bir tespit modelinin çıktısı Doğru Pozitif (TP) doğru tahmin edilen pozitif tahmini, Doğru Negatif (TN) doğru tahmin edilen bir negatif tahmini, Yanlış Pozitif (FP) yanlış tahmin edilen pozitif tahmini, Yanlış Negatif (FN) yanlış negatif tahmini gösterecek şekilde ayrılmaktadır [79].

Doğruluk, makine öğrenmesi ve istatistiksel modellerin performansını değerlendirmek için kullanılan bir ölçüdür. Doğruluk ile, bir sınıflandırma modelinin doğru sonuçları doğru olarak tahmin etme yeteneği olarak tanımlanabilmektedir.

$$\text{Doğruluk(Accuracy)} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \tag{4.1}$$

Denklem 4.1'de görüldüğü gibi doğruluk doğru tahmin edilen örneklerin toplam örnek sayısına oranı olarak hesaplanmaktadır. Doğruluk, basit ve anlaşılır olmasına rağmen bazı durumlar için yanıltıcı sonuçlar ortaya koyabilmektedir. Eğer sınırlardan biri diğerine göre daha fazla varsa bunun sonucunda dengesiz bir sınıf dağılımı oluşmakta, bu durumda doğruluk ölçümü yanıltıcı olabilmektedir.

Dengesiz verilerle tespit modelinin performansı değerlendirilecekse kesinlik, duyarlılık ve F1 skorunun dikkate alınması gerekmektedir. Kesinlik, bir modelin bir saldırıyı gerçek pozitif tahminler olarak belirleme yeteneğidir [80]. Doğru pozitif tahminlerin, pozitif olarak etiketlenen örnek sayısına oranı olarak verilmektedir.

$$\text{Kesinlik(Precison)} = \frac{\text{TP}}{\text{TP} + \text{FP}} \tag{4.2}$$

Duyarlılık modelin tüm saldırıları tanımlama yeteneğidir. Duyarlılık, doğru pozitif tahmin sayısının pozitif numune sayısına oranı olarak tanımlanmaktadır.

$$\text{Duyarlılık(Recall)} = \frac{\text{TP}}{\text{TP} + \text{FN}} \tag{4.3}$$

Kesinlik ve duyarlılık arasında optimal etkileşim elde etmek için, bu iki ölçüm birleştirilerek F1 skoru kullanılmaktadır. Kesinlik veya duyarlılığın aşırı değerlerinden büyük ölçüde etkilenmemek için F1 puanı, aşağıda gösterildiği gibi kesinlik ve duyarlılığın harmonik ortalaması olarak tasarlanmaktadır.

$$\text{F}_1\text{score} = \frac{2\text{x(Recall x Precison)}}{\text{Recall} + \text{Precison}} \tag{4.4}$$

Bir sınıflandırıcıda, duyarlılık ile kesinlik dengeli ve dengesiz veri seti olma durumuna göre değişebilmektedir. Bunun sonucunda bir sınıflandırıcının gerçek performansını değerlendirmek zorlaşmaktadır. Daha doğru bir performans deperlendirmesi için ROC eğrisi kullanılmaktadır. Sürekli bir ikili sınıflandırıcıda, çıktı 0 ile 1 arasında sürekli değişmektedir. Bu nedenle çıktılar pozitif ve negatif olarak ayırmak için bir eşik değeri kullanılmaktadır. ROC eğrisi farklı eşik değerleri altında doğru pozitif oranını (y ekseni) yanlış pozitif oranına (x ekseni) göre çizer. ROC eğrisini (0,1) koordinatlarına ne kadar yakınsa performansın o kadar iyi olduğu anlamı çıkarılmaktadır. Başka bir deyişle eğri altında kalan alan ne kadar büyükse performans da o kadar iyidir.

4.2 Denetimli Öğrenme Algoritmaları

Makine öğrenmesi algoritmaları, denetimli öğrenme, yarı-denetimli öğrenme ve denetimsiz öğrenme olmak üzere üçe ayrılmaktadır. Denetimli öğrenmede, bir girdi ve ona karşılık gelen bir hedef çıktı verisi kullanılarak bir modelin eğitilmesi işlemi yapılmaktadır. Bu veriler sayesinde model karar almayı öğrenir ve yeni girdi verileri ile ilgili tahminler yapabilmektedir. FDI'ların tespit edilmesinde genellikle ikili bir sınıflandırma problemi olduğu kabul edilmektedir. İkili sınıflandırmanın amacı kendisine verilen m özellikli s kadar veriden, normal ölçüm vektörü (negatif sınıf) z, ile saldırılmış ölçüm vektörü (pozitif sınıf) $z_a = z + a$ arasındaki farkı bulmaktır [81]. Yani gelen bir verinin saldırılmış mı yoksa normal ölçüm mü olduğuna karar verilmesi işlemi ikili sınıflandırma olarak adlandırılmaktadır. Çıkış aşağıdaki gibi etiketlenmektedir.

$$y = \begin{cases} +1 & a \neq 0 \\ -1 & a = 0 \end{cases} \tag{4.5}$$

Burada a saldırı vektörüdür. Yaygın kullanılan denetimli öğrenme algoritmaları SVM, k-nn ve lojistik regresyon algoritmalarıdır.

4.2.1 Algılayıcılar

Bir s_i örneği verildiğinde algılayıcı $f(s_i) = \text{sign}(w * s_i)$ sınıflandırma fonksiyonunu kullanarak y_i değerini tahmin etmektedir, burada w bir ağırlık vektörüdür ve $\text{sign}(w * s_i)$ ise aşağıdaki gibi tanımlanmaktadır [82].

$$\text{sign}(w * s_i) = \begin{cases} -1 & \text{eğer } w * s_i < 0 \text{ ise} \\ 1 & \text{aksi takdirde} \end{cases} \tag{4.6}$$

Eğitim aşamasında, ağırlıklar algoritmanın her eğitim örneği için her iterasyonda $t = 1, 2, 3, \ldots, T$ ayarlanmaktadır.

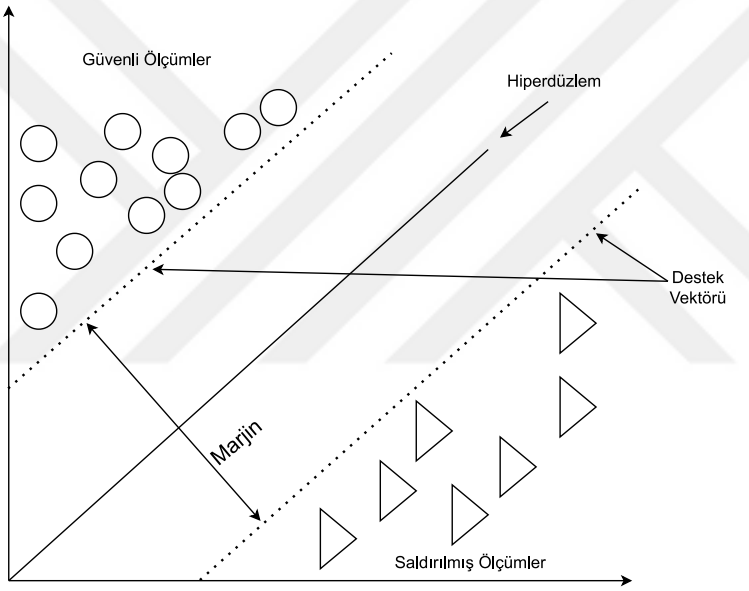
$$w(t+1) \coloneqq w(t) + \Delta w \tag{4.7}$$

Burada $\Delta w = \gamma(y_i - f(s_i))s_i$ ve γ öğrenme oranıdır. Algoritma adım sayısı veya bir hata eşiği değerine kadar çalışmaya devam etmektedir. Test aşamasında yeni bir test örneğinin etiket değeri $f(s_i') = \text{sign}(w(T) * s_i'$ ile tahmin edilmektedir.

Çeşitli makine öğrenimi uygulamalarındaki başarısına rağmen, algoritmanın yakınsaması yalnızca örnekler doğrusal olarak ayrılabilir olduğunda sağlanmaktadır [82]. Bu nedenle, algılayıcı ancak ölçümler bir hiperdüzlemle ayrılabilirse, saldırıların tespitinde başarılı bir şekilde kullanılabilmektedir.

4.2.2 Destek vektör makineleri (SVM)

SVM'lerde, iki farklı sınıfı ayırmak için bir hiper düzlem oluşturulmaktadır. Hiperdüzlem, bir ağırlık vektörü w ve bir bias değeri b ile temsil edilebilmektedir. Doğrusal olarak dağılan veriler için karar sınırları denklem 4.8 kullanılarak iki paralel hiperdüzlem olarak formüle edilebilmektedir. Şekil 4.1'de görülen yuvarlak ve üçgen şekilleri iki ayrı sınıfı temsil etmektedir.



Şekil 4.1: SVM konsepti [86].

$$\begin{cases} w^T s_i + b = +1, \text{eğer } y_i = +1 \text{ ise} \\ w^T s_i + b = -1, \text{eğer } y_i = -1 \text{ ise} \end{cases} \quad (4.8)$$

İki sınıf arasına çizilen kalın çizgi SVM'nin çizdiği karar sınırını göstermektedir. Bu karar sınırı, iki sınıf arasında maksimum mesafeyi (marj) oluşturmak için optimum şekilde yerleştirilmektedir. Destek vektörler, karar sınırına en yakın noktalar olacak şekilde yerleştirilmektedir. Bu noktalar karar sınırının konumunu ve yönelimini belirlediği için oldukça önemlidir. D marjini iki destek vektörü arasındaki ayrılmış alandır ve aşağıdaki gibi hesaplanabilmektedir.

$$D = \frac{2}{w^2} \tag{4.9}$$

Hiperdüzlemler ise 4.10 numaralı denklem çözülerek tanımlanabilmektedir:

$$\min_{w,\,\xi,\,b} \|w\|_2^2 + \zeta \sum_{i=1}^{M_{Tr}} \xi_i \tag{4.10}$$

$$y_i(w^T s_i + b) - 1 + \xi_i \geq 0 \tag{4.11}$$

$$\xi_i \geq 0 \; \forall i = 1, 2, 3, \ldots, M_{Tr}$$

Burada ζ ayarlanabilir regülirizasyon parametresi, ξ_i ayrılabilen nonlineer eğitim seti için gevşek değişken ve M_{Tr} ise özellik vektörüdür.

4.2.3 k-en yakın komşular (k-NN)

k-nn, en yakın komşularına göre örnekleri atayan bir sınıflandırıcıdır. Etiketlenmemiş veri s_i ile tüm etiketli veriler S arasındaki uzaklığı belirlemek için aşağıda verilen Öklid mesafesi kullanılmaktadır:

$$d_{ij} = \|s_i - s_j\|, s_j \in S \tag{4.12}$$

$k = 1$ için tahmin edilen sınıf etiketi y_i, y_i'ye en yakında bulunan etiketli veri tarafından verilmektedir.

$$y_i = \arg \min_{y_j} \{d_{ij}\} \tag{4.13}$$

$k > 1$ ise çoğunluk oylaması ile s_i'nin nihai etiketi belirlenmektedir.

Bu çalışmada çapraz doğrulama performansına göre en yakın komşu sayısı $k = 10$ olarak belirlenmekte ve mesafe ağırlıkları ise eşit seçilmektedir.

4.2.4 Karar ağacı (KA)

Özellik ve hedefe göre birleştirilen karar düğümleri (decision nodes) ve yaprak düğümleri (leaf nodes) ağaç yapısı formundaki modeli oluşturmaktadır. Bu model ile sınıflandırma veya regresyon işlemi yapılmaktadır. Karar ağacındaki ilk düğüme kök düğüm (root node) denmekte ve burada seçilen kök veri setini olabildiğince çok

açıklaması gerekmektedir. Kök düğüm, hedef değişkeni en iyi bölen değişkeni bularak bölme işlemini başlatmaktadır. Bir karar ağacı, belirli kararlar silsilesi ile veri kümesini daha küçük kümelere bölmek için kullanılan bir yapıdır. Bölünmenin nasıl gerçekleştiği karar ağacının doğruluk oranını etkilemektedir. Bir karar düğümü birden fazla dallanma oluşturabilmektedir. Fakat bu çalışmada kullanılan Sınıflandırma ve Regresyon Ağaçları (CART) algoritmasının temel prensibi ağacı iki dala ayırmasıdır [83].

Twoining ve Gini en çok bilinen iki CART algoritmasıdır. Bu çalışmada kullanılan KA algoritması için maksimum bölünme sayısı, 100 ile sınırlandırılmakta ve Gini indeksi kullanılmaktadır. İlk bölünecek özellik ve bölünme değeri Gini endeks değeri ile bulunmaktadır. Gini indeksi ile bir karar ağacının bölünmesi işlemi yapılmaktadır. Gini endeksi ne kadar düşükse, yanlış sınıflandırma olasılığı da o kadar düşüktür. Gini endeksi;

$$\mathrm{Gini}(\mathrm{D}) = 1 - \sum_{\mathrm{j}=1}^{\mathrm{n}} \mathrm{p}(\mathrm{j})^2 \tag{4.14}$$

olarak verilmektedir. Burada n hedef değişendeki sınıf sayısını, p ise D veri setindeki j sınıfının olasılığını temsil etmektedir. Bizim örneğimiz için bu sayı dört olarak belirlenmektedir. Bir D veri seti A üzerinde iki D_1 ve D_2 altkümesine bölünürse, gini endeksi aşağıdaki gibi elde edilmektedir.

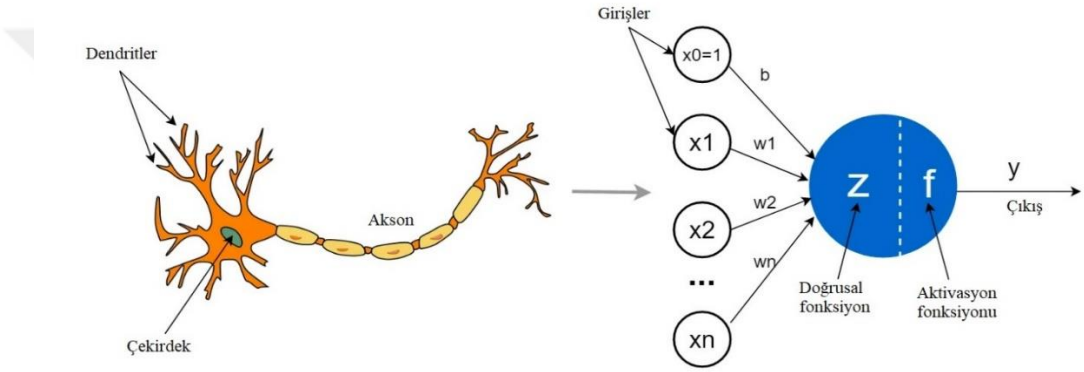
$$\mathrm{Gini}_{\mathrm{A}}(\mathrm{D}) = \frac{|\mathrm{D}_1|}{|\mathrm{D}|}\mathrm{gini}(\mathrm{D}_1) + \frac{|\mathrm{D}_2|}{|\mathrm{D}|}\mathrm{gini}(\mathrm{D}_2) \tag{4.15}$$

4.2.5 Yapay sinir ağları (YSA)

YSA, genellikle insan beyninin yapısını oluşturan biyolojik sinir ağlarına dayalı hesaplamalı bir ağdır [87]. İnsan beyninden esinlenerek biyolojik nöronların birbirlerine sinyal gönderme işlemini taklit etmektedir. Bir yapay nöron, doğal bir nörondan ilham alan hesaplamalı bir modeldir. Doğal nöronlar, nöronun dendritleri veya zarı üzerinde bulunan sinapslar yoluyla sinyalleri almaktadırlar. Alınan sinyaller yeterince güçlü olduğunda (belirli bir eşik değerini aştığında), nöron aktive olmakta ve akson aracılığıyla bir sinyal yaymaktadır. Bu sinyal başka bir sinapse gönderilmekte ve diğer nöronları aktive etmektedir. Yapay nöronlar modellenirken,

gerçek nöronların karmaşıklığı oldukça azaltılmaktadır. Temel olarak ağırlıklarla (sinyal gücü) çarpılan ve nöronun aktivasyonunu belirleyen matematiksel bir fonksiyonla hesaplanan girdilerden (sinapslar) oluşmaktadır. Bir diğer fonksiyon ise yapay nöronun çıktısını hesaplamaktadır.

Şekil 4.2'de doğal bir nöron ile yapay bir nöron gösterimi yer almaktadır. Oluşturulan bu yapay nöronların birleştirilmesi sayesinde YSA'lar bilgiyi işlemektedir. Bir yapay nöronun ağırlığı ne kadar yüksekse, onunla çarpılan girdi o kadar güçlü bir etkiye sahip olmaktadır. Ağırlıklara göre nöronun hesaplanması farklı sonuçlar vermektedir. Bu nedenle yapay bir nöronun ağırlıkları ayarlanarak istenen çıktı elde edilebilmektedir.



Şekil 4.2: Doğal bir nöron ile yapay bir nöronun gösterimi [87].

Fakat YSA'da yüksek sayıda nöron bulunabileceğinden tüm bunların tek tek ayarlanması mümkün değildir. Ağırlıkların ayarlanması işlemi eğitim olarak adlandırılmaktadır. Bir YSA aşağıda açıklanan temel prensibe göre çalışmaktadır.

Şekil 4.2'de gösterilen x_1, x_2, x_n gibi giriş değerleri ağırlıkları ile birlikte gizli katmana iletilmektedir. Her gizli katman nöronlardan oluşmaktadır. Tüm girişler her bir nörona bağlıdır. Şekil 4.2'de gösterilen algılayıcı (mavi daire) içinde tüm girdiler kendi ağırlıkları (w_1, w_2, w_n) ile çarpılmakta ve yanlılık (bias) değişkeni "b"eklenmektedir. Elde edilen sonuç denklem 4.16'da görülmektedir.

$$z = (w_1.x_1 + w_2.x_2 + \cdots + w_n.x_n) + b \tag{4.16}$$

Daha sonra aktivasyon fonksiyonu elde edilen z denklemine uygulanmaktadır. Aktivasyon fonksiyonu, girdiyi sonraki nöron katmanına göndermeden önce uygulanan doğrusal olmayan bir dönüşümdür. Sigmoid, tanh, step, doğrusal, ReLU,

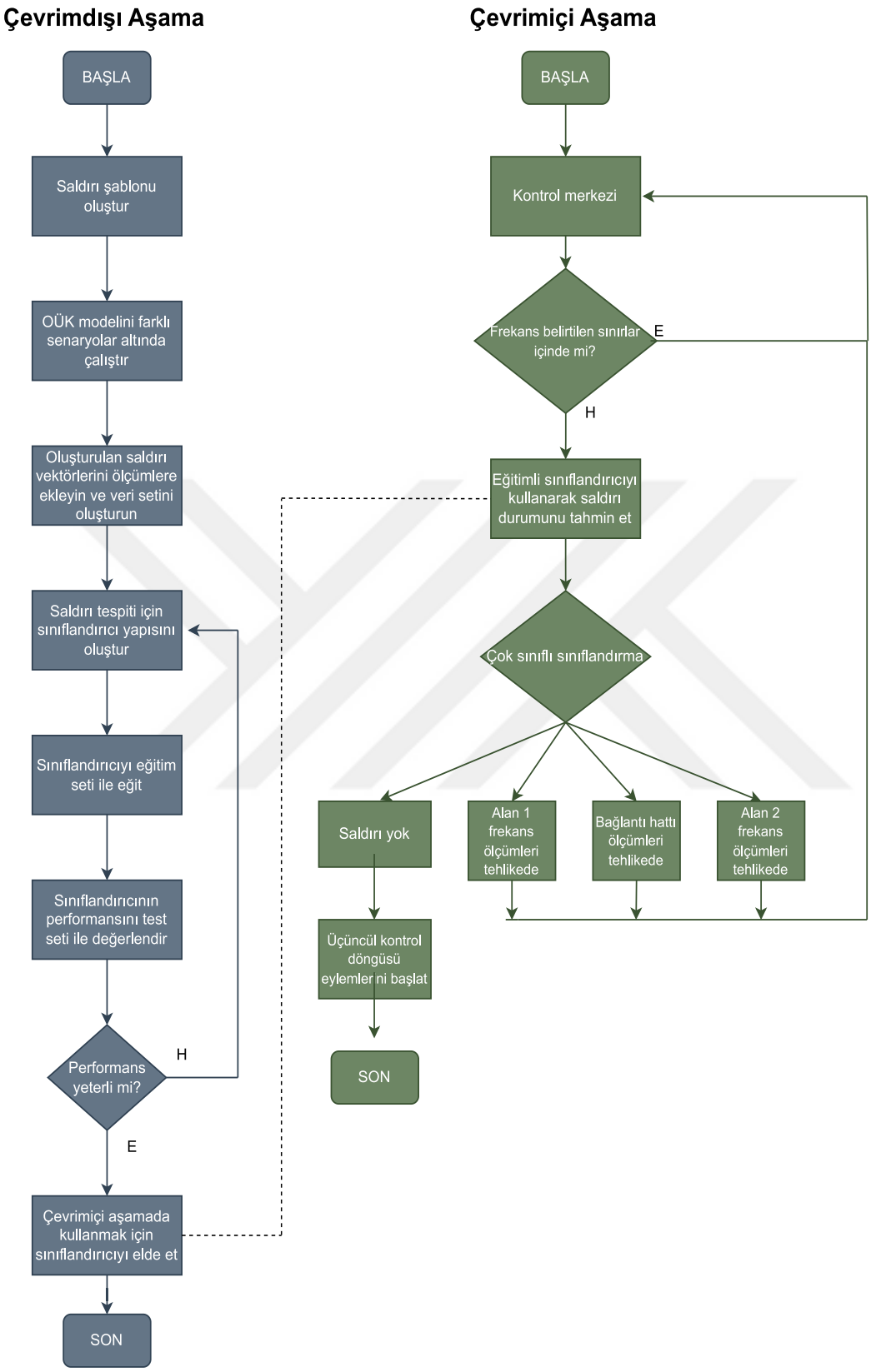
Sızıntı ReLU, softmax gibi farklı aktivasyon fonksiyonu çeşitleri vardır. Burada açıklanan süreç ileri yayılım (forward propagation) olarak bilinmektedir. En son çıkış katmanında tahminler elde edilmkete ve gerçek değer ile tahmin edilen arasındaki fark hesaplanmaktadır. Hatanın düşürülmesi için bu kez de geriye yayılım (back propagation) işlemi başlamaktadır.

5. ÖNERİLEN SALDIRI TESPİT ALGORİTMASI METODOLOJİSİ

Öncelikle oluşturulan OÜK sisteminin f_1, f_2 ve p_{tie} olmak üzere üç farklı noktasına FDI saldırısı yapılmaktadır. Ardından önerilen tespit algoritması metodolojisi ile çevrimiçi ölçümleri kullanarak, OÜK sistemine yapılan siber saldırıları ve bu saldırıların lokasyonunu tahmin eden makine öğrenimi tabanlı topluluk sınıflandırıcısı oluşturulmaktadır. Sınıflandırıcının eğitilmesi için ise sensörlerden elde edilen f_1, f_2, ACE_1, ACE_2 ve p_{tie} ölçümleri kullanılmaktadır. Sınıflandırıcı f_1, f_2, p_{tie} ve "saldırı yok" olarak dört farklı çıkışı tahmin etmektedir.

Bu yaklaşım iki ana bölüme ayrılmaktadır. İlk aşama olan çevrimdışı aşamada sensörlerden gelen ölçüm verileri toplanarak bir veri seti oluşturulmaktadır. Daha sonra oluşturulan bu veri seti ile sınıflandırıcının eğitimi ve performansının değerlendirilmesi işlemi yapılmaktadır. Çevrimiçi aşamada ise eğitilmiş olan bu sınıflandırıcı ile gelen ölçüm verileri girdi olarak alınmaktadır. Bu girdiler ile sistemin siber tehdit altında olup olmadığı ve hangi ölçümün bozulmuş olabileceği tahmin edilmektedir.

Tüm bu işlemler esnasında iki alanlı dört makineli test sistemi kullanılmakta ve farklı oranlarda (%0-%10-%20) RES kaynakları eklenerek önerilen algoritmanın etkinliği gösterilmektedir. Toplamda üç farklı RES entegrasyon oranı için üç farklı veri seti oluşturulmakta ve tüm bu veri setleri önerilen sınıflandırıcı algoritmasının eğitilmesinde kullanılmaktadır. Önerilen metodoloji için akış şeması Şekil 5.1'de sunulmaktadır. Alt bölümlerde farklı senaryoların tanıtılması, veri seti oluşturulması, sınıflandırıcının eğitilmesi prosedürlerinin ayrıntılarını sunarak önerilen topluluk öğrenmesi algoritmasının metodolojisinin çevrimdışı aşaması açıklanmaktadır.



Şekil 5.1: Önerilen siber saldırı tespit ve sınıflandırma metodolojisi.

5.1 Veri Seti Üretilmesi

Makine öğrenmesi algoritmaları, model parametrelerinin optimize edilmesi için bir veri kümesine ihtiyaç duymaktadır. Ayrıca bu verilerin etiketli olması gerekmektedir. Genellikle kullanılan siber saldırı tespit algoritmaları için saldırı var durumu sınıf 1, saldırı yok durumu ise sınıf 0 olarak bir ikili sınıflandırma problemi düşünülmektedir. Bu çalışmada dört farklı sınıf olmak üzere bunlar: Alan 1 frekansına saldırı, alan 2 frekansına saldırı, bağlantı hattı gücüne saldırı ve saldırı yok olarak belirlenmektedir. Önerilen metodolojide siber saldırı tespiti çoklu bir sınıflandırma problemi olarak düşünülmektedir. Öğrenme veri seti bir dizi ölçüm ve her bir örneğin bir etiket ile temsil edildiği veri topluluğudur. Farklı çalışma şartları altında ölçümler elde edilmesi için, saldırı olmadan önceki çalışma koşullarında ve beklenmedik durumun içerdiği belirsizlikler gibi sistemle ilgili tahmin edilemez çeşitli senaryolar veri setinde yer almalıdır. Yani sistemin normal çalışma koşullarında yüklenme durumu, yenilenebilir enerji kaynağı entegrasyon oranı ve saldırı olduğu durumlarda ise saldırı parametresi büyüklüğü, süresi, saldırının yapıldığı ölçüm gibi senaryolar veri setinde yer almalıdır.

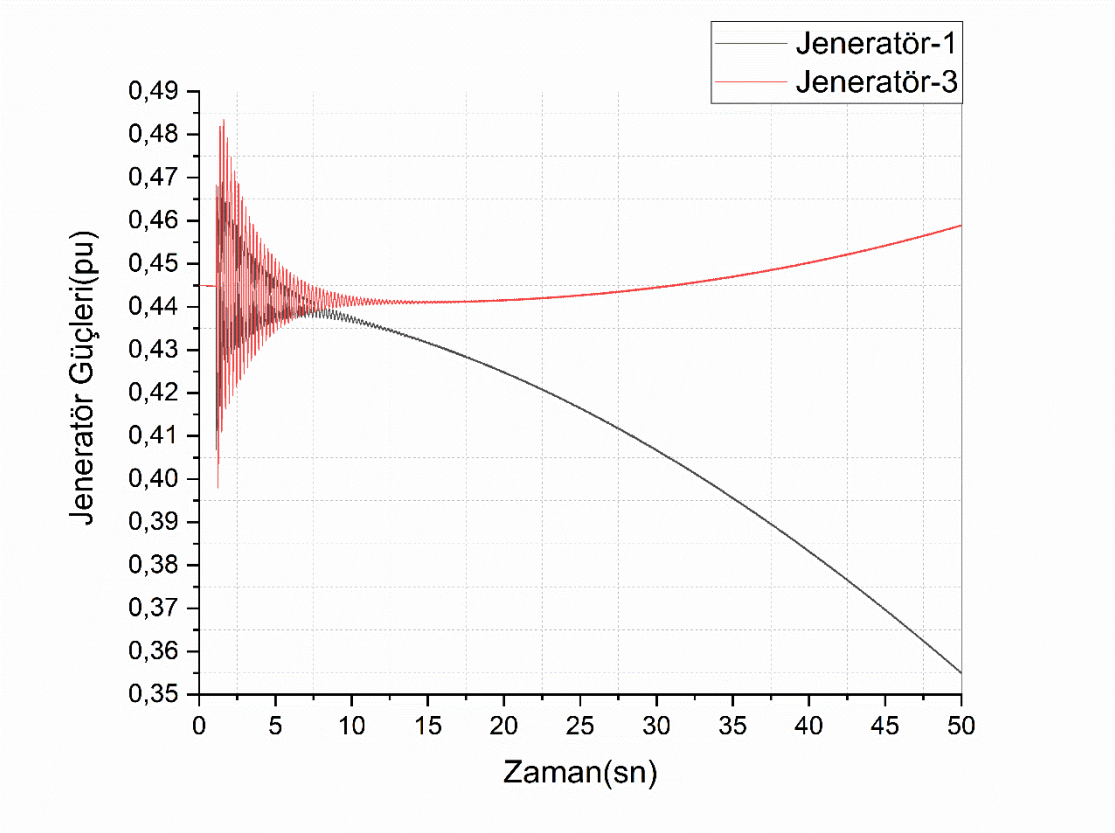
Aşağıda iki alanlı test sistemine yapılan farklı saldırı şablonları ve bunların etkileri üç farklı senaryo ile verilmektedir. Görüldüğü üzere her saldırı farklı ölçüm ve kontrol noktalarını hedef alabilmekte ve her saldırının sistemde oluşturduğu etki farklı olmaktadır. Bu nedenle çalışmamızda sadece saldırı olup olmadığını tespit etmek yerine hangi ölçüm değerine de saldırı olduğunu tespit eden bir sınıflandırma algoritması önerilmektedir.

Siber saldırı içermeyen durumlar, alan içinde yük değişimi, komşu alanda yük değişimi, her iki alanda yük değişimi olmak üzere üçe ayrılmaktadır. Ayrıca yukarıda açıklanan ve etkileri kanıtlanan saldırı şablonları farklı parametre değerleri ile birlikte iki alanlı test sistemine uygulanmaktadır.

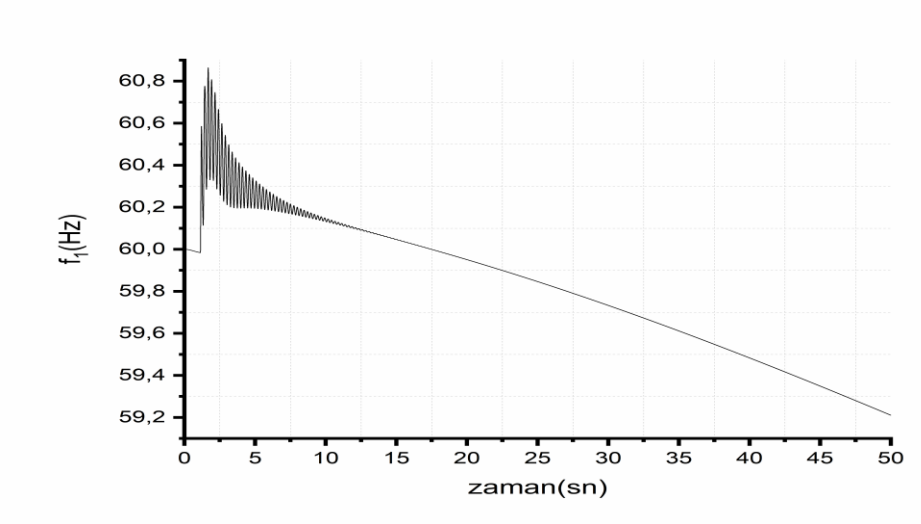
Aşağıda yer alan üç senaryo sadece saldırıların sisteme etkilerinin gösterilmesi açısından açıklanmaktadır. Veri seti oluşturulurken rampa, ölçekleme, sabit değer (compensation) ve işaret (flip) saldırısı olmak üzere dört farklı saldırı şablonu farklı parametre değerleri ile sisteme uygulanmaktadır. Oluşturulan bu saldırılar f_1, f_2, p_{tie} olmak üzere üç farklı noktaya yapılabilmektedir. Ayrıca farklı yüklenme şartları da farklı senaryolar olarak düşünülmektedir. Tüm bunlar göz önüne alındığında 100 farklı senaryo ile toplam 98565 örnek toplanmaktadır.

Burada bahsedilen ilk veri seti oluşturulurken güç sisteminde RES entegresi oranı %0'dır. Aynı senaryo koşullarında %10 RES entegresi ve %20 RES entegresi yapılarak ayrı iki veri seti daha toplanmaktadır.

Senaryo 1: Bu senaryoda 2 numaralı bölümde açıklanan 2-alanlı 4-makineli test sistemi üzerinden $t = 0$'dan itibaren rampa faktörü $\lambda_r = 0.001$ olacak şekilde frekans değerine saldırı yapılmaktadır. Bu durumda saldırganın 1 numaralı jeneratörün frekans ölçüm sinyallerini rampa fonksiyonu ile manipüle ettiği ve üretim seviyesini düşürdüğü Şekil 5.2'de görülmektedir. Komşu alanda bulunan jeneratör-3 ise oluşan bu güç kaybını telafi etmek için üretimini arttırmaktadır. Şekil 5.3'de ise bu saldırı sonucu alan-1 frekansında oluşan düşüş görülmektedir. Bu senaryoda veriler alan 1 frekansına yapılan saldırı verisi olarak etiketlenmektedir.

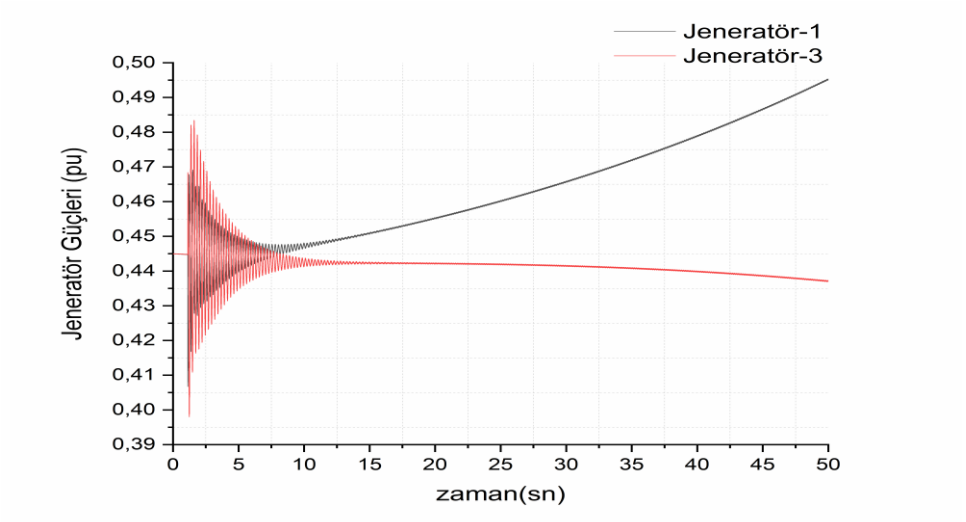


Şekil 5.2: Jeneratör-1 ve Jeneratör-3 çıkış güç değişimleri.

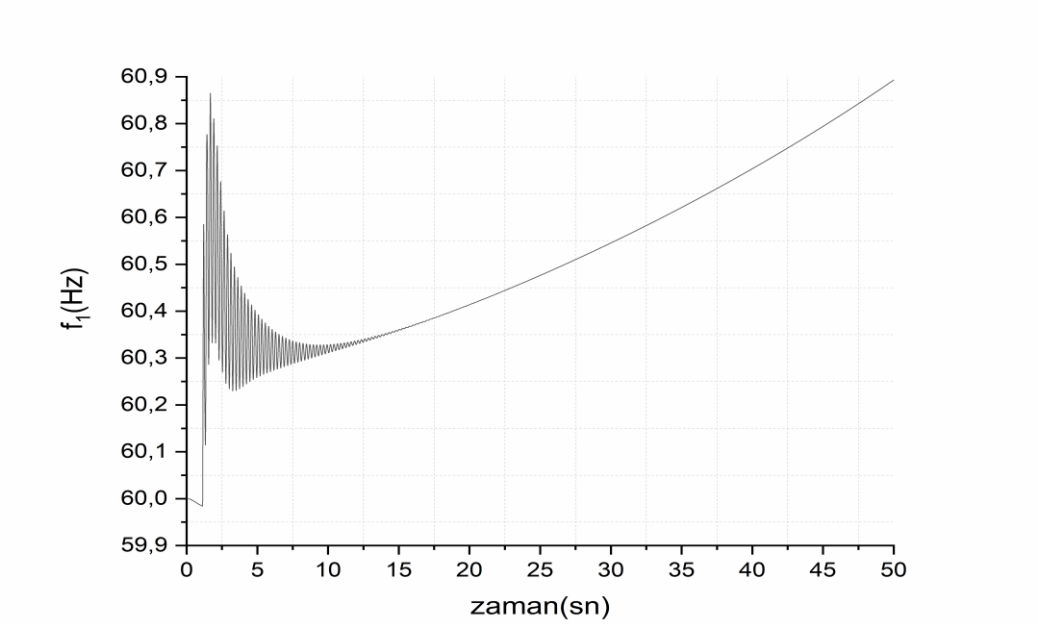


Şekil 5.3: Senaryo 1 için alan-1 frekans değişimi.

Senaryo 2: Bu senaryoda, saldırgan ortadaki adam saldırısı (MITM) ile jeneratör-1'e gönderilen ACE değerlerini sabit bir negatif sayı ile çarparak manipüle etmeyi amaçlamaktadır. Burada $m = -0.75$ olarak belirlenmektedir. Bu sayede ikincil üretim döngüsünü manipüle etmeyi başaran saldırgan jeneratör-1 üretim seviyesini kademeli olarak arttırmayı başarmaktadır. Şekil 5.4'den görüldüğü üzere Jeneratör-3, kendisine gönderilen verilere saldırılmadığı için jeneratör-1'in etkilerini düzeltmeye çalışmaktadır. Bu senaryodaki veriler de alan 1 saldırısına yapılan saldırı olarak etiketlenmektedir. Şekil 5.5'de ise senaryo 2 sonucunda alan-1 frekansında meydana gelen değişim gösterilmektedir.

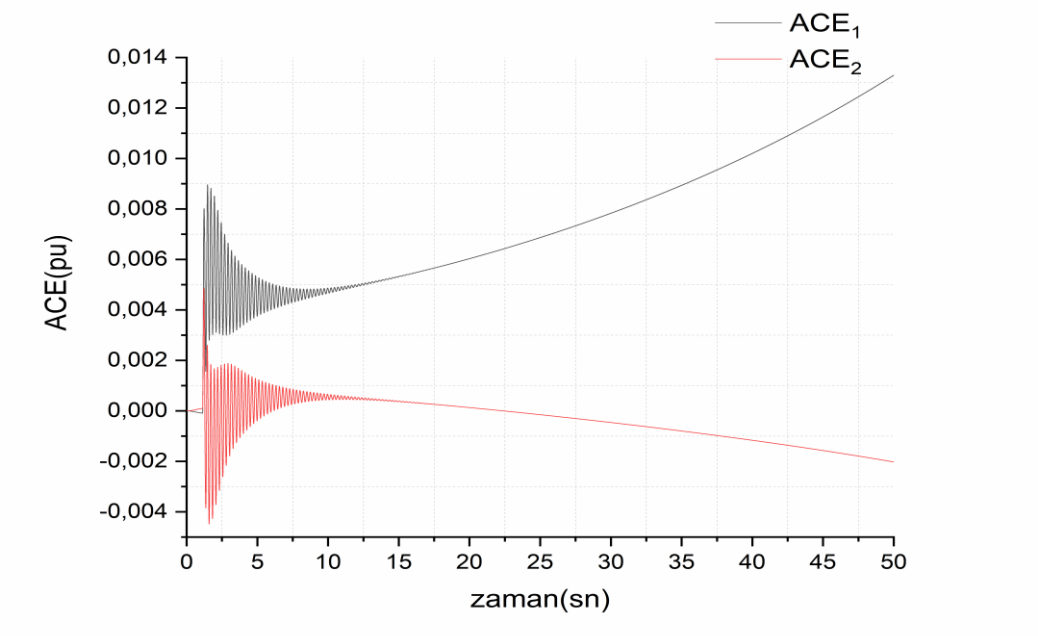


Şekil 5.4: Jeneratör-1 ve Jeneratör-3 çıkış güç değişimleri.

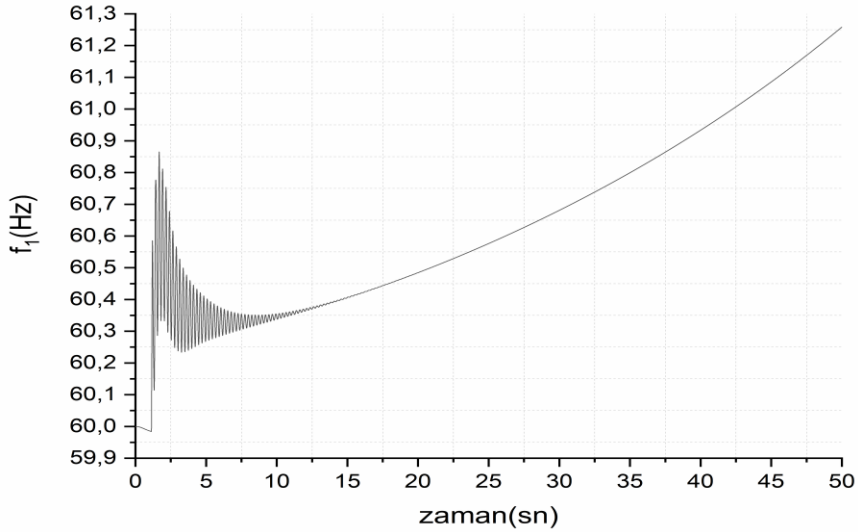


Şekil 5.5: Senaryo 2 için alan-1 frekans değişimi.

Senaryo 3: Bu senaryoda saldırgan jeneratör-1'e gönderilen her ACE değerinin işaretini değiştirmektedir. Bu saldırının sistem frekansına ve ACE değerlerine olan etkisi Şekil 5.6'da gösterilmektedir. Şekil 5.7'de ise senaryo 3 sonucunda alan-1 frekansında meydana gelen değişim gösterilmektedir.

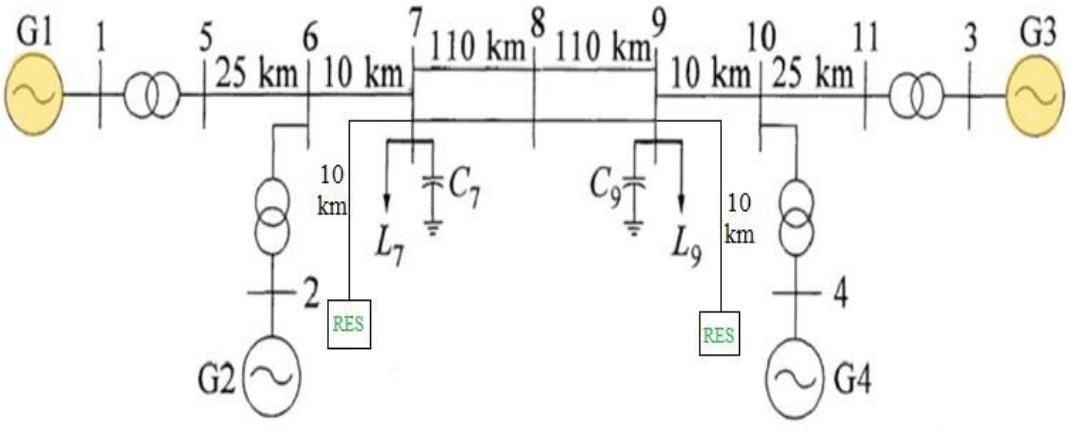


Şekil 5.6: Senaryo 3 için ACE_1 ve ACE_2 değişimi.



Şekil 5.7: Senaryo 3 için alan-1 frekans değişimi.

Saldırı tespit algoritmalarını farklı koşullar altında inceleyebilmek için Şekil 5.8'de görüldüğü üzere 7 ve 9 numaralı baralara toplam 90 MW gücünde RES eklenmektedir. Bölüm 5.1'de yapılan tüm senaryolar bu bölümde tekrarlanmakta ve ayrı bir veri seti oluşturulmaktadır. Benzer olarak sistemde bulunan RES gücü toplam 180 MW değerine çıkarılarak aynı koşullar altında farklı bir veri seti daha oluşturulmaktadır.Bu sayede toplam üç veri seti elde edilmektedir.



Şekil 5.8: RES entegrasyonu ile birlikte iki alanlı dört makineli test sistemi.

100 farklı senaryonun oluşturulma mantığının daha iyi anlaşılabilmesi için Çizelge 5.1'de rastgele 10 senaryo verilmektedir. Geri kalan tüm senaryolar Çizelge 5.1'in saldırı parametre değerlerinin ve sisteme bağlanan yükün değiştirilmesi ile meydana getirilmektedir.

Çizelge 5.1: Oluşturulan farklı senaryolar.

Senaryo numarası	Yük ve saldırı durumu	Senaryo numarası	Yük ve saldırı durumu
Senaryo 1	Saldırı yok, 18 MW yük alan 1'e bağlandı	Senaryo 7	$\lambda_r = 0.001$ saldırı parametresi ile f_2 saldırı altında
Senaryo 2	Saldırı yok, 36 MW yük alan 2'ye bağlandı	Senaryo 8	$\lambda_r = 0.001$ saldırı parametresi ile p_{tie} saldırı altında
Senaryo 3	$\lambda_s = 0.5$ saldırı parametresi ile f_1 saldırı altında	Senaryo 9	$m = -0.75$ saldırı parametresi ile ACE_1 saldırı altında
Senaryo 4	$\lambda_s = 0.5$ saldırı parametresi ile f_2 saldırı altında	Senaryo 10	$m = -0.75$ saldırı parametresi ile ACE_2 saldırı altında
Senaryo 5	$\lambda_s = 0.5$ saldırı parametresi ile p_{tie} saldırı altında	Senaryo 11	Saldırı yok, 54 MW yük alan 1'e, 36 MW yük alan 2'ye bağlandı
Senaryo 6	$\lambda_r = 0.001$ saldırı parametresi ile f_1 saldırı altında	Senaryo 12	Saldırı yok, 45 MW yük alan 1'e, 45 MW yük alan 2'ye bağlandı

5.2 Sınıflandırıcı Yapısı

OÜK, bir elektrik santralinin hız regülatörlerinin ayar noktalarını düzenleyerek şebeke frekansını istenilen değerde tutmayı sağlamaktadır. Bu ayar noktalarının düzenlenmesi için OÜK, SCADA sistemi tarafından sağlanan bağlantı hattı ve frekans ölçümlerini kullanmaktadır. Ölçülen her değişken sistem boyunca meydana gelen dinamik duruma beklenmeyen bir etki yapabilmektedir. Fakat sistemde bulunan tüm ölçümlerin sınıflandırıcı yapısına dahil edilmesi yüksek boyutluluk oluşturmakta ve hesaplama maliyetini arttırmaktadır. Maliyetin artması ile birlikte aşırı öğrenme (overfitting) riski meydana gelmektedir.

Üst paragrafta açıklanan nedenlerden ötürü, FDI saldırılarının sınıflandırılmasında Torbalama Ağaçları "Bagged Trees" (BT) algoritması önerilmektedir. Torbalama Ağaçları, bir topluluk sınıflandırma algoritmasıdır. Birden çok karar ağacının bir araya gelmesiyle daha güçlü bir sınıflandırma modeli oluşturulmaktadır. Algoritmanın işleyişi basitçe aşağıdaki adımları takip etmektedir.

1. Veri kümesi rastgele örneklemler ile yeniden örneklenmektedir. Şekil 5.9'da görünen her bir torba bu veri setinden rastgele bir şekilde seçilerek elde edilmektedir.

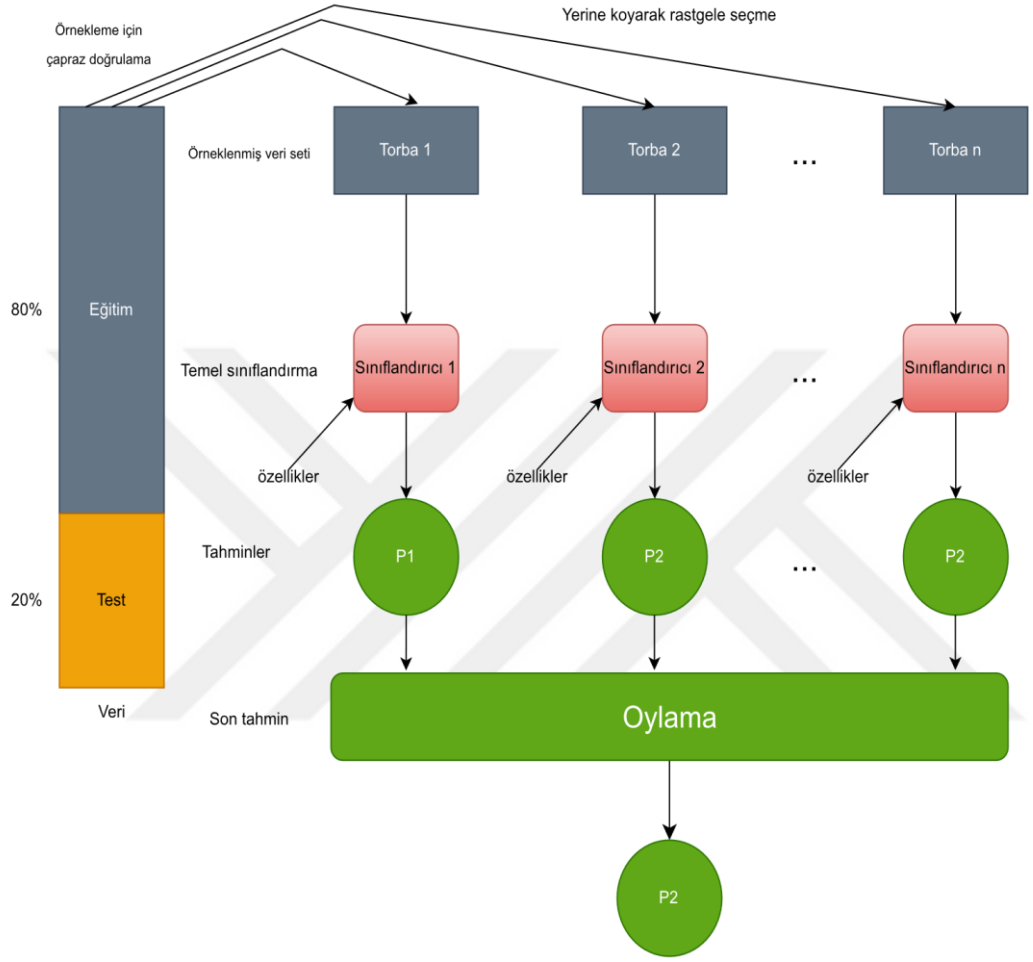
2. Elde edilen her bir veri kümesi (torba) için ayrı bir karar ağacı oluşturulmaktadır. Karar ağaçları, verileri sınıflandırmak için veri kümesindeki özellikleri kullanmaktadır.

3. Her bir sınıflandırıcı, sınıflandırıcı eğitiminde kullanılan örnekleme verilerinin üzerinde bağımsız olarak çalışmakta ve sınıflandırma yapmaktadır.

4. Tüm karar ağaçlarının (sınıflandırıcı) sınıflandırma sonuçları bir araya getirilerek oybirliği (majority voting) prensibiyle son sınıflandırma kararı verilmektedir. Yani her bir sınıflandırıcının verdiği sınıf etiketleri sayılmakta ve en çok tahmin edilen sınıf etiketi, BT'nın tahmin ettiği sınıf etiketi olarak seçilmektedir.

Torbalama Ağaçları birden çok karar ağacını birleştirerek bir topluluk modeli oluşturmaktadır. Her bir karar ağacı farklı veri örneklemleri ile eğitildiği için çeşitlilik sunmaktadır. Bu saldırıların ve normal durumların tespiti için daha güvenilir sonuçlar elde edilmesine katkıda bulunmaktadır. Ek olarak önerilen algoritma paralel olarak çalışmaktadır. Yani her bir karar ağacı bağımsız olarak çalışmakta, eğitim ve tahmin işlemlerini hızlandırmaktadır. Topluluk öğrenmesi algoritmalarının yapısından dolayı

bir karar ağacının hata yapması durumunda diğer karar ağaçları bu sonucu dengelemekte ve bu sayede hata yapılması riskini azaltmaktadır. Öte yandan büyük veri setlerinde etkili olarak kullanılabilmesi ve ölçeklenebilirliği nedeniyle OÜK sistemlerinde saldırı tespiti için önerilmektedir.



Şekil 5.9: Önerilen çoklu sınıflandırıcı yapısı.

5.3. Eğitim Aşaması

Bagged trees (Bagging+Trees) algoritması, Bagging (Bootstrap aggregating) yöntemi kullanarak karar ağaçlarının topluluğunu oluşturmaktadır. Bu topluluk, daha güçlü ve kararlı bir tahmin modeli elde etmek için birden çok karar ağacının tahminlerini birleştirmektedir. Bu bölümde eğitim işlemi açıklanmaktadır.

1. $D = \{(x_1, y_1), (x_2, y_2), \dots, (x_n, y_n)\}$ eğitim veri kümesi olsun. Burada, x_i örneklemenin özellik vektörünü temsil etmekte ve y_i ise etiketi (hedef değer) temsil etmektedir.

2. B alt kümeleri oluşturulmaktadır. Her bir alt küme orijinal veri setinden elde edilen rastgele örneklemeler sonucunda oluşmaktadır. B alt kümeleri D_1, D_2, …, D_B şeklinde gösterilmektedir.

3. Karar ağaçlarının eğitilmesi her torbalama alt kümesinde gerçekleştirilmektedir. CART algoritması, karar ağacı eğitimi için yaygın olarak kullanılmaktadır. Karar ağacı modelleri T_1, T_2, …, T_B olarak gösterilmektedir.

4. Her karar ağacı modelinde kullanılmak üzere girdi örneği x için tahmin edilen değer elde edilmektedir. Çoğunluk oylaması sonucunda, tahmin edilen sınıf etiketi en yüksek oyu alan etiket değeri olarak belirlenmektedir. Aşağıda BT algoritmasının eğitim prosedürü genel aşamaları verilmektedir.

Torbalama alt kümelerinin oluşturulmasının kısa özeti aşağıda açıklanmaktadır.

D_1, D_2, …, D_B= Rastgele_Ornekleme(D)

Karar ağaçlarının eğitilmesi:

T_1 = Karar_Agaci_Egitim(D_1)

T_2 = Karar_Agaci_Egitim(D_2)

...

T_B = Karar_Agaci_Egitim(D_8)

Tahminlerin birleştirilmesi:

Tahmin(x) = Cogunluk_Oylamasi((T_1(x), (T_2(x), ..., (T_B(x))

Burada T_i(x), i'nci karar ağacı tarafından girdi örneği x için tahmin edilen değeri temsil etmektedir. Çizelge 5.2'de eğitim aşaması için kullanılan hiperparametre değerleri yer almaktadır. Ayrıca karşılaştırma için kullanılan diğer üç algoritmanın da parametreleri Çizelge 5.3, Çizelge 5.4 ve Çizelge 5.5'de yer almaktadır.

Çizelge 5.2: Önerilen model hiperparametreleri.

Hiperparametre adı	Değer
Topluluk (Ensemble) metodu	Torbalama (Bagging)
Öğretici tipi	Karar ağacı
Bölünmelerin maksimum sayısı	$6{,}899 \times 10^4$
Öğreticilerin sayısı	30
Örneklenecek tahminci sayısı	Tümü seçili
Eğitim süresi	109.58 sn

Çizelge 5.3: Karar Ağaçları modeli hiperparametreleri.

Hiperparametre adı	Değer
Bölünmelerin maksimum sayısı	100
Bölünme kriteri	Gini bölünme endeksi
Vekil karar bölünmeleri	Kapalı
Eğitim süresi	30.225 sn

Çizelge 5.4: k-NN modeli hiperparametreleri.

Hiperparametre adı	Değer
Komsuların sayısı	10
Uzaklık metriği	Euclidean
Mesafe ağırlığı	Eşit
Standartlaştırılmış veri	Evet
Eğitim süresi	39.143 sn

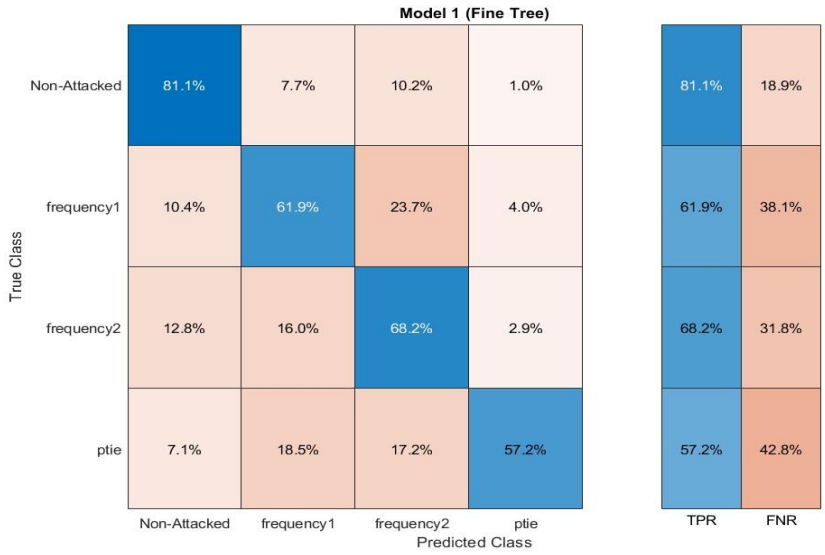
Çizelge 5.5: YSA modeli hiperparametreleri.

Hiperparametre adı	Değer
Tamamen bağlı katman sayısı	1
İlk katman boyutu	10
Aktivasyon fonksiyonu	ReLU
İterasyon limiti	1000
Düzenlileştirme gücü (Lambda)	0
Standartlaştırılmış veri	Evet
Eğitim süresi	641.9 sn

6. SONUÇLAR VE TARTIŞMA

6.1 Test Sisteminde %0 RES

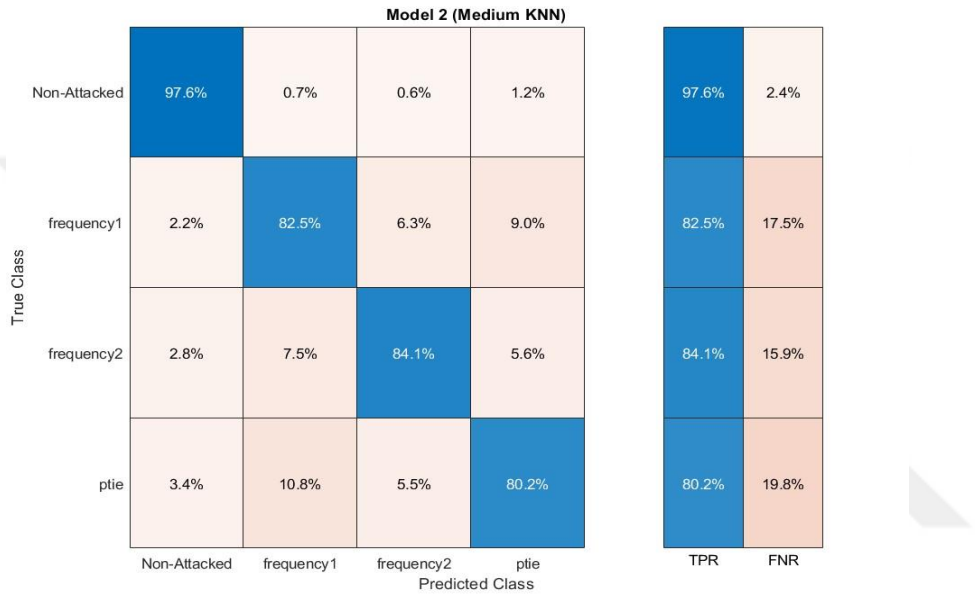
Yapılan saldırılar hangi ölçümü hedef aldığına göre üç gruba ayrılmaktadır. Ayrıca bir grup da saldırı olmayan durumu temsil etmektedir. RES olmayan duruma göre elde edilen veriler ile eğitilen karar ağacı algoritması hata matrisi Şekil 6.1'de verilmektedir. Alan 2 frekansına yapılan saldırıların %12.8 oranında saldırı yok olarak tespit edilmesi sistem kararlılığı için görülen en büyük tehlikedir. Yani frekans 2 değerine yapılan saldırıların %12.8'i, saldırı yok (Non-Attacked) olarak tahmin edilmektedir. Bu durum sisteme saldırı varken yok olarak tahmin edilen durumlar arasında en yüksek oran olarak göze çarpmaktadır. Bu hata oranı ile saldırganlar sistem kararlılığını bozmak için yeterli veriyi sisteme enjekte edebilmektedirler. Ayrıca algoritma %42.8 Yanlış Pozitif Oranı (FNR) ile en yüksek hatalı tahmini bağlantı hattı gücüne yapılan saldırıları tespit etmekte yapmaktadır. Yani en çok yanlış sınıflandırılan saldırı türü bağlantı hattı gücüne (ptie) yapılan saldırılar olmaktadır.



Şekil 6.1: Karar Ağacı Algoritması ile saldırı tespiti hata matrisi (%0 RES).

k-NN algoritması 0.800 doğruluk oranına sahiptir. Şekil 6.2'ye göre en çok hata, %19.8 FNR ile bağlantı hattı gücüne yapılan saldırıların sınıflandırılmasında gerçekleşmektedir.

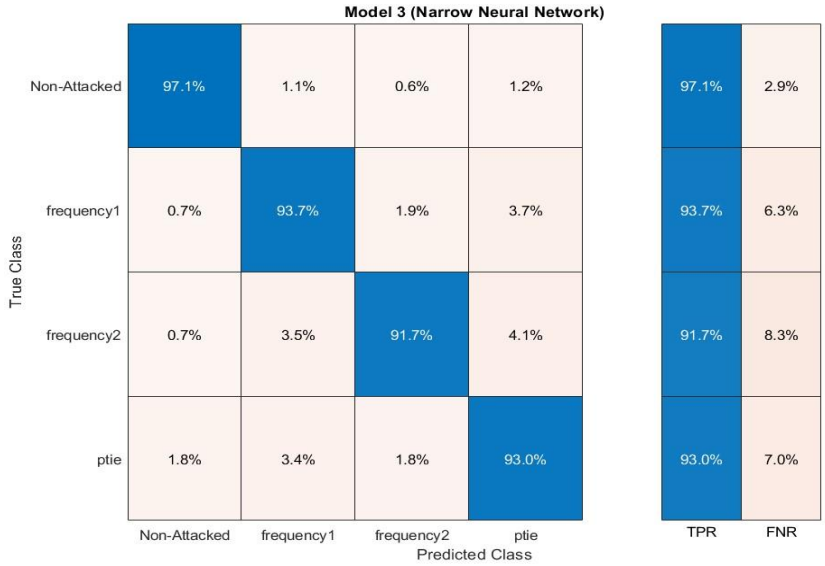
İkinci önemli durum ise %3.4 ile bağlantı hattı gücüne yapılan saldırının saldırı yok olarak sınıflandırılmasıdır. Saldırı varken yok olarak sınıflandırılması sistem kararlılığını etkileyebilecek önemli metriklerden biridir. k-NN algoritması, karar ağacı algoritmasına göre daha başarılı olmaktadır.



Şekil 6.2: k-En Yakın Komşular Algoritması ile saldırı tespiti hata matrisi (%0 RES).

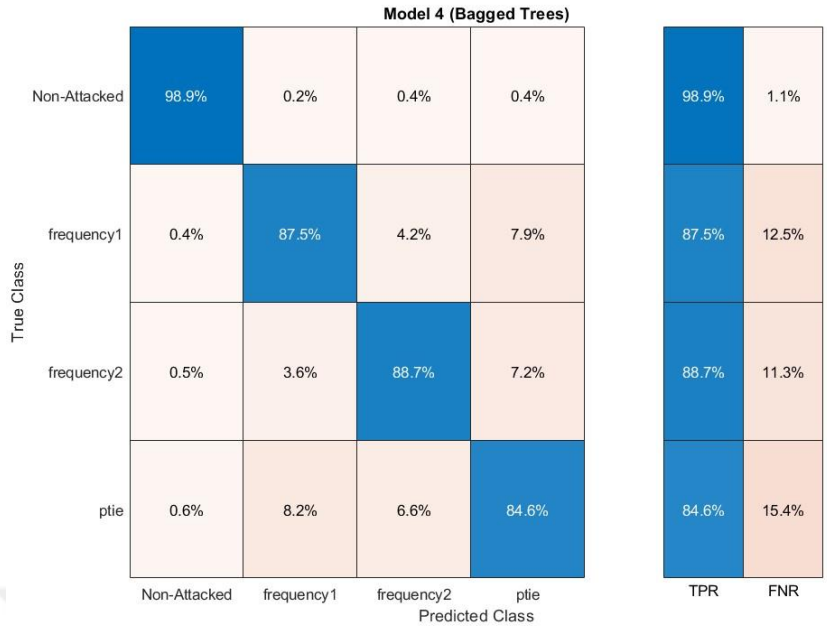
0.924 doğruluk oranı ile yapay sinir ağları en yüksek doğruluk oranına sahiptir. Şekil 6.3'den de görüldüğü üzere sırasıyla %97.1, %93.7, %91.7 ve %93.0 Doğru Pozitif Oranı (TPR) ile saldırıların büyük çoğunluğunu doğru sınıflandırmaktadır. YSA, en yüksek hatayı %8.3 ile alan 2 frekansına yapılan saldırının tespitinde yapmaktadır.

İki sınıf arasındaki sınıflandırmada ise en yüksek hatayı %4.1 ile alan 2 frekansına yapılan saldırıyı, bağlantı hattı gücüne yapılan saldırı olarak tahmin ederek yapmaktadır.



Şekil 6.3: Yapay Sinir Ağları ile saldırı tespiti hata matrisi (%0 RES).

Saldırı tespiti için kullanılan dördüncü algoritma ise topluluk modelleri kapsamında değerlendirilen torbalama ağaçları algoritmasıdır. Bu yöntem torbalama yöntemi kullanılarak oluşturulan karar ağaçlarıdır. Torbalama Ağaçları algoritması, her bir karar ağacını bağımsız olarak farklı veri örnekleriyle eğiterek birleştirmekte ve veri setinin örnekleme rastgeleliğini kullanarak ağaçların farklı örneklemeler ile de öğrenebilmesini sağlamaktadır. Bu da genel performansı arttırabilir ve aşırı öğrenme "overfitting" sorununu azaltabilmektedir. Ek olarak bu yöntem 0.920 doğruluk oranına sahiptir. Şekil 6.4'de görüldüğü gibi saldırı varken saldırı yok olarak tahmin ettiği en yüksek veri oranı bağlantı hattı gücüne yapılan saldırıdır. Bu oran sadece %0.6'dır. Bir tespit algoritmasının en önemli görevi olan saldırı tespitinde diğer algoritmalardan daha üstündür. En yüksek hatayı ise bağlantı hattı gücüne yapılan saldırıların tespitinde yapmaktadır.

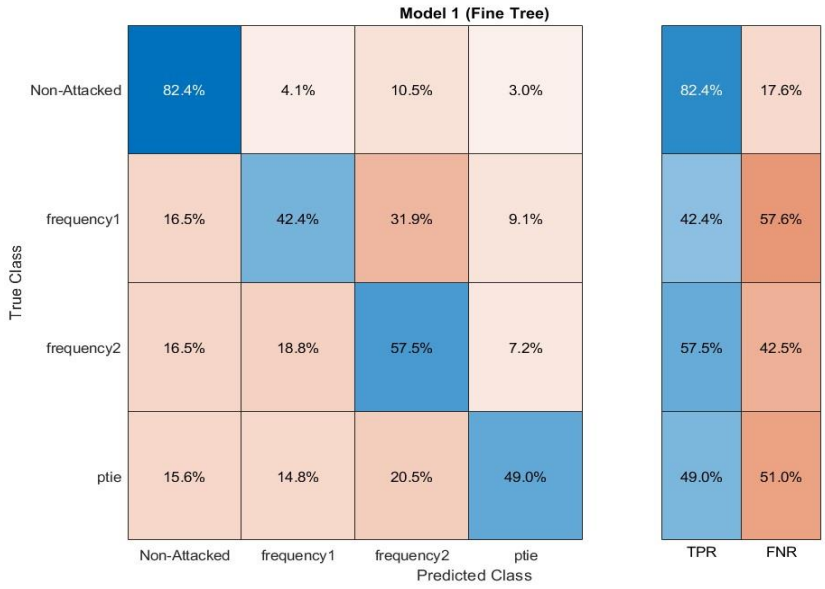


Şekil 6.4: Torbalama Ağaçları ile saldırı tespiti hata matrisi (%0 RES).

6.2 Test Sisteminde %10 RES

Bölüm 5.2'de açıklandığı gibi toplam gücü 90MW olacak RES sisteme eklenmektedir. Farklı senaryolar sonucu toplanan veriler, ayrı bir veri seti olarak saldırı tespiti için kullanılacak olan algoritmaların eğitimi için ayrılmaktadır.

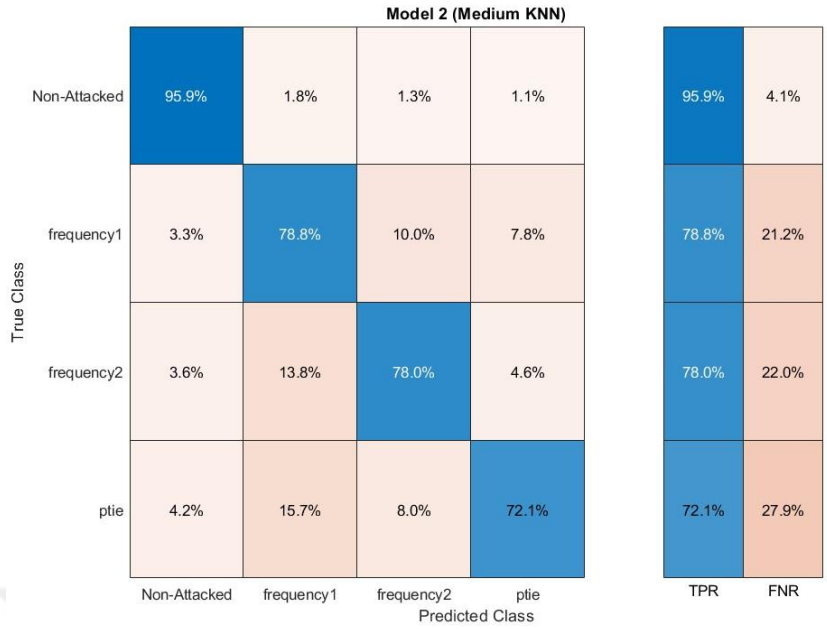
Karar ağacı algoritması bu test sistemi için 0.630 doğruluk oranına sahiptir. Bu oran RES entegresi olmayan sisteme göre oldukça düşüktür. Ek olarak Şekil 6.5'te görülen hata matrisine göre bütün saldırıların tespit oranları RES entegresi olmayan duruma göre düşmektedir. Karar ağacı algoritması alan 1 frekansına yapılan saldırıların sadece %42.4'ünü doğru sınıflandırabilmektedir. Ayrıca bir diğer göze çarpan detay ise frekans 1'e %16.5, frekans 2'ye %16.5 ve bağlantı hattı gücüne %15.6 oranında yapılan saldırıların saldırı yok olarak tespit edilmesi olmaktadır.



Şekil 6.5: Karar Ağacı algoritması ile saldırı tespiti hata matrisi (%10 RES).

Daha önce de açıklandığı gibi bu durum sistem kararlılığının bozulmasına yetebilecek bir orandır. Ek olarak KA algoritması %31.9 oranında bir veriyi, frekans 1'e saldırı varken frekans 2'ye bir saldırı olarak tespit etmektedir. Bu yanlış sınıflandırma güç sistemi operatörlerini yanlış yönlendirmekte ve yapılacak eylemlerin hatalı olmasına neden olabilmektedir.

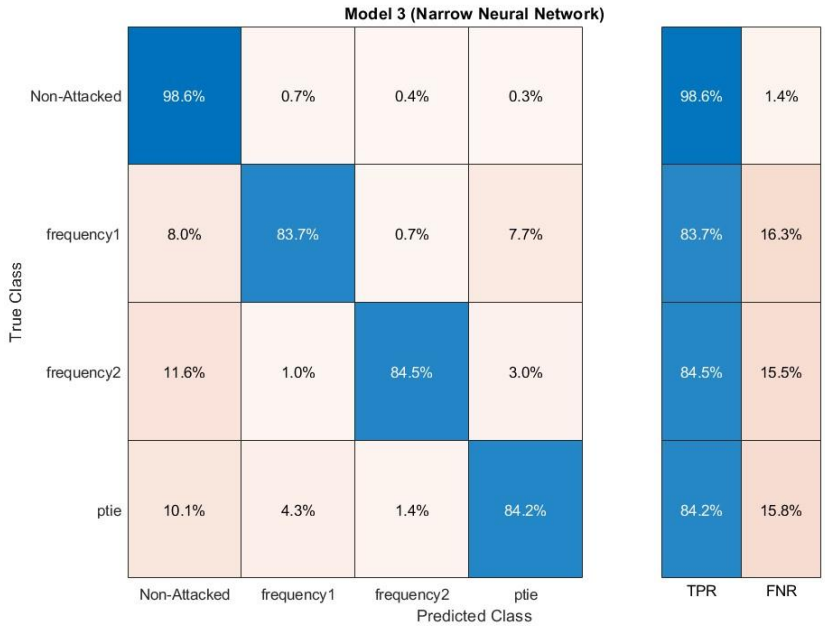
k-en yakın komşular algoritması %10 RES olan durum için saldırıların tespitinde 0.842 doğruluk oranına ulaşmaktadır. Bu algoritmada da güç sistemine RES eklenmesi doğruluk oranını düşürmektedir. Şekil 6.6'da görülen hata matrisinde ise yine RES olmayan duruma göre hata oranları artmaktadır. En büyük hata ise %27.9 oranı ile güç akışı ölçümlerine yapılan saldırılar sonucunda ortaya çıkmaktadır. Karar ağacı algoritması ile karşılaştırıldığında sınıflandırmada daha başarılı sonuçlara ulaştığı görülmektedir.



Şekil 6.6: k-En Yakın Komşular algoritması ile saldırı tespiti hata matrisi (%10 RES).

7 ve 9 numaralı baralara eklenen toplam 90MW gücündeki RES ile elde edilen veriler sonucunda eğitilen YSA algoritması, saldırı tespitinde 0.889 doğruluk oranına ulaşmaktadır. YSA algoritmasında da doğruluk oranı RES olmayan güç sistemine göre daha düşük kalmaktadır.

Ek olarak Şekil 6.7'de verilen hata matrisi ile saldırı tespit oranlarının düştüğü açıkça gözlemlenmektedir. En çok dikkat çeken noktalardan biri ise sırasıyla %8.0-%11.6-%10.1 yanlış veri tespiti ile frekans 1, frekans 2 ve bağlantı hattı gücü sınıflarında yapılan hatalı sınıflandırma olmaktadır. Yapılan bu hatalı sınıflandırma, sisteme saldırı varken yok olarak tahmin edilmesine neden olmaktadır. Oluşan yanlış algı sonucunda, güç sistemi operatörü güç sistemini yük atmaya veya üretim atmaya götürecek eylemleri yapmaktadır.



Şekil 6.7: Yapay Sinir Ağları ile saldırı tespiti hata matrisi (%10 RES).

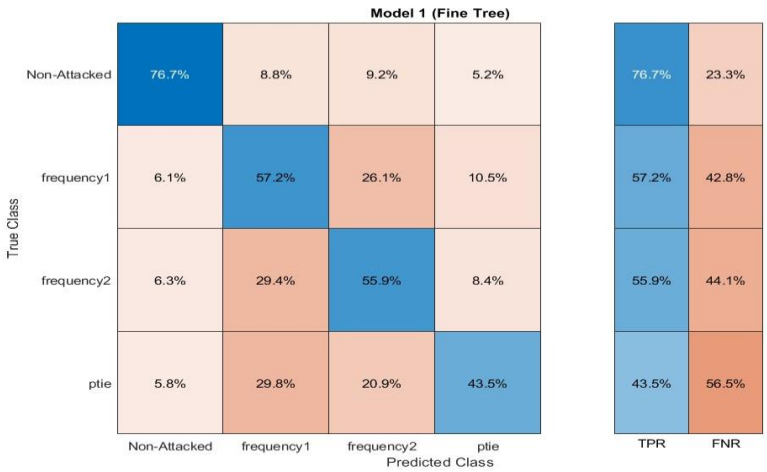
Torbalama ağaçları algoritması ile %10 RES entegresi durumunda doğruluk oranı 0.871 olmaktadır. Görüldüğü üzere RES entegresi bu algoritma için de doğruluk oranını düşürmektedir. Bu algoritmada dikkat çeken nokta, sistemde saldırı varken saldırı yok olarak tahmin ettiği oranların çok düşük olmasıdır. Örneğin şekil 6.8'e bakıldığında frekans 1'e saldırı varken saldırı yok olarak tahmin ettiği oran sadece %1.4'dür. Diğer saldırı noktaları için de bu oran diğer tüm algoritmalara göre daha düşük olmaktadır. Bunun dışında frekans 1'e yapılan saldırıları %80.0, frekans 2'ye %82.1 ve bağlantı hattı gücüne %78.1 ile tahmin etmektedir. Diğer algoritmalar ile karşılaştırıldığında %10 RES eklenmiş olan güç sistemine yapılan saldırılarda en başarılı algoritmanın torbalama ağaçları olduğu söylenebilmektedir.

Şekil 6.8: Torbalama Ağaçları ile saldırı tespiti hata matrisi (%10 RES).

6.3 Test Sisteminde %20 RES

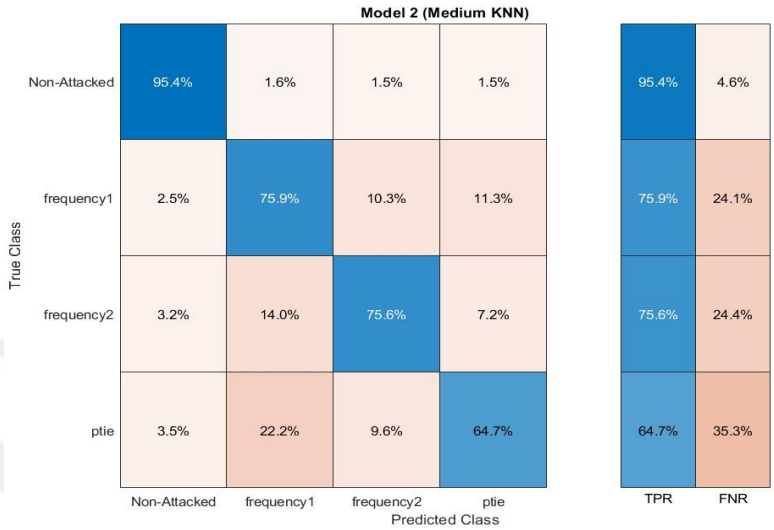
Bu bölümde yedi ve dokuz numaralı baralara toplam 180 MW gücünde RES eklenmektedir. Bu veri setinin %30'u test verisi olarak ayrılmaktadır. Eğitilen bu algoritmalar sonra test verisi ile test edilmekte ve aşağıda verilen sonuçlar elde edilmektedir.

Şekil 6.9'da ise %20 RES ilavesi durumunda karar ağacı algoritması hata matrisi verilmektedir. Karar ağacı algoritmasının doğruluk oranı %20 RES eklenmesi sonucu 0.622 değerine düşmektedir. Görüldüğü üzere RES entegrasyonu, KA algoritması ile saldırı tespit oranlarını düşürmektedir.



Şekil 6.9: Karar Ağacı algoritması ile saldırı tespiti hata matrisi (%20 RES).

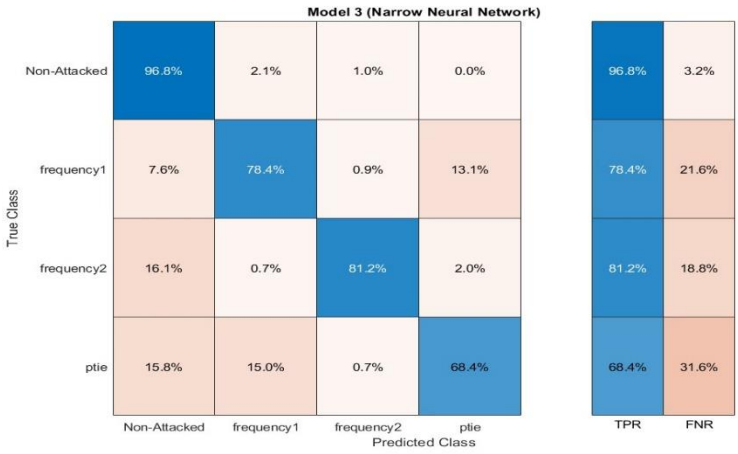
Şekil 6.10'da ise %20 RES ilavesi durumunda k-en yakın komşu algoritması hata matrisi verilmektedir. Bu şartlarda doğruluk oranı 0.821 olarak tespit edilmektedir. Görüldüğü üzere güç sistemindeki rüzgar enerjisi gücünün artması k-en yakın komşu algoritmasının doğruluk oranlarını düşürmektedir.



Şekil 6.10: k-NN algoritması ile saldırı tespiti hata matrisi (%20 RES).

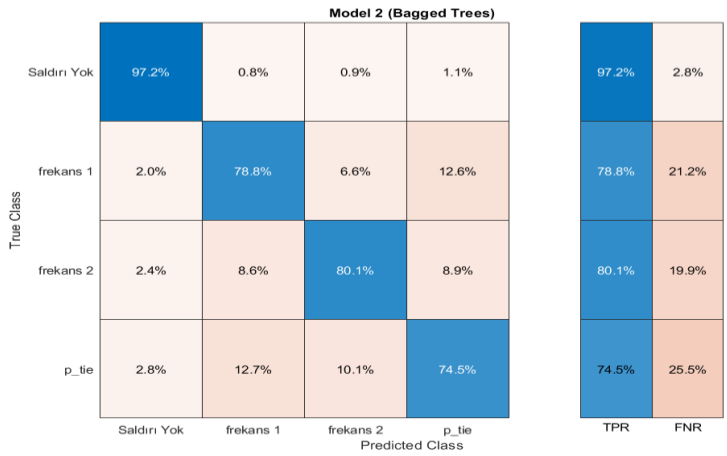
Şekil 6.11'de, 7 ve 9 numaralı baralara eklenen toplam 180MW gücündeki RES ile elde edilen veriler sonucunda eğitilen YSA algoritması hata martisi görülmektedir. Bu şartlar altında YSA algoritması saldırı tespitinde 0.814 doğruluk oranına ulaşılmaktadır. Bu algoritmada da doğruluk oranı sistemdeki RES oranı arttıkça düşüş göstermektedir. En büyük artış bağlantı hattı gücüne yapılan saldırılarda oluşmaktadır. Güç sistemine %20 RES ilavesi durumu için YSA algoritmasının saldırı tespitinde en zayıf olduğu nokta, iki alan arasındaki güç akışının kontrol merkezine iletildiği haberleşme noktaları olmaktadır.

Sistemdeki RES oranının %20 seviyesine ulaşmasıyla birlikte en yüksek doğruluk oranına 0.855 ile Torbalama Ağaçları algoritması ulaşmaktadır. Ayrıca en tehlikeli yanlış alarm durumlarından olan sisteme saldırı varken yok olarak tahmin edilmesi durumunu en düşük seviyeye indiren algoritma Torbalama Ağaçları algoritması olmaktadır. Bu algoritma için RES oranının artması, yanlış alarm durumu çok küçük bir oranda arttırmaktadır.



Şekil 6.11: Yapay Sinir Ağları ile saldırı tespiti hata matrisi (%20 RES).

Örneğin algoritmada RES entegresi yokken frekans 1 değerine yapılan saldırının saldırı yok olarak tahmin edilmesi %0.5 oranındayken %20 RES entegresi durumunda aynı durum %2.0 olarak tahmin edilmektedir. Torbalama Ağaçları algoritmasında diğer algoritmalara kıyasla güç sisteminde RES entegresinin artması saldırı tespiti ve sınıflandırılması oranını fazla düşürmemektedir. Fakat diğer algoritmalarda olduğu gibi BT algoritması da bağlantı hattı gücüne yapılan saldırıların tespitinde oldukça zorlanmaktadır. Şekil 6.12'de gösterildiği gibi en yüksek yanlış sınıflandırma oranına bu noktaya yapılan saldırılar neden olmaktadır. Bu çalışmadaki tüm deneyler 2.3 GHz hızında i7-12650H CPU, 16 GB RAM, 64-bit Windows işletim sistemine sahip dizüstü bilgisayarda gerçekleştirilmektedir.



Şekil 6.12: Torbalama Ağaçları ile saldırı tespiti hata matrisi (%20 RES).

Çizelge 6.1: RES ilavesi oranına göre makine öğrenmesi algoritmalarının performans değerlendirmesi.

Makine öğrenmesi algoritmaları	Ölçüm metrikleri	Saldırı yok			Alan-1 frekansına saldırı			Alan-2 frekansına saldırı			Bağlantı hattı gücüne saldırı		
		0% (RES)	10% (RES)	20% (RES)	0% (RES)	10% (RES)	20% (RES)	0% (RES)	10% (RES)	20% (RES)	0% (RES)	10% (RES)	20% (RES)
BT	**Kesinlik**	0.992	0.971	0.964	0.877	0.780	0.771	0.885	0.842	0.813	0.841	0.785	0.757
	Duyarlılık	0.989	0.973	0.973	0.875	0.800	0.788	0.887	0.821	0.801	0.846	0.781	0.740
	F1	0.990	0.972	0.968	0.876	0.790	0.776	0.886	0.831	0.810	0.843	0.783	0.748
KA	**Kesinlik**	0.843	0.773	0.894	0.553	0.504	0.427	0.526	0.439	0.460	0.866	0.687	0.597
	Duyarlılık	0.811	0.824	0.767	0.619	0.424	0.572	0.682	0.575	0.559	0.572	0.490	0.435
	F1	0.827	0.798	0.826	0.589	0.461	0.489	0.594	0.498	0.505	0.689	0.572	0.503
k-NN	**Kesinlik**	0.959	0.945	0.954	0.807	0.705	0.658	0.866	0.792	0.768	0.825	0.832	0.750
	Duyarlılık	0.976	0.959	0.954	0.825	0.788	0.759	0.841	0.780	0.756	0.802	0.721	0.647
	F1	0.967	0.952	0.954	0.816	0.744	0.705	0.853	0.786	0.762	0.813	0.773	0.695
YSA	**Kesinlik**	0.984	0.870	0.830	0.911	0.926	0.797	0.951	0.966	0.957	0.901	0.883	0.820
	Duyarlılık	0.971	0.986	0.968	0.937	0.837	0.784	0.917	0.845	0.812	0.930	0.842	0.684
	F1	0.977	0.924	0.894	0.924	0.879	0.790	0.934	0.901	0.879	0.915	0.862	0.746

7. SONUÇLAR VE GELECEK ÇALIŞMALAR

Bu tezde OÜK sistemlerine yapılan siber saldırıların tespiti için makine öğrenimi temelli bir topluluk öğrenme algoritması önerilmektedir. Bu bağlamda, öncelikle genelleştirilmiş 2-Alanlı bir güç sistemi oluşturulmaktadır. Oluşturulan bu sisteme, OÜK'de meydana gelen GDB, GRC ve zaman gecikmesi doğrusalsızlıkları entegre edilmektedir. Simülasyonlar sonucunda bu doğrusalsızlıkların sistem dinamiklerini etkilediği kanısına varılmaktadır. Yapılan tüm simülasyonlar için bu doğrusalsızlıklar sisteme dahil edilmektedir.

Sonraki aşamada çeşitli siber saldırı şablonları oluşturulmakta ve genelleştirilmiş test sistemi üzerindeki etkileri analiz edilmektedir. Çeşitli parametre değerleri ile gerçekleştirilen bu saldırı şablonlarının, sistem frekansını yük ve üretim atma gibi üçüncül kontrol eylemlerine götürdüğü kanıtlanmaktadır.

Saldırıların kapsamlı analizi için, belirlenen saldırı şablonları iki alanlı test sistemine uygulanmaktadır. Oluşturulan saldırı şablonları gerçek bir test sistemi üzerinde de etkili olmakta ve güç sistemini üçüncül kontrol döngüsü eylemlerini almaya zorlamaktadır. Bu saldırıların tespiti için KA, k-NN, YSA ve BT yöntemleri karşılaştırılmaktadır. Bu yöntemlerin kapsamlı performans değerlendirmeleri için iki alanlı test sistemine %10 ve %20 oranında RES eklenmektedir. Farklı oranlarda RES entegresi ile oluşturulan üç test sistemine yapılan siber saldırıların tespiti verilen dört farklı makine öğrenmesi yöntemiyle yapılmaktadır. Elde edilen sonuçlar aşağıda yer almaktadır:

Sisteme entegre edilen RES oranı arttıkça bütün algoritmaların saldırı tespit etme oranları düşmektedir. YSA algoritması ve BT algoritması artan RES oranına göre en başarılı iki algoritma olarak öne çıkmaktadır.

Oluşturulan OÜK sistemi için sınıflandırılması en zor olan saldırı bağlantı hattı gücüne yapılan saldırılar olmaktadır. Hata matrislerine bakıldığında Karar Ağaçları algoritması sırasıyla %0-10-20 RES oranlarında %42.8-51.0-56.5 ile en yüksek FPR

oranını bağlantı hattı gücüne yapılan saldırıların sınıflandırılmasında elde etmektedir. k-NN algoritması sırasıyla %0-10-20 RES entegresinde, %19.8-27.9-35.3 ile en yüksek FPR oranını bağlantı hattı gücü ölçümlerinin sınıflandırılmasında oluşturmaktadır. YSA algoritması sistemde RES olmadığı durumda, %8.3 ile en yüksek FPR oranını frekans-2 ölçümlerinin sınıflandırılmasında oluşturmaktadır. Fakat %10 ve %20 RES ilave edilmesiyle birlikte YSA algoritması sırasıyla %15.8 ve %31.6 ile en yüksek FPR oranını bağlantı hattı gücü ölçümlerinin sınıflandırılmasında elde etmektedir. BT algoritması sırasıyla %0-10-20 RES entegresinde, %15.4-21.9-25.5 ile en yüksek FPR oranını bağlantı hattı gücü ölçümlerinin sınıflandırılmasında oluşturmaktadır. Toplamda 12 durumdan 11 tanesinde en çok yanlış sınıflandırılan ölçümler bağlantı hattı gücüne yapılan saldırılar olmaktadır. Görüldüğü üzere RES oranının artması BT algoritmasının FPR oranını yükseltse de diğer algoritmalara göre daha dirençli olmaktadır.

OÜK sistemlerine yapılan siber saldırıların tespiti için önerilen BT algoritması, sırasıyla %0-10-20 RES oranlarında, 0.920-0.871-0.855 doğruluk oranı ile iyi bir performans yakalamaktadır.

YSA ise sırasıyla %0-10-20 RES oranlarında, 0.924-0.889-0.814 doğruluk oranlarına ulaşmaktadır. Görüldüğü üzere doğruluk oranları oldukça yakındır. Ek olarak Çizelge 6.1'e bakıldığında YSA ve BT en başarılı iki algoritma olarak öne çıkmakta ve diğer ölçüm metriklerine göre de iki algoritma benzer sonuçlar elde etmektedir.

Şekil 6.3'de görüldüğü üzere %0 RES entegresi varken en tehlikeli yanlış alarm (saldırı varken yok olarak tahmin edilmesi) oranı %0.7-0.7-1.8 olan YSA, RES oranı arttıkça Şekil 6.7 ve Şekil 6.11'de verilen hata matrislerinde görüldüğü gibi daha yüksek oranlara çıkmaktadır. BT algoritması için ise RES oranının artması bu yanlış alarm durumunu çok küçük bir oranda arttırmaktadır. Sonuç olarak en tehlikeli yanlış alarm durumu için, karşılaştırılan algoritmalar arasından BT algoritması en başarılısı olarak tespit edilmektedir. Fakat genel olarak saldırı tespitinde YSA daha başarılıdır.

Çizelge 5.2 ile Çizelge 5.5'e bakıldığında BT algoritmasının eğitim süresinin 109.58 sn, YSA algoritmasının eğitim süresinin ise 641.9 sn olduğu görülmektedir. Önerilen BT algoritması, karar ağaçlarının bağımsız olarak çalışması ve paralel hesaplamaların yapılmasını sağladığı için YSA'na göre daha hızlıdır. Bu, OÜK sistemine yapılan saldırıların gerçek zamanlı olarak tespit edilmesini kolaylaştırmaktadır.

Sonuç olarak, önerilen metodoloji OÜK sistemlerine yapılan FDI saldırılarının çoklu sınıflandırmasında uygulanabilecek bir seçenek olduğu gerekçelendirilmektedir. Ayrıca aşağıda daha fazla çalışma gerektirebilecek noktalar verilmekte ve bu noktalar gelecekte yapılacak çalışmalar olarak kabul edilmektedir:

Daha gerçekçi bir güç sistemi modeli için röle ve özel koruma ekipmanları entegre edilebilir.

Enerji depolama birimleri, dağıtılmış üretim, rüzgar türbinlerine OÜK entegre edilmesi ve sanal atalet benzetim teknolojilerinin dahil edilmesi güç sisteminin yapısını değiştirecektir ve bu sayede yenilenebilir enerjinin bazı olumsuz etkilerini azaltabilir. Bu teknolojiler dahil edilerek yapılacak çalışmalar sistem güvenilirliği açısından farklı bir bakış sağlayabilir.

Alan sayısının 2'den fazla olması siber açıklıkları arttırır. Çok alanlı bir güç sistemi için tespit ve azaltma algoritmaları geliştirilebilir.

Tezde, elektrik piyasası üzerindeki herhangi bir etki dikkate alınmamıştır. Fakat sistemin ekonomik çalışması da göz önüne alınırsa gelecekteki çalışmalar için bu tür faktörlerin belirsizliği ile ilgili çalışmalar ilgi çekici olabilir.

KAYNAKLAR

[1] **Amitkumar, V., Appasani, B., Pattanayak, P., Gurjar, D., Kabalci, E., & Mohanta, D.** (2021). Smart grid cyber-physical systems: communication technologies, standards and challenges. *Wireless Networks*, s. 2595–2613.

[2] **Url-1** <*https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01*>, erişim tarihi 20.07.2021.

[3] **Liu, Y., Ning, P., & Reiter, M. K.** (2011). False data injection attacks against state estimation in electric power grids. *ACM Transactions on Information and System Security (TISSEC), 14*(1), 1-33.

[4] **Teixeira, A., Pérez, D., Sandberg, H., & Johansson, K. H.** (2012). Attack models and scenarios for networked control systems. *Proceedings of the 1st international conference on High Confidence Networked Systems.*

[5] **Sridhar, S., & Govindarasu, M.** (2014). Model-Based Attack Detection and Mitigation for Automatic Generation Control. *IEEE Transactions on Smart Grid, 5*(2), 580-591.

[6] **Tan, R., Nguyen, H. H., Foo, E. Y., Dong, X., Yau, D. K., Kalbarczyk, Z., Gooi, H. B.** (2016). Optimal False Data Injection Attack against Automatic Generation Control in Power Grids. *ACM/IEEE 7th International Conference on Cyber-Physical Systems (ICCPS).*

[7] **Liang, G., Zhao, J., Luo, F., Weller, S. R., & Dong, Z. Y.** (2017). A Review of False Data Injection Attacks Against Modern Power Systems. *IEEE Transactions on Smart Grid, 8*(4), 1630-1638.

[8] **Yang, Q., Yang, J., Yu, W., An, D., Zhang, N., & Zhao, W.** (2014). On False Data-Injection Attacks against Power System State Estimation: Modeling and Countermeasures. *IEEE Transactions on Parallel and Distributed Systems, 25*(3), 717-729.

[9] **Mohan, A. M., Meskin, N., & Mehrjerdi, H.** (2020). A Comprehensive Review of the Cyber-Attacks and Cyber-Security on Load Frequency Control of Power Systems. *Energies, 13*(15), 3860.

[10] **Bobba, R. B., Rogers, K. M., Wang, Q., Khurana, H., Nahrstedt, K., & Overbye, T. J.** (2010). Detecting False Data Injection Attackson DC State Estimation. *Preprints of the first workshop on secure control systems CPSWEEK.*

[11] **Dán, G., & Sandberg, H.** (2010). Stealth Attacks and Protection Schemes

for State Estimators in Power Systems. *First IEEE International Conference on Smart Grid Communications.* Gaithersburg, MD, USA.

[12] **Mishra, S., Li, X., Pan, T., Kuhnle, A., Thai, M. T., & Seo, J.** (2016). Price Modification Attack and Protection Scheme in Smart Grid. *IEEE Transactions on Smart Grid, 8*(4), 1864-1875.

[13] **Kim, T. T., & Poor, H. V.** (2011). Strategic Protection Against Data Injection Attacks on Power Grids. *IEEE Transactions on Smart Grid, 2*(2), 326-333.

[14] **Konstantinou, C., Sazos, M., Musleh, A. S., Keliris, A., Al-Durra, A., & Maniatakos, M.** (2017). GPS spoofing effect on phase angle monitoring and control in a real-time digital simulator-based hardware-in-the-loop environment. *IET Cyber-Physical Systems: Theory & ApplicationsVolume 2, Issue 4 p. 180-187, 2*(4), 180-187.

[15] **Wei, L., Sarwat, A. I., Saad, W., & Biswas, S.** (2018). Stochastic Games for Power Grid Protection Against Coordinated Cyber-Physical Attacks. *IEEE Transactions on Smart Grid, 9*(2), 684-694.

[16] **Ma, C. Y., Yau, D. K., Lou, X., & Rao, N. S.** (2012). Markov game analysis for attack-defense of power networks under possible misinformation. *IEEE Transactions on Power Systems, 28*(2), 1676-1686.

[17] **Sanjab, A., & Saad, W.** (2016). Data Injection Attacks on Smart Grids With Multiple Adversaries: A Game-Theoretic Perspective. *IEEE Transactions on Smart Grid, 7*(4), 2038-2049.

[18] **Liang, X., & Xiao, Y.** (2013). Game Theory for Network Security. *IEEE Communications Surveys & Tutorials, 15*(1), 472 - 486.

[19] **Sun, Y., Mao, Y., Liu, T., Sun, Y., Liu, Y., & Guan, X.** (2012). A dynamic secret-based encryption method in smart grids wireless communication. *IEEE PES Innovative Smart Grid Technologies.* Tianjin.

[20] **Li, X., & Hedman, K. W.** (2020). Enhancing Power System Cyber-Security With Systematic Two-Stage Detection Strategy. *IEEE Transactions on Power Systems, 35*(2), 1549-1561.

[21] **Yang, L., Li, Y., & Li, Z.** (2017). Improved-ELM method for detecting false data attack in smart grid. *International Journal of Electrical Power & Energy Systems, 91*, 183-191.

[22] **Wang, X., Luo, X., Zhang, M., & Guan, X.** (2019). Distributed detection and isolation of false data injection attacks in smart grids via nonlinear unknown input observers. *International Journal of Electrical Power & Energy Systems, 110*(5), 208-222.

[23] **Zhang, H., Liu, B., & Wu, H.** (2021). Smart Grid Cyber-Physical Attack and Defense: A Review. *IEEE Access, 9*, 9641 - 29659.

[24] **Ozay, M., Esnaola, I., Yarman Vural, F. T., Kulkarni, S. R., & Poor, H.**

V. (2016). Machine Learning Methods for Attack Detection in the Smart Grid. *IEEE Transactions on Neural Networks and Learning Systems, 27*(8), 1773-1786.

[25] **Zimmerman, R. D., Murillo-S´anchez, C. E., & Thomas, R. J.** (2011). MATPOWER: Steady-state operations, planning, and analysis tools for power systems research and education. *IEEE Transactions on Power Systems, 26*(1), 12-19.

[26] **Foroutan, S. A., & Salmasi, F. R.** (2017). Detection of false data injection attacks against state estimation in smart grids based on a mixture Gaussian distribution learning method. *IET Cyber-Physical Systems: Theory & Applications, 2*(4), 161-171.

[27] **Ganjkhani, M., Fallah, S. N., Badakhshan, S., Shamshirband, S., & Chau, K.-w.** (2019). A Novel Detection Algorithm to Identify False Data Injection Attacks on Power System State Estimation. *Energies, 12*(11), 2209.

[28] **He, Y., Mendis, G. J., & Wei, J.** (2017). Real-Time Detection of False Data Injection Attacks in Smart Grid: A Deep Learning-Based Intelligent Mechanism. *IEEE Transactions on Smart Grid, 8*(5), 2505-2516.

[29] **Ashrafuzzaman, M., Chakhchoukh, Y., Jillepalli, A. A., Tosic, P. T., de Leon, D. C., Sheldon, F. T., & Johnson, B. K.** (2018). Detecting Stealthy False Data Injection Attacks in Power Grids Using Deep Learning. *14th International Wireless Communications & Mobile Computing Conference (IWCMC).* Limassol.

[30] **Mohammadpourfard, M., Weng, Y., Pechenizkiy, M., Tajdinian, M., & Mohammadi-Ivatloo, B.** (2020). Ensuring cybersecurity of smart grid against data integrity attacks under concept drift. *International Journal of Electrical Power & Energy Systems, 119*.

[31] **Niu, X., Li, J., Sun, J., & Tomsovic, K.** (2019). Dynamic Detection of False Data Injection Attack in Smart Grid using Deep Learning. *IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT).* Washington, DC, USA.

[32] **Mohammadpourfard, M., Khalili, A., Genc, V. İ., & Konstantinou, C.** (2021). Cyber-Resilient Smart Cities: Detection of Malicious Attacks in Smart Grids. *Sustainable Cities and Society, 75*(103116).

[33] **Sakhnini, J., Karimipour, H., & Dehghantanha, A.** (2019). Smart Grid Cyber Attacks Detection Using Supervised Learning and Heuristic Feature Selection. *IEEE 7th International Conference on Smart Energy Grid Engineering (SEGE).* Oshawa, ON, Canada.

[34] **Kothari, M. L., Satsangi, P. S., & Nanda, J.** (1981). Sampled-Data Automatic Generation Control of Interconnected Reheat Thermal Systems Considering Generation Rate Constraints. *IEEE Transactions on Power Apparatus and Systems, 100*(5), 2334-

2342.

[35] **Shiroei, M., Toulabi, M. R., & Ranjbar, A. M.** (2013). Robust multivariable predictive based load frequency control considering generation rate constraint. *International Journal of Electrical Power & Energy Systems, 46*, 405-413.

[36] **Golpîra, H., & Bevrani, H.** (2011, May). Application of GA optimization for automatic generation control design in an interconnected power system. *Energy Conversion and Management*, s. 2247-2255.

[37] **Naduvathuparambil, B., Valenti, M. C., & Feliachi, A.** (2002). Communication delays in wide area measurement systems. *Proceedings of the Thirty-Fourth Southeastern Symposium on System Theory (Cat. No.02EX540).* Huntsville, AL, USA.

[38] **Rahimi, K., Parchure, A., Centeno, V., & Broadwater, R.** (2015). Effect of communication Time-Delay attacks on the performance of Automatic Generation Control. *North American Power Symposium (NAPS).* Charlotte, NC, USA.

[39] **Ayad, A., Khalaf, M., Salama, M., & El-Saadany, E. F.** (2022). Mitigation of false data injection attacks on automatic generation control considering nonlinearities. *Electric Power Systems Research, 209*(107958).

[40] **Khalaf, M., Youssef, A., & El-Saadany, E.** (2018). A Particle Filter-Based Approach for the Detection of False Data Injection Attacks on Automatic Generation Control Systems. *IEEE Electrical Power and Energy Conference (EPEC).* Toronto, ON, Canada.

[41] **Ayad, A., Khalaf, M., & El-Saadany, E.** (2018). Detection of False Data Injection Attacks in Automatic Generation Control Systems Considering System Nonlinearities. *IEEE Electrical Power and Energy Conference (EPEC).* Toronto, ON, Canada.

[42] **Semshchikov, E., Hamilton, J., Wu, L., Negnevitsky, M., Wang, X., & Lyden, S.** (2019). Frequency control within high renewable penetration hybrid systems adopting low load diesel methodologies. *Energy Procedia, 160*, 483-490.

[43] **Kumar, G. B., Sarojini, R. K., Palanisamy, K., Padmanaban, S., & Holm-Nielsen, J. B.** (1996). Large Scale Renewable Energy Integration: Issues and Solutions. *Energies, 12*(10).

[44] **Rezkalla, M., Pertl, M., & Marinelli, M.** (2018). Electric power system inertia: requirements, challenges and solutions. *Electrical Engineering, 100*, 2677-2693.

[45] **Magdy, G., Mohamed, E. A., Shabib, G., Elbaset, A. A., & Mitani, Y.** (2018). Microgrid dynamic security considering high penetration of renewable energy. *Protection and Control of Modern Power Systems, 3*, 1-11.

[46] **Sarangan, S., Singh, V. K., & Govindarasu, M.** (2018). Cyber Attack-Defense Analysis for Automatic Generation Control with

Renewable Energy Sources. *North American Power Symposium (NAPS).* Fargo, ND, USA.

[47] **Chen, Z., Zhu, J., Li, S., Liu, Y., & Luo, T.** (2022). Detection of False Data Injection Attacks on Load Frequency Control System with Renewable Energy Based on Fuzzy Logic and Neural Networks. *Journal of Modern Power Systems and Clean Energy, 10*(6), 1576-1587.

[48] **Shankar, R., & Kundur, P.** (1994). *Power system stability and control II.* New York: McGraw-Hill Books pp581.

[49] **Bevrani, H.** (2014). *Robust power system frequency control.* New York: Springer.

[50] **Lokay, H. E., & Reps, D. N.** (1958). Distribution System Primary-Feeder Voltage Control I - A New Approach Using the Digital Computer. *Transactions of the American Institute of Electrical Engineers. Part III: Power Apparatus and Systems, 77*(3), 845-855.

[51] **Gönen, T.** (1986). *Electric power distribution system engineering.* New York: McGraw-Hill.

[52] **IEEE** Recommended Practice for Excitation System Models for Power System Stability Studies. (1992). *IEEE Std 421.5*, 1-56.

[53] **Kundur, P., Lee, D. C., Bayne, J., & Dandeno, P. L.** (1985). Impact of Turbine Generator Overspeed Controls on Unit Performance Under System Disturbance Conditions. *IEEE Transactions on Power Apparatus and Systems, PAS-104*(6), 1262-1269.

[54] **IEEE.** (1999). Large frequency disturbances: analysis and modeling needs. *IEEE Power Engineering Society. 1999 Winter Meeting (Cat. No.99CH36233).* New York, NY, USA.

[55] **Kirby, B. J., Dyer, J., Martinez, C., Shoureshi, R. A., Guttromson, R., & Dagle, J.** (2003, December). Frequency control concerns in the North American electric power system. *United States. Department of Energy*, s. 1-18.

[56] **Saadat, H.** (2009). *Power system analysis,(2nd).* McGraw-Hill Higher Education.

[57] **Egido, I., Fernandez-Bernal, F., Rouco, L., Porras, E., & Saiz-Chicharro, A.** (2004, January). Modeling of thermal generating units for automatic generation control purposes. *IEEE Transactions on Control Systems Technology*, s. 205 - 210.

[58] **Gozde, H., & Taplamacioglu, M. C.** (2011, January). Automatic generation control application with craziness based particle swarm optimization in a thermal power system. *International Journal of Electrical Power & Energy Systems*, s. 8-16.

[59] **Mallesham, G., & Akula, R.** (2006). Automatic generation control using fuzzy logic. *Proc. of 8th International Conference on Development and Application Systems.* Suceava, Romania.

[60] **East, S., Butts, J., Papa, M., & Shenoi, S.** (2009). A Taxonomy of Attacks on the DNP3 Protocol. *Critical Infrastructure Protection III: Third Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection.* Hanover, New Hampshire, USA.

[61] **Darwish, I., Igbe, O., Celebi, O., Saadawi, T., & Soryal, J.** (2015). Smart Grid DNP3 Vulnerability Analysis and Experimentation. *2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing.* New York, NY, USA.

[62] **Siddavatam, I. A., & Kazi, F.** (2015). Security assessment framework for cyber physical systems: A case-study of DNP3 protocol. *IEEE Bombay Section Symposium (IBSS).* Mumbai, India.

[63] **Mahmoud, M. S., Hamdan, M. M., & Baroudi, U. A.** (2019). Modeling and control of Cyber-Physical Systems subject to cyber attacks: A survey of recent advances and challenges. *Neurocomputing, 338*, 101-115.

[64] **Sridhar, S., & Manimaran, G.** (2010). Data integrity attacks and their impacts on SCADA control system. *IEEE PES General Meeting.* Minneapolis, MN, USA.

[65] **Cetinkaya, A., Ishii, H., & Hayakawa, T.** (2019). An Overview on Denial-of-Service Attacks in Control Systems: Attack Models and Security Analyses. *Entropy, 21*(2), 210.

[66] **Teixeira, A., Shames, I., Sandberg, H., & Johansson, K. H.** (2015). A secure control framework for resource-limited adversaries. *Automatica, 51*, 135-148.

[67] **Yuancheng, L., Pan, Z., & Longqiang, M.** (2019). Denial of service attack and defense method on load frequency control system. *Journal of the Franklin Institute, 356*(15), 8625-8645.

[68] **Kundur, P.** (1994). *Power System Stability and Control* (s. 400-711). içinde New York, NY, USA: McGraw-Hill.

[69] **Report, I. C.** (1973, November). Dynamic Models for Steam and Hydro Turbines in Power System Studies. *IEEE Transactions on Power Apparatus and Systems, PAS-92*(6), 1904-1915.

[70] **NEPLAN, A. G.** *TURBINE-GOVERNOR MODELS Standard Dynamic Turbine-Governor Systems in NEPLAN Power System Analysis Tool* . https://www.neplan.ch/wp-content/uploads/2015/08/Nep_TURBINES_GOV.pdf adresinden alındı.

[71] **Kundur, P.** (1994). *Power System Stability and Control* (s. 425-711). içinde New York, NY, USA: McGraw-Hill.

[72] **Url-2** *<https://uk.mathworks.com/help/sps/powersys/ref>*, erişim tarihi 20.07.2023.

[73] **Kundur, P.** (1994). *Power System Stability and Control* (s. 813). içinde McGraw-Hill.

[74] **Mei, F.** (2008). Small-signal modelling and analysis of doubly-fed induction generators in wind power applications.

[75] **Li, X., Hui, D., Lai, X., & Yan, T.** (2011). Power Quality Control in Wind/Fuel Cell/Battery/Hydrogen Electrolyzer Hybrid Micro-grid Power System. IntechOpen.

[76] **Michigami, T., & Ishii, T.** (2002). Construction of fluctuation load model and dynamic simulation with LFC control of DC power system and frequency converter interconnection. *IEEE/PES Transmission and Distribution Conference and Exhibition.* Yokohama, Japan.

[77] **Huang, Y.-L., Cárdenas, A. A., Amin, S., Lin, Z.-S., Tsai, H.-Y., & Sastry, S.** (2009). Understanding the physical and economic consequences of attacks on control systems. *International Journal of Critical Infrastructure Protection, 2*(3), 73-83.

[78] **Ameli, A., Hooshyar, A., El-Saadany, E. F., & Youssef, A. M.** (2018). Attack Detection and Identification for Automatic Generation Control Systems. *IEEE Transactions on Power Systems, 33*(5), 4760-4774.

[79] **Wood, A. J., Wollenberg, B. F., & Sheblé, G. B.** (2013). *Power generation, operation, and control* (s. 485-497). içinde New York, NY, USA: Wiley.

[80] **MRO.** (2005). *Under-Frequency Load Shedding (UFLS) Program Midwest Reliability Organization.* Tech. Rep.

[81] **Hemsley, K. E., & Fisher, R. E.** (2018, December 31). *History of industrial control system cyber incidents.* January 21, 2021 tarihinde https://www.osti.gov/servlets/purl/1505628 adresinden alındı.

[82] **Abdallah, A., & Shen, X.** (2018). *Security and Privacy in Smart Grid.* Springer International Publishing.

[83] **Koehrsen, W.** (2018, March). *Beyond Accuracy: Precison and Recall.* https://towardsdatascience.com/beyond-accuracy-precision-and-recall-3da06bea9f6c adresinden alındı.

[84] **Yan, J., Tang, B., & He, H.** (2016). Detection of false data attacks in smart grid with supervised learning. *2016 International Joint Conference on Neural Networks (IJCNN).* Vancouver, BC, Canada.

[85] **Kulkarni, S., & Harman, G.** (2011). *An Elementary Introduction to Statistical Learning Theory.* John Wiley & Sons.

[86] **Sayghe, A., Hu, Y., Zografopoulos, I., Liu, X., Dutta, R. G., Jin, Y., & Konstantinou, C.** (2020, October 6). Survey of machine learning methods for detecting false data injection attacks in power systems. *IET Smart Grid, 3*(5), 581-595.

[87] **Breiman, L., Friedman, J. H., Olshen, R. A., & Stone, C. J.** (1984). *Classification and Regression Trees.* New York: Routledge.

[88] **Hardesty, L.** (2017, April 14). *Explained: Neural networks.* https://news.mit.edu/2017/explained-neural-networks-deep-

learning-0414 adresinden alındı.

[89] **Url-3** <*https://towardsdatascience.com/the-concept-of-artificial-neurons-perceptrons-in-neural-networks-fab22249cbfc*, erişim tarihi 12.05.2023.

[90] **Jha, A. V.** (2021, March 30). Smart grid cyber-physical systems: communication technologies, standards and challenges. *Wireless Networks*, s. 2595-2613.

[91] **Saxena, S., Bhatia, S., & Gupta, R.** (2021, August 4). Cybersecurity Analysis of Load Frequency Control in Power Systems: A Survey. *Designs, 5*(3), 52.

[92] **Sridhar, S., & Govindarasu, M.** (2014, March 2). Model-Based Attack Detection and Mitigation for Automatic Generation Control. *IEEE Transactions on Smart Grid*, s. 580 - 591.

ÖZGEÇMİŞ

Adı-Soyadı **:** Atakan ÖZTÜRK

ÖĞRENİM DURUMU:

- **Lisans** **:** 2019, Fırat Üniversitesi, Mühendislik Fakültesi, Elektrik-Elektronik Mühendisliği Bölümü

MESLEKİ DENEYİM VE ÖDÜLLER:

- 2020 yılı kasım ayından itibaren Afyon Kocatepe Üniversitesi, Elektrik-Elektronik Mühendisliği Bölümünde Araştırma Görevlisi olarak çalışmaktadır.

YÜKSEK LİSANS TEZİNDEN TÜRETİLEN YAYINLAR, SUNUMLAR VE PATENTLER:

- **Ozturk, A.**, Mohammadpourfard, M., and Genc, V. M. I. (2023). Detection of Multiple False Data Injection Attacks on Automatic Generation Control Considering Nonlinearities with Random Forest. International Graduate Research Symposium-IGRS'2023. 2-5 Mayıs İstanbul-Türkiye.