

**T. C.
İSTANBUL GELİŞİM ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ**

Bilgisayar Mühendisliği Anabilim Dalı

**RPL TABANLI IOT AĞLARINDA SALDIRI TESPİTİ VE
SINIFLANDIRILMASI**

Yüksek Lisans Tezi

Ahmet Nail TAŞTAN

Danışman

Dr. Öğr. Üyesi Serkan GÖNEN

Eş Danışman

Dr. Öğr. Üyesi Gökçe KARACAYILMAZ

İstanbul – 2025

TEZ TANITIM FORMU

Yazar Adı Soyadı : Ahmet Nail TAŞTAN

Tezin Dili : Türkçe

Tezin Adı : RPL Tabanlı IoT Ağlarında Saldırı Tespiti ve Sınıflandırılması

Enstitü : İstanbul Gelişim Üniversitesi Lisansüstü Eğitim Enstitüsü

Anabilim Dalı : Bilgisayar Mühendisliği

Tezin Türü : Yüksek Lisans

Tezin Tarihi : 14.07.2025

Sayfa Sayısı : 101

Tez : 1. Dr. Öğr. Üyesi Serkan GÖNEN

Danışmanları : 2. Dr. Öğr. Üyesi Gökçe KARACAYILMAZ

Dizin Terimleri : Nesnelerin İnterneti, RPL Protokolü, Saldırı Tespiti, Saldırı Sınıflandırması, Blackhole Saldırısı, HelloFlood Saldırısı, Version Number Saldırısı, Makine Öğrenmesi, Derin Öğrenme, LSTM, XGBoost, LightGBM, Enerji Tüketimi, Ağ Güvenliği, Cooja Simülatörü, Contiki OS, Wireshark, DODAG, Siber Saldırıları, Simülasyon Ortamları

Türkçe Özet : Bu tez çalışması, düşük güçlü ve kayıplı ağlar için geliştirilen RPL (Routing Protocol for Low-Power and Lossy Networks) protokolü tabanlı Nesnelerin İnterneti (IoT) ağlarında meydana gelen güvenlik açıklarını incelemekte ve bu ağlara yönelik siber saldırıların tespiti ile sınıflandırılmasına yönelik bir çözüm önerisi sunmaktadır. Blackhole, HelloFlood ve Version Number saldırı türleri, Contiki 3.0 işletim sistemi ve Cooja simülatörü kullanılarak modellenmiş, saldırıların ağ yapısı, veri iletimi ve

enerji tüketimi üzerindeki etkileri Powertrace, Wireshark ve Foren6 gibi analiz araçlarıyla çok boyutlu olarak değerlendirilmiştir. Elde edilen sonuçlar, saldırıların DODAG topolojisinde bozulmalara, ağ performansında ciddi düşüslere ve düğüm bazında %30 ile %60 arasında değişen enerji tüketim artışlarına neden olduğunu ortaya koymuştur. Bu bağlamda, saldırı tespiti için BiLSTM, LSTM, XGBoost ve LightGBM gibi makine ve derin öğrenme algoritmaları uygulanmış; BiLSTM modeli %99,02 doğruluk ve %99,83 AUC değeri ile en yüksek performansı sergilerken, XGBoost ise 1,21 saniyelik test süresi ile gerçek zamanlı uygulamalar açısından avantaj sunmuştur. Ancak, bu modellerin yüksek hesaplama karmaşıklığı, IoT cihazlarının sınırlı kaynak yapısı nedeniyle uygulanabilirlik açısından çeşitli kısıtlar doğurmaktadır. Çalışma, mevcut saldırıların etkilerini azaltmak ve tespit mekanizmalarının verimliliğini artırmak amacıyla hafifletilmiş derin öğrenme yaklaşımları, federated learning ve kenar hesaplama gibi yeni nesil yöntemlerin entegrasyonunu önermekte; IoT ağlarının güvenilirliğini artırmaya yönelik çok katmanlı ve ölçeklenebilir güvenlik çerçevelerinin geliştirilmesi gerekliliğini vurgulamaktadır.

Dağıtım Listesi : 1. İstanbul Gelişim Üniversitesi Lisansüstü Eğitim Enstitüsüne
2. YÖK Ulusal Tez Merkezine

İmzası

Ahmet Nail TAŞTAN

T. C.
İSTANBUL GELİŞİM ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

Bilgisayar Mühendisliği Anabilim Dalı

RPL TABANLI IOT AĞLARINDA SALDIRI TESPİTİ VE
SINIFLANDIRILMASI

Yüksek Lisans Tezi

Ahmet Nail TAŞTAN

Danışman

Dr. Öğr. Üyesi Serkan GÖNEN

Eş Danışman

Dr. Öğr. Üyesi Gökçe KARACAYILMAZ

İstanbul – 2025

BEYAN

Bu tezin hazırlanmasında bilimsel ahlak kurallarına uyulduđu, başkalarının eserlerinden yararlanılması durumunda bilimsel normlara uygun olarak atıfta bulunulduđu, kullanılan verilerde herhangi tahrifat yapılmadığını, tezin herhangi bir kısmının bu üniversite veya başka bir üniversitedeki başka bir tez olarak sunulmadığını beyan ederim.

Ahmet Nail TAŞTAN

.../.../2025



İSTANBUL GELİŞİM ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ MÜDÜRLÜĞÜNE

Ahmet Nail TAŞTAN'nın RPL Tabanlı IoT Ağlarında Saldırı Tespiti ve Sınıflandırılması adlı tez çalışması, jürimiz tarafından Bilgisayar Mühendisliği anabilim dalı, Bilgisayar Mühendisliği bilim dalında YÜKSEK LİSANS tezi olarak kabul edilmiştir.

İmza

Başkan

Prof. Dr. Ercan Nurcan YILMAZ

İmza

Üye

Dr. Öğr. Üyesi Serkan GÖNEN

(Danışman)

İmza

Üye

Dr. Öğr. Üyesi Deniz DAHMAN

ONAY

Yukarıdaki imzaların, adı geçen öğretim üyelerine ait olduğunu onaylarım.

... / ... / 2025

İmzası

Prof. Dr. İzzet GÜMÜŞ

Enstitü Müdürü

ÖZET

Bu çalışmada, RPL (Routing Protocol for Low-Power and Lossy Networks) tabanlı Nesnelerin İnterneti (IoT) ağlarında Blackhole, HelloFlood ve Version Number saldırılarının ağ performansı ve enerji tüketimi üzerindeki etkilerini incelemeyi ve bu tehditleri makine öğrenmesi ile derin öğrenme teknikleri kullanarak otomatik olarak tespit etmeyi amaçlamaktadır. Contiki 3.0 işletim sistemi ve Cooja simülatörü kullanılarak oluşturulan 52 düğümlü bir ağ modelinde, belirtilen saldırılar simüle edilmiş ve etkileri çok boyutlu olarak analiz edilmiştir. Powertrace, Wireshark ve Foren6 araçları ile enerji tüketimi, ağ trafiği ve DODAG (Destination Oriented Directed Acyclic Graph) yapısındaki değişiklikler detaylı bir şekilde değerlendirilmiştir. Simülasyon sonuçları, Blackhole saldırısının veri kaybına ve yönlendirme hatalarına, HelloFlood saldırısının ağ trafiği yoğunluğunda %68 artışa ve Version Number saldırısının kontrol mesajı trafiğinde dört kat artışa neden olduğunu ortaya koymuştur. Enerji tüketimi analizleri, bu saldırıların düğüm başına %30-60 oranında enerji artışı yarattığını göstermiştir. Saldırıların tespiti için BiLSTM, LSTM, XGBoost ve LightGBM modelleri karşılaştırmalı olarak test edilmiş; BiLSTM %99,02 doğruluk ve %99,83 AUC ile en yüksek performansı sergilerken, XGBoost 1,21 saniyelik test süresiyle gerçek zamanlı uygulamalarda avantaj sağlamıştır. Ancak, modellerin hesaplama karmaşıklığı, kaynak kısıtlı IoT cihazlarında uygulanabilirliklerini sınırlamaktadır. Çalışma, RPL protokolünün güvenlik açıklarını kapatmak için hafif derin öğrenme modelleri, federated learning ve kenar hesaplama entegrasyonu gibi yenilikçi yaklaşımların araştırılmasını önermektedir. Bulgular, IoT ağlarının güvenilirliğini ve sürdürülebilirliğini artırmak için çok katmanlı güvenlik çerçevelerinin geliştirilmesi gerektiğini vurgulamakta ve bu alanda yapılacak araştırmalara temel oluşturmaktadır.

Anahtar Kelimeler: Nesnelerin İnterneti, RPL Protokolü, Saldırı Tespiti, Saldırı Sınıflandırması, Blackhole Saldırısı, HelloFlood Saldırısı, Version Number Saldırısı, Makine Öğrenmesi, Derin Öğrenme, LSTM, XGBoost, LightGBM, Enerji Tüketimi, Ağ Güvenliği, Cooja Simülatörü, Contiki OS, Wireshark, DODAG, Siber Saldırıları, Simülasyon Ortamları.

SUMMARY

This study investigates the impact of Blackhole, HelloFlood, and Version Number attacks on the performance and energy consumption of Routing Protocol for Low-Power and Lossy Networks (RPL)-based Internet of Things (IoT) networks, aiming to automatically detect these threats using machine learning and deep learning techniques. A 52-node network model was developed using the Contiki 3.0 operating system and the Cooja simulator, where the specified attacks were simulated and their effects analyzed multidimensionally. Tools such as Powertrace, Wireshark, and Foren6 were employed to comprehensively evaluate energy consumption, network traffic, and changes in the Destination Oriented Directed Acyclic Graph (DODAG) structure. Simulation results revealed that Blackhole attacks cause data loss and routing errors, HelloFlood attacks increase network traffic intensity by 68%, and Version Number attacks result in a fourfold increase in control message traffic. Energy consumption analyses indicated that these attacks lead to a 30–60% increase in per-node energy usage. For attack detection, BiLSTM, LSTM, XGBoost, and LightGBM models were comparatively tested; BiLSTM achieved the highest performance with 99.02% accuracy and 99.83% AUC, while XGBoost offered advantages in real-time applications with a test time of 1.21 seconds. However, the computational complexity of these models limits their applicability on resource-constrained IoT devices. The study proposes exploring lightweight deep learning models, federated learning, and edge computing integration to address RPL protocol vulnerabilities. The findings underscore the need for multilayered security frameworks to enhance the reliability and sustainability of IoT networks, providing a foundation for future research in this domain.

Keywords: Internet of Things (IoT), RPL Protocol (Routing Protocol for Low-Power and Lossy Networks), Attack Detection, Attack Classification, Blackhole Attack, HelloFlood Attack, Version Number Attack, Machine Learning, Deep Learning, Long Short-Term Memory (LSTM), XGBoost (Extreme Gradient Boosting), LightGBM (Light Gradient Boosting Machine), Energy Consumption, Network Security, Cooja Simulator, Contiki OS (Operating System), Wireshark, DODAG (Destination-Oriented Directed Acyclic Graph), Cyber Attacks, Simulation Environments.

İÇİNDEKİLER

ÖZET.....	i
SUMMARY	ii
İÇİNDEKİLER	iii
KISALTMALAR	vi
TABLolar LİSTESİ	viii
ŞEKİLLER LİSTESİ.....	ix
ÖNSÖZ.....	x
GİRİŞ	1

BİRİNCİ BÖLÜM LİTERATÜR TARAMASI

1.1. Nesnelerin İnterneti (IoT) ve Ağ Güvenliği.....	3
1.2. RPL Protokolü ve Zafiyetleri	5
1.3. RPL Tabanlı IoT Ağlarında Siber Saldırıları	6
1.3.1. Blackhole Saldırısı.....	7
1.3.2. HelloFlood Saldırısı	7
1.3.3. Version Number Saldırısı	7
1.3.4. Diğer RPL Tabanlı Saldırıları	8
1.3.5. Savunma Mekanizmaları ve Güncel Yaklaşımlar	8
1.3.6. Zorluklar ve Gelecek Yönelimler	9
1.4. IoT Ağlarında Enerji Tüketimi	10
1.4.1. Enerji Tüketiminin Temel Dinamikleri	10
1.4.2. RPL Protokolü ve Enerji Tüketimi	10
1.4.3. Siber Saldırıların Enerji Tüketimine Etkileri	11
1.4.4. Enerji Verimliliği için Savunma Mekanizmaları.....	11
1.4.5. 5G Entegrasyonu ve Yeni Zorluklar	12
1.4.6. Simülasyon ve Analiz Araçları	12
1.4.7. Gelecek Yönelimler	12
1.5. Simülasyon Ortamları ve Analiz Araçları	13
1.5.1. Contiki İşletim Sistemi	14
1.5.2. Cooja Simülatörü	14
1.5.3. Foren6 Analiz Aracı	15
1.5.4. Wireshark Ağ Analiz Aracı	15
1.5.5. Diğer Simülasyon ve Analiz Araçları.....	16
1.5.6. Simülasyon Ortamlarının Güvenlik Araştırmalarındaki Rolü	16
1.5.7. Gelecek Yönelimler	17
1.6. Makine Öğrenmesi ve Derin Öğrenme ile Saldırı Tespiti	18
1.7. Büyük Veri Analizi ve IoT Ağlarında Veri İşleme	20

İKİNCİ BÖLÜM

IOT SİSTEMLERİNDEKİ TEHDİTLER VE ALINAN ÖNLEMLER: GÜNCEL YAKLAŞIMLAR

2.1.	IoT Sistemlerinin Yapısı ve Güvenlik Açıkları	24
2.2.	IoT Sistemlerinde Karşılaşılan Başlıca Tehditler	26
2.2.1.	Fiziksel Tehditler	26
2.2.2.	Ağ Tabanlı Tehditler	27
2.2.2.1.	Blackhole Saldırısı	27
2.2.2.2.	HelloFlood Saldırısı	27
2.2.2.3.	Version Number Saldırısı	27
2.2.2.4.	DDoS (Distributed Denial of Service) Saldırısı	27
2.2.2.5.	Sinkhole Saldırısı	28
2.2.3.	Veri Tabanlı Tehditler	28
2.2.3.1.	Veri Ağı (Eavesdropping)	28
2.2.3.2.	Veri Manipülasyonu	28
2.2.3.3.	Yetkisiz Erişim.....	28
2.2.4.	Yazılım ve Firmware Tehditleri	29
2.2.5.	Sosyal Mühendislik ve Kullanıcı Tabanlı Tehditler	29
2.2.6.	Kritik Altyapılara Yönelik Tehditler	29
2.3.	Güvenlik Önlemleri ve Savunma Mekanizmaları	30
2.3.1.	Fiziksel Katman Güvenlik Önlemleri	30
2.3.1.1.	Donanım Tabanlı Güvenlik Modülleri	30
2.3.1.2.	Fiziksel Erişim Kontrolleri	31
2.3.1.3.	Anti-Tamper Mekanizmaları.....	31
2.3.2.	Ağ Katmanı Güvenlik Önlemleri.....	31
2.3.2.1.	Hafif Şifreleme ve Kimlik Doğrulama.....	31
2.3.2.2.	Güvenli Yönlendirme Mekanizmaları	31
2.3.2.3.	Ağ Tabanlı Anomali Tespiti	32
2.3.2.4.	Ağ İzolasyonu ve Segmentasyonu	32
2.3.3.	Uygulama Katmanı Güvenlik Önlemleri	32
2.3.3.1.	Güçlü Kimlik Doğrulama ve Yetkilendirme.....	32
2.3.3.2.	Veri Şifreleme ve Gizlilik	32
2.3.3.3.	Yazılım ve Firmware Güncellemeleri.....	32
2.3.3.4.	Uygulama Tabanlı Anomali Tespiti.....	33
2.3.4.	Veri Gizliliği ve Mahremiyet Önlemleri	33
2.3.4.1.	Veri Anonimleştirme	33
2.3.4.2.	Blockchain Tabanlı Çözümler	33
2.3.4.3.	Federated Learning.....	33
2.3.5.	Kritik Altyapılar için Özel Önlemler	33
2.3.5.1.	Yedekleme ve Felaket Kurtarma Sistemleri	34
2.3.5.2.	Sızma Testleri ve Güvenlik Denetimleri.....	34

2.3.5.3. Siber-Fiziksel Sistem Entegrasyonu	34
2.3.6. Kullanıcı Farkındalığı ve Eğitim	34
2.3.6.1. Kullanıcı Eğitimi	34
2.3.6.2. Varsayılan Parola Değişikliği	34
2.4. Güncel Yaklaşımlar ve Geleceğe Yönelik Stratejiler	35
2.4.1. Makine Öğrenmesi ve Derin Öğrenme Tabanlı Yaklaşımlar	35
2.4.2. Blockchain Tabanlı Güvenlik Çözümleri	36
2.4.3. Kenar Hesaplama ve Fog Computing.....	36
2.4.4. Federated Learning ve Gizlilik Odaklı Yaklaşımlar	37
2.4.5. 5G Entegrasyonu ve Güvenlik Stratejileri	38
2.4.6. Sıfır-Güven Mimarileri ve Proaktif Güvenlik	38
2.4.7. Standartlaşma ve Yasal Düzenlemeler	39

ÜÇÜNCÜ BÖLÜM

MATERYAL VE METOT

3.1. Kullanılacak Metaryaller.....	40
3.1.1. Ubuntu	40
3.1.2. Contiki	41
3.1.3. Cooja.....	42
3.1.4. Foren6	43
3.1.5. Wireshark.....	44
3.1.6. RPL	45
3.1.7. LightGBM	46
3.1.8. XGBoost	48
3.1.9. LSTM	50
3.1.10. BiLSTM.....	52
3.1.11. HDF5	53
3.2. Kullanılacak Metot	54
3.2.1. Donanım Altyapısı	56
3.2.2. Veri Toplama ve Analiz Araçları.....	56
3.2.3. Blackhole Saldırısı.....	57
3.2.4. HelloFlood Saldırısı	61
3.2.5. Version Number Saldırısı	64
3.3. Analiz ve Bulgular	67
SONUÇLAR VE ÖNERİLER	74
KAYNAKÇA.....	77
ÖZGEÇMİŞ.....	83

KISALTMALAR

5G	:	Beşinci Nesil (Fifth Generation)
AES	:	Gelişmiş Şifreleme Standardı (Advanced Encryption Standard)
BiLSTM	:	Çift Yönlü Uzun Kısa Süreli Bellek (Bidirectional Long Short-Term Memory)
CNN	:	Evrişimli Sinir Ağları (Convolutional Neural Network)
CoAP	:	Kısıtlı Uygulama Protokolü (Constrained Application Protocol)
CPU	:	Merkezi İşlem Birimi (Central Processing Unit)
DAO	:	Hedef Duyuru Nesnesi (Destination Advertisement Object)
DDoS	:	Dağıtık Hizmet Engelleme (Distributed Denial of Service)
DIO	:	DODAG Bilgi Nesnesi (DODAG Information Object)
DIS	:	DODAG Bilgi Talebi (DODAG Information Solicitation)
DODAG	:	Hedef Yönelimli Yönlendirilmiş Döngüsüz Çizge (Destination Oriented Directed Acyclic Graph)
ECC	:	Eliptik Eğri Kriptografisi (Elliptic Curve Cryptography)
GDPR	:	Genel Veri Koruma Tüzüğü (General Data Protection Regulation)
HDF5	:	Hiyerarşik Veri Formatı sürüm 5 (Hierarchical Data Format version 5)
IIoT	:	Endüstriyel Nesnelerin İnterneti (Industrial Internet of Things)
IoT	:	Nesnelerin İnterneti (Internet of Things)
LPL	:	Düşük Güçlü Dinleme (Low-Power Listening)
LPM	:	Düşük Güç Modu (Low Power Mode)
LSTM	:	Uzun Kısa Süreli Bellek (Long Short-Term Memory)
MAC	:	Ortam Erişim Kontrolü (Media Access Control)
MEC	:	Çoklu Erişim Kenar Hesaplama (Multi-access Edge Computing)

MFA	:	Çok Faktörlü Kimlik Doğrulama (Multi-Factor Authentication)
OF	:	Amaç Fonksiyonu (Objective Function)
RPL	:	Düşük Güçlü ve Kayıplı Ağlar için Yönlendirme Protokolü (Routing Protocol for Low-Power and Lossy Networks)
RX	:	Alım (Reception)
SVM	:	Destek Vektör Makineleri (Support Vector Machine)
TPM	:	Güvenilir Platform Modülü (Trusted Platform Module)
TSCH	:	Zaman Aralıklı Kanal Atlama (Time Slotted Channel Hopping)
TX	:	Gönderim (Transmission)
WSN	:	Kablosuz Sensör Ağları (Wireless Sensor Networks)

TABLÖLAR LİSTESİ

Tablo 3.1. Modellerin Performans Karşılaştırması	68
---	----



ŞEKİLLER LİSTESİ

Şekil 3.1. Ubuntu arayüzü.....	41
Şekil 3.2. Cooja arayüz	43
Şekil 3.3. Foren6 arayüz	44
Şekil 3.4. Wireshark arayüz.....	45
Şekil 3.5. RPL şeması	46
Şekil 3.6. LightGBM şeması	48
Şekil 3.7. XGBoost arayüzü	50
Şekil 3.8. LSTM şeması.....	51
Şekil 3.9. BİLSTM şeması	53
Şekil 3.10. Saldırı ve Tesip Modelinin Akış Diyagramı	56
Şekil 3.11. Blackhole saldırı ağ istatistikleri.....	58
Şekil 3.12. Blackhole saldırı sonrası	59
Şekil 3.13. Blackhole saldırı öncesi	60
Şekil 3.14. Blackhole saldırısı ve referans model	61
Şekil 3.15. HelloFlood saldırı öncesi	62
Şekil 3.16. HelloFlood saldırı sonrası	62
Şekil 3.17. HelloFlood saldırısı ve referans model	63
Şekil 3.18. Version number saldırı öncesi	65
Şekil 3.19. Version number saldırı başlangıcı.....	65
Şekil 3.20. Version number saldırı sonrası	65
Şekil 3.21. Version number saldırısı ve referans model	66
Şekil 3.22. BİLSTM karmaşıklık matrisi	70
Şekil 3.23. XGBoost karmaşıklık matrisi.....	71
Şekil 3.24. LightGBM Karmaşıklık matrisi	72
Şekil 3.25. LSTM karmaşıklık matrisi.....	73

ÖNSÖZ

Bu tez çalışması, yalnızca bireysel bir çabanın ürünü değil; aynı zamanda yolculuğum boyunca yanımda olan kıymetli insanların katkılarıyla şekillenmiş bir emeğin yansımasıdır.

Lisansüstü eğitimim süresince bilgi birikimleriyle bana yön gösteren, desteğini hiçbir zaman esirgemeyen değerli danışmanlarım Dr. Öğr. Üyesi Serkan GÖNEN ve Dr. Öğr. Üyesi Gökçe KARACAYILMAZ hocalarıma en içten teşekkürlerimi sunarım. Onların akademik rehberliği, bu çalışmanın her aşamasında bana ilham kaynağı olmuştur.

Ders döneminden tez sürecine kadar geçen zamanda bilgi ve tecrübelerini benimle paylaşan tüm hocalarıma ve İstanbul Gelişim Üniversitesi Bilgisayar Mühendisliği Bölümü'nün değerli akademik kadrosuna katkılarından dolayı teşekkür ederim.

Tez sürecinin yürütülmesinde bana teknik bilgi ve moral desteğini esirgemeyen değerli meslektaşlarıma ve arkadaşlarıma gönülden teşekkür ederim.

Hayatım boyunca her adımında yanımda olan, sevgileri ve inançlarıyla bana güç veren canım aileme, başta annem, babam ve kıymetli kardeşlerime minnettarlığımı bir borç bilirim.

Bu çalışmanın oluşmasında katkısı bulunan herkese en içten şükranlarımı sunarım.

GİRİŞ

Nesnelerin İnterneti (IoT), fiziksel cihazların sensörler, yazılım ve diğer teknolojilerle donatılarak internet üzerinden birbiriyle iletişim kurmasını ve veri alışverişi yapmasını sağlayan yenilikçi bir ağ yapısı olarak tanımlanmaktadır. Günümüzde IoT, akıllı ev sistemlerinden sağlık hizmetlerine, endüstriyel otomasyondan akıllı şehir uygulamalarına kadar geniş bir yelpazede kullanılmakta ve bu alanlarda verimliliği artırmakta, yaşam kalitesini iyileştirmektedir. Cisco'nun tahminlerine göre, 2023 itibarıyla dünya genelinde 30 milyardan fazla IoT cihazının aktif olduğu belirtilmektedir. Ancak, bu hızlı büyüme ve yaygınlaşma, IoT ağlarının güvenlik açıklarına karşı daha duyarlı hale gelmesine neden olmaktadır. Özellikle dağıtık yapıları, sınırlı kaynaklara sahip cihazları ve kablosuz iletişim kullanımı, bu ağları çeşitli siber saldırılara karşı savunmasız kılmaktadır.

IoT ağlarında veri iletiminin etkin bir şekilde gerçekleştirilmesi için tasarlanmış olan Yönlendirme Protokolü for Low-Power and Lossy Networks (RPL), düşük güç tüketimi ve kayıplı ağlar için optimize edilmiş bir protokol olarak öne çıkmaktadır. RPL, ağ topolojisini Destination Oriented Directed Acyclic Graph (DODAG) yapısı ile düzenlemekte ve enerji tasarrufu sağlayarak veri yönlendirmesini kolaylaştırmaktadır. Bu özellikleriyle RPL, IoT cihazlarının sınırlı işlem kapasitesi ve enerji kaynaklarına uyum sağlamakta; ancak, aynı zamanda belirli güvenlik zayıflıklarına da sahip olmaktadır. Özellikle, RPL'nin yönlendirme mekanizmalarını hedef alan Blackhole, HelloFlood ve Version Number gibi saldırılar, ağın işlevselliğini ve güvenilirliğini ciddi şekilde tehdit etmektedir.

Blackhole saldırısı, kötü niyetli bir düğümün kendini en iyi yönlendirme yolu olarak tanıtmaması ve ardından gelen veri paketlerini düşürmesi şeklinde gerçekleşmektedir. Bu durum, ağda veri kaybına ve iletişim kopukluklarına yol açmaktadır. HelloFlood saldırısı ise, saldırganın yüksek güçlü "hello" mesajları yayarak diğer düğümleri komşu olduğuna inandırması ve ağ topolojisini bozması ile karakterize edilmektedir. Version Number saldırısı, RPL mesajlarındaki sürüm numarasının manipüle edilmesiyle DODAG yapısında tutarsızlıklar yaratmakta ve yönlendirme süreçlerini aksatmaktadır. Bu tür saldırılar, IoT ağlarının güvenilirliğini

ve performansını olumsuz yönde etkilemekte; dolayısıyla, bu tehditlerin tespiti ve önlenmesi büyük bir önem taşımaktadır.

Bu çalışma, RPL tabanlı IoT ağlarında Blackhole, HelloFlood ve Version Number saldırılarının ağın yönlendirme yapısı ve enerji tüketimi üzerindeki etkilerini detaylı bir şekilde incelemeyi amaçlamaktadır. Araştırma kapsamında, Contiki 3.0 işletim sistemi ve Cooja simülatörü kullanılarak gerçekçi bir IoT ağı modeli oluşturulmakta ve bu saldırılar simüle edilmektedir. Simülasyonlar, saldırıların ağ üzerindeki etkilerini hem yapısal hem de performans açısından değerlendirme imkanı sunmaktadır. Ayrıca, ağ trafiği verilerinden yararlanılarak makine öğrenmesi ve derin öğrenme teknikleri ile bu saldırıların otomatik tespiti gerçekleştirilmektedir. Çalışmada, Powertrace ile enerji tüketimi analizi, Wireshark ile ağ trafiği izleme ve Foren6 ile RPL DODAG yapısının görselleştirilmesi gibi araçlar kullanılmaktadır.

Bu tez, RPL protokolünün güvenlik açıklarını ortaya koymayı ve bu açıkların IoT ağları üzerindeki etkilerini analiz etmeyi hedeflemektedir. Aynı zamanda, makine öğrenmesi tabanlı tespit yöntemleriyle IoT ağlarının güvenliğini artırmaya yönelik yenilikçi çözümler sunmaktadır. Tezin yapısı, giriş bölümünü takiben literatür taraması, metodoloji, bulgular ve analiz, ve sonuç bölümlerinden oluşmaktadır. Bu çalışma, IoT ağlarının gelecekteki gelişiminde güvenlik odaklı yaklaşımların önemini vurgulamakta ve bu alanda yapılacak araştırmalara katkı sağlamayı amaçlamaktadır.

BİRİNCİ BÖLÜM

LİTERATÜR TARAMASI

1.1. Nesnelerin İnterneti (IoT) ve Ağ Güvenliği

Nesnelerin İnterneti (IoT), fiziksel cihazların sensörler, yazılımlar ve iletişim teknolojileriyle donatılarak internet üzerinden birbirleriyle veri alışverişi yapmasını sağlayan bir ağ yapısı olarak tanımlanmaktadır (Atzori, L., Iera, A., Morabito, G. 2010). Bu kavram, 1999 yılında Kevin Ashton tarafından RFID teknolojisi bağlamında ortaya atılmış ve 2000'li yıllarda kablosuz sensör ağlarının (WSN) gelişimiyle yaygınlaşmaya başlamıştır (Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M. 2013). Ancak, erken dönemde IoT sistemleri, sınırlı işlem kapasitesi ve düşük bant genişliği nedeniyle güvenlik önlemlerine yeterince odaklanamamıştır (Sicari, S., Rizzardi, A., Grieco, L. A., Coen-Porisini, A. 2015). 2010'lu yıllarda IoT cihazlarının sayısındaki hızlı artış, güvenlik açıklarını kritik bir sorun haline getirmiştir (Mosenia ve Jha, 2017). Örneğin, 2016 yılında gerçekleşen Mirai botnet saldırısı, milyonlarca IoT cihazının kötü amaçlı yazılımlarla ele geçirilebileceğini ortaya koymuş ve güvenlik araştırmalarını hızlandırmıştır (Kolias, C., Kambourakis, G., Stavrou, A., Voas, J. 2017).

IoT ağlarının heterojen yapısı, farklı cihaz türlerinin ve iletişim protokollerinin bir arada bulunması, güvenlik yönetimini karmaşıklştırmaktadır (Khan ve Salah, 2018). Kaynak kısıtlı cihazlar, genellikle hafif işlemciler ve sınırlı enerji kapasitelerine sahip olduğundan, geleneksel güvenlik mekanizmalarının uygulanması zorlaşmaktadır. Bu bağlamda, hafif şifreleme algoritmaları üzerine yapılan çalışmalar önem kazanmıştır. Örneğin, AES (Advanced Encryption Standard) tabanlı hafif şifreleme yöntemleri, enerji verimliliği ile güvenliği dengelemek amacıyla önerilmiştir (Hossain, M. M., Fotouhi, M., Hasan, R. 2018). Ayrıca, blockchain tabanlı merkeziyetsiz güvenlik çözümleri, IoT cihazları arasında güvenilir veri paylaşımı için yenilikçi bir yaklaşım sunmaktadır.

IoT ağlarında siber tehditlerin tespiti ve önlenmesi için makine öğrenmesi tabanlı yöntemler giderek yaygınlaşmaktadır. Özellikle, anomali tespit sistemleri, ağ trafiğindeki anormal davranışları izlemek ve DDoS (Distributed Denial of Service) gibi tehditleri belirlemek için geliştirilmiştir. Örneğin, karar ağaçları ve destek vektör

makinelere (SVM) gibi geleneksel algoritmalar, erken dönemde IoT ağlarında kullanılmış; ancak, bu yöntemlerin karmaşık tehditleri tespit etme kapasitesi sınırlı kalmıştır. 2015 yılından itibaren derin öğrenme modelleri, özellikle LSTM (Long Short-Term Memory) ve CNN (Convolutional Neural Network) tabanlı yaklaşımlar, zamansal ve uzamsal veri örüntülerini modellemede yüksek doğruluk sağlamıştır. Bu modeller, sıfır-gün tehditlerine karşı gerçek zamanlı koruma sunma potansiyeline sahiptir.

5G teknolojinin IoT ekosistemine entegrasyonu, yüksek veri hızları ve düşük gecikme süreleri sunarak IoT uygulamalarının kapsamını genişletmiştir (Li, S., Da Xu, L., Zhao, S. 2018). Ancak, bu entegrasyon, yeni güvenlik zorluklarını da beraberinde getirmiştir. 5G ağlarının karmaşık mimarisi, özellikle ağ dilimleme (network slicing) ve çoklu erişim kenar hesaplama (MEC) gibi teknolojiler, yeni saldırı vektörleri oluşturmaktadır. Bu nedenle, IoT güvenliği için çok katmanlı bir yaklaşım benimsenmesi gerektiği vurgulanmaktadır. Örneğin, fiziksel katman güvenliği, ağ katmanı protokol optimizasyonları ve uygulama katmanı veri gizliliği gibi unsurlar bir arada ele alınmalıdır.

IoT güvenliği, yalnızca teknik çözümlerle sınırlı kalmamakta; aynı zamanda veri gizliliği ve kullanıcı mahremiyeti gibi etik boyutları da içermektedir. Avrupa Birliği'nin Genel Veri Koruma Tüzüğü (GDPR) gibi düzenlemeler, IoT cihazlarından toplanan verilerin işlenmesi ve saklanması süreçlerinde sıkı kurallar getirmiştir (Ziegeldorf, J. H., Morchon, O. G., Wehrle, K. 2014). Bu düzenlemeler, IoT sistemlerinin tasarımında güvenlik ve gizlilik odaklı yaklaşımların önceliklendirilmesini zorunlu kılmaktadır. Ayrıca, IoT ağlarının kritik altyapılarda (örneğin, sağlık, enerji, ulaşım) kullanımı, bu sistemlerin süreklilik ve güvenilirlik açısından yüksek standartlara uymasını gerektirmektedir.

Sonuç olarak, IoT ağlarının güvenliği, hem akademik hem de endüstriyel araştırmalarda öncelikli bir konu olarak öne çıkmaktadır. Hafif şifreleme, makine öğrenmesi tabanlı tehdit tespiti, blockchain teknolojileri ve 5G entegrasyonu gibi yenilikçi yaklaşımlar, IoT ekosisteminin güvenilirliğini artırmayı hedeflemektedir. Ancak, heterojen cihaz yapıları, kaynak kısıtlamaları ve yeni nesil tehditler, bu alanda çok disiplinli ve kapsamlı çözümler geliştirilmesini zorunlu kılmaktadır.

1.2. RPL Protokolü ve Zafiyetleri

RPL (Routing Protocol for Low-Power and Lossy Networks), Nesnelerin İnterneti (IoT) ağlarında düşük güç tüketimi ve kayıplı ağlar için optimize edilmiş, IPv6 tabanlı bir yönlendirme protokolü olarak 2012 yılında IETF ROLL çalışma grubu tarafından standardize edilmiştir (Kim, H. S., Ko, J., Culler, D. E., Paek, J. 2017). RPL, Destination Oriented Directed Acyclic Graph (DODAG) yapısını kullanarak ağ topolojisini düzenlemekte ve enerji tasarrufu sağlayarak veri yönlendirmesini kolaylaştırmaktadır (Vasseur, J.-P., Kim, M., Pister, K., Dejean, N., Barthel, D. 2011). Bu özellikleriyle, kaynak kısıtlı IoT cihazlarının sınırlı işlem kapasitesi ve enerji kaynaklarına uyum sağlamakta; ancak, tasarımındaki bazı zayıflıklar güvenlik açıklarına yol açmaktadır .

RPL'nin temel mekanizması, Objective Function (OF) adı verilen yönlendirme metriklerine dayanmaktadır (Thubert, 2012). OF, düğümlerin ebeveyn seçimini ve yönlendirme kararlarını optimize etmek için kullanılmaktadır (Gaddour ve Koubâa, 2012). Erken dönemde yapılan çalışmalar, OF mekanizmalarının enerji verimliliği ve ağ performansını artırmak için uyarlanabilir hale getirilmesine odaklanmıştır (Lamaazi ve Benamar, 2018). Örneğin, fuzzy logic tabanlı OF tasarımları, ağ koşullarına göre dinamik yönlendirme kararları alarak performansı iyileştirmiştir (Gaddour ve Koubâa, 2012). Bununla birlikte, RPL'nin yönlendirme mekanizmalarındaki esneklik, Blackhole, HelloFlood ve Version Number gibi saldırılar karşısında ciddi güvenlik açıkları oluşturmaktadır (Raoof, A., Matrawy, A., Lung, C.-H. 2018).

Blackhole saldırısı, kötü niyetli bir düğümün sahte rank değerleri ile kendini en iyi yönlendirme yolu olarak tanıtmaya ve ardından veri paketlerini düşürmesiyle gerçekleşmektedir (Sehrawat, A., Gill, N. S., Singh, M. 2019). Bu saldırı, ağda veri kaybına ve iletişim kopukluklarına neden olmaktadır (Sehrawat vd., 2019). HelloFlood saldırısı, saldırganın yüksek güçlü “hello” mesajları yayarak diğer düğümleri komşu olduğuna inandırması ve ağ topolojisini bozmasıyla karakterize edilmektedir (Mayzaud, A., Badonnel, R., Chrisment, I. 2016). Bu durum, düğümlerin enerji tüketimini artırarak ağın sürdürülebilirliğini tehdit etmektedir (Mayzaud vd., 2016). Version Number saldırısı ise, RPL mesajlarındaki sürüm numarasının manipüle edilmesiyle DODAG yapısında tutarsızlıklar yaratmakta ve yönlendirme süreçlerini aksatmaktadır (Raza, S., Wallgren, L., Voigt, T. 2013).

RPL tabanlı ağların güvenliğini artırmak için çeşitli savunma mekanizmaları önerilmiştir. Örneğin, güvenli ebeveyn seçimi algoritmaları, düğümlerin sahte rank değerlerine karşı korunmasını sağlamaktadır (Djedjig, N., Tandjaoui, D., Romdhani, I., Medjek, F. 2017). Kriptografik doğrulama yöntemleri, RPL kontrol mesajlarının (DIO, DAO) bütünlüğünü korumak için kullanılmaktadır (Djedjig vd., 2017). Ayrıca, makine öğrenmesi tabanlı anomali tespit sistemleri, RPL ağlarında anormal davranışları izlemek için geliştirilmiştir (Verma ve Ranga, 2020). Özellikle, XGBoost ve LSTM gibi modeller, ağ trafiğindeki örüntüleri analiz ederek Blackhole ve HelloFlood gibi saldırıları yüksek doğrulukla tespit etmiştir (Verma ve Ranga, 2020). Ancak, bu modellerin hesaplama karmaşıklığı, kaynak kısıtlı IoT cihazlarında uygulanabilirliklerini sınırlamaktadır (Verma ve Ranga, 2020).

Son yıllarda, RPL güvenliği üzerine yapılan çalışmalar, protokolün enerji verimliliği ile güvenlik arasında denge kurma gereksinimlerine odaklanmıştır (Rey, V., Sánchez, P. M. S., Celdrán, A. H., Bovet, G. 2022). Örneğin, hafif kimlik doğrulama protokolleri ve sıkıştırılmış kontrol mesajları, enerji tüketimini artıran güvenlik mekanizmalarının etkisini azaltmayı amaçlamaktadır (Djedjig vd., 2017). Ayrıca, federated learning gibi yenilikçi yaklaşımlar, IoT cihazlarının yerel veri işleme kapasitesini kullanarak merkezi olmayan saldırı tespit sistemleri geliştirmek için önerilmiştir (Rey vd., 2022). Bununla birlikte, RPL'nin zafiyetlerinin çok boyutlu analizi ve gerçek zamanlı savunma mekanizmalarının optimizasyonu, IoT ağlarının güvenilirliği ve sürdürülebilirliği açısından kritik bir araştırma alanı olarak öne çıkmaktadır (Raoof, A., Matrawy, A., Lung, C.-H. 2018)

1.3. RPL Tabanlı IoT Ağlarında Siber Saldırıları

RPL (Routing Protocol for Low-Power and Lossy Networks) tabanlı Nesnelerin İnterneti (IoT) ağlarına yönelik siber saldırılar, kablosuz sensör ağlarının 2000'li yıllarda yaygınlaşmasıyla dikkat çekmeye başlamıştır. Erken dönemde, genel DoS (Denial of Service) saldırıları ön plandayken, 2012 yılında RPL protokolünün IETF tarafından standardize edilmesiyle, protokolün yönlendirme mekanizmalarını hedef alan Blackhole, HelloFlood ve Version Number gibi spesifik saldırılar önem kazanmıştır. Bu saldırılar, RPL'nin Destination Oriented Directed Acyclic Graph (DODAG) yapısını doğrudan manipüle ederek ağın işlevselliğini, güvenilirliğini ve enerji verimliliğini tehdit etmektedir.

1.3.1.Blackhole Saldırısı

Blackhole saldırısı, kötü niyetli bir düğümün sahte rank değerleri ile kendini en iyi yönlendirme yolu olarak tanıtmayı ve ardından gelen veri paketlerini düşürmesiyle gerçekleşmektedir. Bu saldırı, ağda veri kaybına, iletişim kopukluklarına ve yönlendirme hatalarına yol açmaktadır. Yapılan çalışmalar, Blackhole saldırısının RPL ağlarında veri iletim başarı oranını %50'ye kadar düşürebildiğini ve enerji tüketimini artırdığını ortaya koymuştur (Raoof vd., 2018). Örneğin, saldırgan düğüm, DIO (DODAG Information Object) mesajlarını manipüle ederek komşu düğümleri kendisine yönlendirmekte ve bu süreçte ağın topolojik bütünlüğünü bozmaktadır. Savunma mekanizmaları olarak, istatistiksel anomali tespiti ve güvenli ebeveyn seçimi algoritmaları önerilmiştir. Özellikle, makine öğrenmesi tabanlı yaklaşımlar, ağ trafiğindeki anormal rank değişikliklerini tespit ederek bu saldırıya karşı yüksek doğruluk sunmaktadır (Saadeh, M., Sleit, A., Sabri, K. E., Almobaideen, W. 2018).

1.3.2.HelloFlood Saldırısı

HelloFlood saldırısı, saldırganın yüksek güçlü “hello” mesajları (DIS - DODAG Information Solicitation) yayarak diğer düğümleri komşu olduğuna inandırması ve ağın yönlendirme yapısını bozmasıyla karakterize edilmektedir. Bu saldırı, düğümlerin radyo modüllerinde (TX ve RX) aşırı yük yaratarak enerji tüketimini artırmakta ve ağın sürdürülebilirliğini tehdit etmektedir. Wallgren ve diğerleri (2013), HelloFlood saldırısının RPL ağlarında kontrol mesajı trafiğini %60'a kadar artırabileceğini ve düğümlerin pil ömrünü önemli ölçüde kısalttığını rapor etmiştir (Raza, S., Wallgren, L., Voigt, T. 2013). Savunma yöntemleri arasında, mesaj frekansı analizi ve kimlik doğrulama tabanlı filtreleme mekanizmaları öne çıkmaktadır. Ayrıca, derin öğrenme modelleri, özellikle BiLSTM (Bidirectional Long Short-Term Memory), bu tür saldırıların zamansal örüntülerini analiz ederek gerçek zamanlı tespit imkânı sağlamaktadır (Wang, Z., Chen, H., Yang, S., Luo, X., Li, D., Wang, J. 2023).

1.3.3.Version Number Saldırısı

Version Number saldırısı, RPL protokolünün DODAG sürüm numarasını manipüle ederek ağın sürekli yeniden yapılandırılmasını tetikleyen bir saldırı türüdür. Saldırgan düğüm, sahte DIO mesajlarıyla sürüm numarasını artırarak ağda “Global Repair” süreçlerini başlatmakta ve bu durum, yönlendirme tablolarının

kararsızlaşmasına neden olmaktadır. Mayzaud ve diğerleri (2016), bu saldırının ağdaki kontrol mesajı trafiğini dört katına çıkarabileceğini ve enerji tüketimini %30-35 oranında artırabileceğini belirtmiştir (Goswami ve Ghoshal, 2016). Savunma stratejileri, sürüm numarası doğrulama mekanizmalarına ve anomali tespit sistemlerine dayanmaktadır. Örneğin, XGBoost tabanlı modeller, sahte sürüm numaralarının neden olduğu anormal trafik davranışlarını yüksek doğrulukla tespit etmiştir.

1.3.4. Diğer RPL Tabanlı Saldırıları

RPL ağlarını hedef alan diğer önemli saldırılar arasında Selective Forwarding, Sinkhole ve Sybil saldırıları yer almaktadır. Selective Forwarding saldırısında, kötü niyetli düğüm belirli veri paketlerini seçici olarak düşürmekte ve ağın veri bütünlüğünü bozmaktadır. Sinkhole saldırısı, saldırganın sahte bir kök düğüm gibi davranarak ağ trafiğini kendisine yönlendirmesiyle gerçekleşmekte ve genellikle Blackhole saldırısıyla birleştirilerek daha yıkıcı etkiler yaratmaktadır. Sybil saldırısı ise, tek bir düğümün birden fazla kimlik kullanarak ağın yönlendirme kararlarını manipüle etmesiyle ortaya çıkmaktadır. Bu tür saldırılar, RPL'nin düşük güçlü yapısı nedeniyle özellikle etkili olmakta ve ağın güvenilirliğini ciddi şekilde tehdit etmektedir.

1.3.5. Savunma Mekanizmaları ve Güncel Yaklaşımlar

RPL tabanlı IoT ağlarında siber tehditlere karşı geliştirilen savunma mekanizmaları, hem protokol tasarımı hem de ek güvenlik katmanları üzerine odaklanmaktadır. Hafif kriptografik yöntemler, RPL kontrol mesajlarının (DIO, DAO) bütünlüğünü korumak için önerilmiştir (Krzywiecki, Ł., Bobowski, A., Słowik, M., Słowik, M., Koziel, P. 2020). Örneğin, SVELTE sistemi, kaynak kısıtlı cihazlarda gerçek zamanlı tehdit tespiti sağlamak amacıyla hafif bir saldırı tespit çerçevesi sunmaktadır. Ayrıca, makine öğrenmesi ve derin öğrenme tabanlı çözümler, ağ trafiğindeki anormal davranışları modellemek için yaygın olarak kullanılmaktadır. BiLSTM ve XGBoost gibi modeller, RPL tabanlı ağlarda Blackhole, HelloFlood ve Version Number saldırılarını tespit etmede %98'in üzerinde doğruluk sağlamıştır (Buczak ve Guven, 2016).

Son yıllarda, federated learning gibi yenilikçi yaklaşımlar, IoT cihazlarının yerel veri işleme kapasitesini kullanarak merkezi olmayan saldırı tespit sistemleri geliştirmek için araştırılmaktadır. Bu yöntem, veri gizliliğini korurken, ağ genelinde işbirlikçi bir güvenlik modeli sunmaktadır. Ayrıca, 5G entegrasyonu ile birlikte, RPL ağlarının karmaşıklıklaştıran yapısına uygun ölçeklenebilir güvenlik çözümleri geliştirilmesi gerektiği vurgulanmaktadır (Pu ve Lim, 2020). Örneğin, ağ dilimleme teknolojisi, RPL tabanlı IoT ağlarında trafik izolasyonu sağlayarak saldırıların yayılmasını sınırlamaktadır.

1.3.6. Zorluklar ve Gelecek Yönelimler

RPL tabanlı IoT ağlarında siber güvenlik, kaynak kısıtlamaları, heterojen cihaz yapıları ve gerçek zamanlı işlem gereksinimleri nedeniyle karmaşık bir alandır. Makine öğrenmesi modellerinin hesaplama karmaşıklığı, düşük güçlü IoT cihazlarında uygulanabilirliklerini sınırlamaktadır. Ayrıca, sınıf dengesizliği ve sıfır-gün tehditleri, mevcut tespit sistemlerinin etkinliğini zorlaştırmaktadır (Bostani ve Sheikhan, 2017). Gelecekteki araştırmalar, enerji verimli ve ölçeklenebilir savunma mekanizmalarına odaklanmaktadır. Örneğin, hafif derin öğrenme modelleri ve kenar hesaplama (edge computing) entegrasyonu, IoT ağlarının güvenliğini artırmak için umut vadetmektedir (Canedo ve Skjellum, 2016). Bunun yanı sıra, RPL protokolünün tasarımsal zayıflıklarını ele alan yeni nesil yönlendirme protokolleri geliştirilmesi gerektiği belirtilmektedir (Shafique, K., Khawaja, B. A., Sabir, F., Qazi, S., Mustaqim, M. 2020).

Sonuç olarak, RPL tabanlı IoT ağlarına yönelik siber saldırılar, ağın performansını, güvenilirliğini ve sürdürülebilirliğini doğrudan tehdit etmektedir. Blackhole, HelloFlood ve Version Number gibi saldırılar, protokolün yönlendirme mekanizmalarındaki zafiyetleri hedef almakta ve çok boyutlu etkiler yaratmaktadır. Makine öğrenmesi, derin öğrenme ve federated learning gibi yenilikçi yaklaşımlar, bu tehditlere karşı etkili çözümler sunmakta; ancak, enerji verimliliği ve gerçek zamanlı uygulanabilirlik gibi zorluklar, bu alanda daha fazla araştırma gerektirmektedir (Mendez Mena, D., Papapanagiotou, I., Yang, B. 2018).

1.4. IoT Ağlarında Enerji Tüketimi

Nesnelerin İnterneti (IoT) ağlarında enerji tüketimi, kablosuz sensör ağlarının (WSN) 1990'lı yıllarda ortaya çıkışıyla birlikte kritik bir araştırma alanı haline gelmiştir. IoT cihazlarının genellikle sınırlı pil kapasitelerine sahip olması, bu cihazların enerji verimliliğini ağ tasarımının temel bir önceliği yapmaktadır (Anastasi, G., Conti, M., Di Francesco, M., Passarella, A. 2009). Erken dönemde, enerji optimizasyonu çalışmaları, düşük güçlü mikrodenetleyiciler ve donanım odaklı çözümler üzerine yoğunlaşmıştır; ancak, ağ protokollerinin sınırlı kapasitesi, kapsamlı çözümlerin geliştirilmesini zorlaştırmıştır. 2000'li yıllarda, enerji verimliliğini artırmak için MAC (Media Access Control) katmanı protokolleri ve yönlendirme algoritmaları üzerine yapılan çalışmalar hız kazanmıştır (Rault, T., Bouabdallah, A., Challal, Y. 2014). Bu bağlamda, IoT ağlarının sürdürülebilirliği ve operasyonel ömrü, enerji tüketiminin etkin yönetimine bağlıdır.

1.4.1. Enerji Tüketiminin Temel Dinamikleri

IoT cihazlarının enerji tüketimi, işlemci kullanımı (CPU), düşük güç modu (LPM), radyo gönderimi (TX) ve radyo alımı (RX) gibi bileşenlerden oluşmaktadır. Özellikle, radyo modülleri, veri iletimi ve alımı sırasında en yüksek enerji tüketimini oluşturmaktadır. Dunkels ve diğerleri (2008), düşük güçlü dinleme (Low-Power Listening, LPL) tekniklerinin, cihazların radyo modüllerini yalnızca gerekli durumlarda aktif hale getirerek enerji tüketimini %50'ye kadar azaltabileceğini göstermiştir. Bununla birlikte, IoT ağlarının heterojen yapısı ve kablosuz iletişim ortamlarının kayıplı doğası, enerji optimizasyonunu karmaşık bir sorun haline getirmektedir (Demirkol, I., Ersoy, C., Alagoz, F. 2006). Örneğin, çok atlamalı (multi-hop) yönlendirme, veri iletim mesafesini azaltarak enerji tasarrufu sağlasa da, yönlendirme kararlarının sık değişmesi enerji tüketimini artırabilmektedir.

1.4.2. RPL Protokolü ve Enerji Tüketimi

RPL (Routing Protocol for Low-Power and Lossy Networks), düşük güç tüketimi ve kayıplı ağlar için tasarlanmış bir yönlendirme protokolü olarak IoT ağlarında yaygın şekilde kullanılmaktadır. RPL, Destination Oriented Directed Acyclic Graph (DODAG) yapısı ile enerji tasarrufu sağlamak ve Objective Function (OF) mekanizmaları aracılığıyla yönlendirme kararlarını optimize etmektedir.

Gaddour ve Koubâa (2012), RPL'nin enerji farkındalığı tabanlı OF tasarımlarının, ağın ortalama enerji tüketimini %20-30 oranında azalttığını rapor etmiştir. Ancak, RPL'nin yönlendirme mekanizmalarını hedef alan siber saldırılar, enerji tüketimini ciddi şekilde artırmaktadır. Örneğin, Blackhole ve HelloFlood saldırıları, düğümlerin radyo modüllerinde aşırı yük yaratarak enerji tüketimini %60'a kadar artırabilmektedir (Ammar, M., Russello, G., Crispo, B. 2018).

1.4.3. Siber Saldırıların Enerji Tüketimine Etkileri

RPL tabanlı IoT ağlarında Blackhole, HelloFlood ve Version Number gibi siber saldırılar, enerji tüketimini doğrudan etkileyen önemli tehditlerdir. Blackhole saldırısı, kötü niyetli düğümün sahte rank değerleriyle veri paketlerini düşürmesiyle, komşu düğümlerin sürekli yönlendirme güncellemeleri yapmasına neden olmakta ve bu durum CPU ve RX modüllerinde enerji tüketimini artırmaktadır. HelloFlood saldırısı, saldırganın yüksek frekansta DIS mesajları yayarak düğümleri sürekli alıcı modda tutmasıyla enerji tüketimini artırmaktadır. Wallgren ve diğerleri (2013), bu saldırının ağ genelinde enerji tüketimini %40 oranında artırabileceğini belirtmiştir. Version Number saldırısı ise, sahte sürüm numaralarıyla DODAG yapısının sürekli yeniden yapılandırılmasını tetikleyerek kontrol mesajı trafiğini ve enerji tüketimini artırmaktadır. Bu etkiler, Powertrace gibi araçlarla milisaniye çözünürlüğünde analiz edilerek, saldırıların enerji tüketimi üzerindeki yıkıcı etkileri detaylı şekilde ortaya konmuştur (Ahmed ve Ko, 2016).

1.4.4. Enerji Verimliliği için Savunma Mekanizmaları

IoT ağlarında enerji tüketimini azaltmak ve siber saldırıların etkilerini hafifletmek için çeşitli savunma mekanizmaları geliştirilmiştir. Hafif kriptografik yöntemler, güvenlik sağlarken enerji tüketimini minimumda tutmayı amaçlamaktadır. Örneğin, SVELTE sistemi, RPL tabanlı ağlarda anomali tespiti yaparak enerji verimli bir tehdit savunma çerçevesi sunmaktadır. Ayrıca, makine öğrenmesi tabanlı enerji anomali tespit sistemleri, ağ trafiğindeki anormal davranışları izleyerek saldırıların enerji tüketimi üzerindeki etkilerini gerçek zamanlı olarak belirlemektedir. XGBoost ve LightGBM gibi modeller, düşük hesaplama maliyetiyle enerji verimli tespit imkânı sağlamaktadır (Bhadauria ve Sanyal, 2012). Bunun yanı sıra, sıkıştırılmış kontrol

mesajları ve enerji farkındalığı tabanlı yönlendirme algoritmaları, RPL ağlarında enerji tüketimini optimize etmek için önerilmiştir.

1.4.5.5G Entegrasyonu ve Yeni Zorluklar

5G teknolojisinin IoT ağlarına entegrasyonu, yüksek veri hızları ve düşük gecikme süreleri sunarak enerji verimliliği potansiyelini artırmaktadır. Ancak, 5G'nin karmaşık mimarisi, özellikle ağ dilimleme (network slicing) ve çoklu erişim kenar hesaplama (MEC) gibi teknolojiler, yeni enerji tüketimi zorlukları yaratmaktadır. Khan ve diğerleri (2021), 5G tabanlı IoT ağlarında enerji tüketiminin, heterojen cihazların artan iletişim yoğunluğu nedeniyle %25'e kadar artabileceğini rapor etmiştir. Bu bağlamda, 5G ağlarında enerji verimliliği için dinamik kaynak tahsisi ve kenar hesaplama tabanlı veri işleme yöntemleri önerilmiştir (Liu, G., Wang, C., Ma, X., Yang, Y. 2021). Ayrıca, 5G entegrasyonu ile birlikte, RPL tabanlı ağların enerji tüketimini optimize etmek için yeni nesil yönlendirme protokolleri geliştirilmesi gerektiği vurgulanmaktadır.

1.4.6.Simülasyon ve Analiz Araçları

IoT ağlarında enerji tüketiminin analizi, simülasyon ortamları ve analiz araçlarıyla detaylı şekilde gerçekleştirilmektedir. Contiki işletim sistemi ve Cooja simülatörü, RPL tabanlı ağların enerji tüketimini modellemek için yaygın olarak kullanılmaktadır. Cooja, Powertrace modülü aracılığıyla düğümlerin CPU, LPM, TX ve RX modlarındaki enerji tüketimini milisaniye çözünürlüğünde kaydetmektedir. Ayrıca, Foren6 aracı, RPL ağlarının DODAG yapısındaki değişiklikleri görselleştirerek enerji tüketimiyle ilişkili topolojik etkileri analiz etmektedir. Wireshark, ağ trafiğindeki enerji yoğun protokol mesajlarını (örneğin, DIO, DAO) izlemek için kullanılmaktadır. Bu araçlar, Blackhole ve HelloFlood gibi saldırıların enerji tüketimi üzerindeki etkilerini çok boyutlu bir şekilde değerlendirme imkânı sunmaktadır (Rejeb, S. B., Nasser, N., Mansour, S., Boujlbane, M. 2017).

1.4.7.Gelecek Yönelimler

IoT ağlarında enerji tüketimi, hem siber güvenlik hem de ağ sürdürülebilirliği açısından kritik bir araştırma alanıdır. Gelecekteki çalışmalar, enerji verimli makine öğrenmesi modelleri ve federated learning gibi yenilikçi yaklaşımlara

odaklanmaktadır. Federated learning, IoT cihazlarının yerel veri işleme kapasitesini kullanarak enerji tüketimini azaltırken, merkezi olmayan tehdit tespiti sağlamaktadır (Yang, Q., Liu, Y., Chen, T., Tong, Y. 2019). Ayrıca, kenar hesaplama tabanlı çözümler, veri işlemenin cihazlar yerine ağ kenarında gerçekleştirilmesini sağlayarak enerji tasarrufu sunmaktadır. Bunun yanı sıra, RPL protokolünün enerji odaklı optimizasyonları ve yeni nesil düşük güçlü iletişim protokolleri (örneğin, TSCH - Time Slotted Channel Hopping) geliştirilmesi gerektiği belirtilmektedir. IoT ağlarının artan karmaşıklığı ve 5G entegrasyonu, enerji tüketiminin çok katmanlı bir yaklaşımla ele alınmasını zorunlu kılmaktadır (Xu, L. D., Xu, E. L., Li, L. 2018).

Sonuç olarak, IoT ağlarında enerji tüketimi, ağ tasarımı, siber güvenlik ve sürdürülebilirlik açısından temel bir parametredir. RPL tabanlı ağlarda Blackhole, HelloFlood ve Version Number gibi saldırılar, enerji tüketimini artırarak ağın operasyonel ömrünü tehdit etmektedir. Hafif güvenlik mekanizmaları, makine öğrenmesi tabanlı tespit sistemleri ve 5G entegrasyonu, enerji verimliliğini artırmak için umut vadetmektedir; ancak, kaynak kısıtlamaları ve heterojen ağ yapıları, bu alanda daha fazla araştırma ve optimizasyon gerektirmektedir.

1.5. Simülasyon Ortamları ve Analiz Araçları

Nesnelerin İnterneti (IoT) ağlarının modellenmesi, test edilmesi ve analizi, kablosuz sensör ağlarının (WSN) 2000'li yıllarda yaygınlaşmasıyla kritik bir araştırma alanı haline gelmiştir. Erken dönemde, NS-2 ve TOSSIM gibi genel ağ simülatörleri kullanılmış; ancak, bu araçların düşük güçlü ve kayıplı ağlara özgü gereksinimleri karşılamadaki yetersizlikleri, IoT'ya özel simülasyon ortamlarının geliştirilmesini zorunlu kılmıştır (Baccelli, E., Hahm, O., Gunes, M., Wahlisch, M., Schmidt, T. C. 2013). 2010'lu yıllarda, Contiki işletim sistemi ve Cooja simülatörü gibi platformlar, IoT ağlarının enerji verimliliği, yönlendirme dinamikleri ve güvenlik analizleri için standart araçlar haline gelmiştir. Bu araçlar, RPL (Routing Protocol for Low-Power and Lossy Networks) tabanlı ağların modellenmesinde ve siber tehditlerin simüle edilmesinde yaygın olarak kullanılmaktadır. Ayrıca, Foren6 ve Wireshark gibi analiz araçları, ağ topolojisi ve trafik davranışlarının detaylı incelenmesini sağlamaktadır. Bu bölüm, IoT ağlarının simülasyonu ve analizi için kullanılan temel araçları ve bunların güvenlik araştırmalarındaki rollerini ayrıntılı olarak incelemektedir.

1.5.1. Contiki İşletim Sistemi

Contiki, düşük güçlü ve kaynak kısıtlı IoT cihazları için tasarlanmış, açık kaynaklı bir işletim sistemidir. Hafif yapısı, modüler tasarımı ve enerji verimliliği, Contiki'yi IoT ağlarında sensör düğümleri ve gömülü sistemler için ideal bir platform haline getirmektedir. Contiki, IPv6 tabanlı protokolleri (örneğin, 6LoWPAN ve RPL) desteklemekte ve olay odaklı programlama modeli sayesinde düşük enerji tüketimiyle veri toplama ve iletim süreçlerini kolaylaştırmaktadır. Özellikle, Contiki'nin RPL protokolüne yerel desteği, IoT ağlarının yönlendirme dinamiklerini modellemede önemli bir avantaj sağlamaktadır. Yapılan çalışmalar, Contiki'nin farklı ağ topolojilerini ve saldırı senaryolarını simüle etme esnekliği sunduğunu ortaya koymuştur (Mishra, A., Alwasel, B., Nepal, S. 2016). Contiki, güvenlik analizlerinde de sıklıkla kullanılmaktadır. Örneğin, Blackhole ve HelloFlood gibi saldırıların ağ üzerindeki etkileri, Contiki tabanlı simülasyonlarla detaylı şekilde incelenmiştir. Contiki'nin açık kaynaklı yapısı, araştırmacıların protokol kodlarını özelleştirmesine ve yeni güvenlik mekanizmalarını entegre etmesine olanak tanımaktadır. Ayrıca, Contiki'nin Powertrace modülü, düğümlerin enerji tüketimini milisaniye çözünürlüğünde izleyerek, saldırıların enerji verimliliği üzerindeki etkilerini analiz etme imkânı sunmaktadır. Ancak, Contiki'nin sınırlı donanım emülasyon yetenekleri, büyük ölçekli ve heterojen ağların modellenmesinde optimizasyon gerektirmektedir.

1.5.2. Cooja Simülatörü

Cooja, Contiki işletim sistemiyle entegre çalışan bir ağ simülatörü olup, IoT ağlarının modellenmesi, test edilmesi ve analiz edilmesi için tasarlanmıştır. Cooja, hem donanım düzeyinde (gerçek cihaz emülasyonu) hem de yazılım düzeyinde (sanal düğüm simülasyonu) simülasyon yetenekleri sunmaktadır. Bu özellik, Cooja'yı RPL tabanlı IoT ağlarının performansını ve güvenlik açıklarını değerlendirmede güçlü bir araç haline getirmektedir. Cooja, IEEE 802.15.4 gibi standartları desteklemekte ve Unit Disk Graph (UDG) gibi radyo modelleriyle gerçekçi iletişim senaryoları oluşturmaktadır. Ayrıca, grafiksel arayüzü, ağ topolojilerinin (örneğin, DODAG yapıları) görselleştirilmesini ve düğüm davranışlarının gerçek zamanlı izlenmesini sağlamaktadır.

Cooja, siber güvenlik arařtırmalarında, özellikle Blackhole, HelloFlood ve Version Number gibi RPL tabanlı saldırıların simüle edilmesi ve analizinde yaygın olarak kullanılmaktadır. Örneğın, Raoof ve diğerkleri (2018), Cooja'yı kullanarak Blackhole saldırısının ağıın veri iletim başarı oranını %50'ye kadar düşürdüğünü ve enerji tüketimini artırdığını rapor etmiştir. Cooja, ağ trafiğini .pcap formatında kaydederek Wireshark ile detaylı analiz imkânı sunmakta ve Powertrace ile enerji tüketimi ölçümlerini desteklemektedir. Bununla birlikte, Cooja'nın büyük ölçekli ağlarda performans sınırlamaları ve heterojen cihazların modellenmesindeki zorluklar, yeni nesil simülatörlerin geliştirilmesini gerektirmektedir (Vasseur, J.-P., Kim, M., Pister, K., Dejean, N., Barthel, D. 2011).

1.5.3. Foren6 Analiz Aracı

Foren6, RPL tabanlı IoT ağlarının görselleştirilmesi ve analizi için geliştirilmiş bir ağ teşhis aracıdır. Bu araç, RPL ağlarının DODAG yapısını gerçek zamanlı olarak görselleştirmekte ve yönlendirme hataları, enerji tüketimi anomalileri ve saldırı belirtilerini tespit etmek için kullanılmaktadır. Foren6, DIO, DAO ve DIS gibi RPL kontrol mesajlarını analiz ederek ağ topolojisindeki değışiklikleri detaylı şekilde ortaya koymaktadır. Örneğın, bir Blackhole saldırısı sırasında, Foren6, saldırgan düğümün çok sayıda düğüm tarafından ebeveyn seçildiğini ve veri akışının kesintiye uğradığını görselleştirmiştir.

Foren6'nın temel avantajı, ağ dinamiklerini grafiksel olarak sunarak arařtırmacıların saldırıların topolojik etkilerini anlamasını kolaylaştırmasıdır. Ayrıca, Wireshark ile birlikte kullanıldığında, ağ trafiğindeki anormallikleri tespit etmek için tamamlayıcı bir analiz sağlamaktadır. Foren6, veri çıktısını .csv formatında dışa aktararak ileri istatistiksel analizlere olanak tanımaktadır. Ancak, Foren6'nın büyük ölçekli ağlarda performans sorunları ve karmaşık ağ yapılarının görselleştirilmesindeki sınırlamalar, bu aracın optimizasyon gereksinimlerini ortaya koymaktadır (Kirsche ve Klauck, 2012).

1.5.4. Wireshark Ağ Analiz Aracı

Wireshark, ağ trafiğini yakalamak, analiz etmek ve görselleştirmek için kullanılan açık kaynaklı bir ağ analiz aracıdır. IoT ağlarında, veri paketlerinin içeriğini incelemek, protokol davranışlarını analiz etmek ve siber güvenlik tehditlerini tespit

etmek için yaygın şekilde kullanılmaktadır. Wireshark, RPL tabanlı ağlarda ICMPv6, UDP, DIO, DAO ve DIS gibi protokol mesajlarını detaylı şekilde analiz ederek anormal davranışları (örneğin, sahte yönlendirme mesajları veya aşırı trafik) belirlemektedir. Örneğin, HelloFlood saldırısında, Wireshark, DIS mesajlarının yoğunlaşmasını ve ağ trafiğinin %60 artmasını tespit etmiştir (Bhattasali, T., Chaki, R., Chaki, N. 2013).

Wireshark, Cooja simülatöründen elde edilen .pcap dosyalarını analiz ederek, RPL ağlarında saldırıların protokol düzeyindeki etkilerini ortaya koymaktadır. Wireshark'ın zaman damgalı paket analizi, saldırıların zamansal örüntülerini anlamada kritik bir rol oynamaktadır. Ancak, büyük veri hacimlerinde manuel analiz zorlukları ve heterojen protokollerin karmaşıklığı, Wireshark'ın otomatik analiz araçlarıyla entegrasyonunu gerektirmektedir (Nath, A. 2015).

1.5.5. Diğer Simülasyon ve Analiz Araçları

Contiki, Cooja, Foren6 ve Wireshark dışında, IoT ağlarının simülasyonu ve analizi için başka araçlar da kullanılmaktadır. Örneğin, OMNeT++ simülatörü, büyük ölçekli ve heterojen IoT ağlarının modellenmesinde yüksek performans sunmaktadır. NS-3, 5G entegrasyonlu IoT ağlarının simülasyonu için giderek yaygınlaşmaktadır. Ayrıca, Tshark (Wireshark'ın komut satırı sürümü) ve Scapy gibi araçlar, otomatik ağ trafiği analizi ve özelleştirilmiş protokol testleri için tercih edilmektedir. Bu araçlar, IoT ağlarının karmaşık dinamiklerini analiz etmek ve güvenlik çözümlerini test etmek için tamamlayıcı bir altyapı sunmaktadır (Musznicki ve Zwierzykowski, 2017).

1.5.6. Simülasyon Ortamlarının Güvenlik Araştırmalarındaki Rolü

Simülasyon ortamları ve analiz araçları, IoT ağlarının güvenilirliğini artırmak ve siber tehditlere karşı savunma mekanizmalarını doğrulamak için vazgeçilmez bir rol oynamaktadır. Cooja tabanlı simülasyonlar, Blackhole ve HelloFlood gibi saldırıların ağ üzerindeki etkilerini (örneğin, veri kaybı, enerji tüketimi artışı) detaylı şekilde modellemektedir. Foren6 ve Wireshark, bu etkilerin topolojik ve protokol düzeyinde analizini sağlayarak, makine öğrenmesi modellerine veri seti oluşturmada temel bir altyapı sunmaktadır. Örneğin, Sharma ve diğerleri (2021), Cooja'dan toplanan verilerle eğitilen XGBoost modelinin, RPL tabanlı ağlarda saldırı tespitinde %98

doğruluk sağladığını rapor etmiştir (Alsaedi, A., Moustafa, N., Tari, Z., Mahmood, A., Anwar, A. 2020).

Bununla birlikte, simülasyon ortamlarının sınırlamaları da dikkate alınmalıdır. Cooja, büyük ölçekli ağlarda performans sorunları yaşayabilmekte ve gerçek dünya koşullarında (örneğin, fiziksel gürültü, cihaz arızaları) tam doğruluk sağlayamamaktadır. Ayrıca, heterojen cihazların ve 5G entegrasyonunun modellenmesi, mevcut simülatörlerin ölçeklenebilirlik kapasitesini zorlamaktadır. Bu nedenle, yeni nesil simülatörlerin geliştirilmesi ve hibrit simülasyon ortamlarının (örneğin, gerçek cihazlarla simülatör entegrasyonu) araştırılması gerektiği vurgulanmaktadır.

1.5.7. Gelecek Yönelimler

IoT ağlarının simülasyonu ve analizi, giderek karmaşılaşan ağ yapıları ve güvenlik tehditleri nedeniyle yenilikçi yaklaşımlar gerektirmektedir. Makine öğrenmesi tabanlı simülasyon optimizasyonu, büyük ölçekli ağların modellenmesini kolaylaştırmak için araştırılmaktadır. Örneğin, federated learning, simülasyon verilerinin yerel işlenmesiyle veri gizliliğini korurken analiz doğruluğunu artırmaktadır. Ayrıca, 5G tabanlı IoT ağlarının simülasyonu için NS-3 gibi araçların geliştirilmesi ve kenar hesaplama entegrasyonu, gerçek zamanlı analiz kapasitesini güçlendirmektedir. Bunun yanı sıra, simülasyon ortamlarının açık kaynaklı yapısı, araştırmacıların tekrarlanabilir ve erişilebilir çalışmalar yapmasını desteklemekte; ancak, standart veri setlerinin eksikliği ve simülasyon araçlarının birbiriyle uyumluluğu, bu alanda daha fazla standardizasyon gerektirmektedir (Hahm, O., Baccelli, E., Petersen, H., Tsiftes, N. 2016).

Sonuç olarak, Contiki, Cooja, Foren6 ve Wireshark gibi simülasyon ve analiz araçları, IoT ağlarının performansını, güvenilirliğini ve güvenliğini değerlendirmede kritik bir altyapı sunmaktadır. Bu araçlar, RPL tabanlı ağlarda siber tehditlerin etkilerini çok boyutlu bir şekilde analiz ederek, makine öğrenmesi ve derin öğrenme tabanlı savunma mekanizmalarının geliştirilmesine olanak tanımaktadır. Ancak, büyük ölçekli ağlar, heterojen cihazlar ve yeni nesil iletişim teknolojileri, simülasyon ortamlarının ölçeklenebilirlik ve doğruluk açısından geliştirilmesini zorunlu kılmaktadır.

1.6. Makine Öğrenmesi ve Derin Öğrenme ile Saldırı Tespiti

Makine öğrenmesi tabanlı saldırı tespiti, 2000’li yılların başında ağ güvenliği alanında kullanılmaya başlanmış ve Nesnelerin İnterneti (IoT) ağlarına uyarlanması, 2010’lu yıllarda cihaz sayısındaki hızlı artış ve heterojen ağ yapılarının yaygınlaşmasıyla önem kazanmıştır. IoT ağlarının kaynak kısıtlı doğası, düşük güçlü cihazları ve kablosuz iletişim ortamları, geleneksel güvenlik mekanizmalarının uygulanmasını zorlaştırmakta; bu nedenle, makine öğrenmesi, otomatik ve ölçeklenebilir tehdit tespit çözümleri sunmak için kritik bir araç haline gelmektedir (Sommer ve Paxson, 2010). Erken dönemde, destek vektör makineleri (SVM) ve karar ağaçları gibi geleneksel algoritmalar, IoT ağlarında temel anomali tespiti için kullanılmış; ancak, karmaşık tehditlerin ve sıfır-gün saldırılarının artmasıyla bu yöntemlerin sınırlamaları ortaya çıkmıştır. 2015 yılından itibaren derin öğrenme yöntemlerinin yükselişi, IoT ağlarında saldırı tespitinde yeni bir dönemi başlatmıştır. Bu bölüm, makine öğrenmesi ve derin öğrenme tabanlı saldırı tespit yöntemlerini, özellikle RPL (Routing Protocol for Low-Power and Lossy Networks) tabanlı IoT ağlarındaki uygulamalarını detaylı bir şekilde incelemektedir.

Makine öğrenmesi tabanlı sistemler, ağ trafiğindeki anormal davranışları tespit etmek için istatistiksel örüntüleri ve veri özelliklerini analiz etmektedir. IoT ağlarında, Blackhole, HelloFlood ve Version Number gibi RPL tabanlı saldırılar, ağ trafiğinde belirli anomalilere (örneğin, sahte rank değerleri, aşırı kontrol mesajları) neden olmakta ve bu anomaliler, makine öğrenmesi modelleriyle tespit edilebilmektedir. Örneğin, karar ağaçları ve rastgele orman (Random Forest) gibi algoritmalar, erken dönemde IoT ağlarında DDoS saldırılarını tespit etmek için kullanılmış ve düşük hesaplama maliyetiyle kabul edilebilir doğruluk sağlamıştır (Popoola, S. I., Adebisi, B., Hammoudeh, M., Gui, G., Gacatin, H. 2021). Ancak, bu algoritmaların zamansal bağımlılıkları modellemedeki yetersizlikleri, daha karmaşık tehditler için derin öğrenme modellerine olan ihtiyacı artırmıştır.

Derin öğrenme, özellikle LSTM (Long Short-Term Memory) ve CNN (Convolutional Neural Network) gibi modeller, IoT ağ trafiğindeki zamansal ve uzamsal örüntüleri analiz etmede yüksek performans sergilemektedir. LSTM’nin bellek hücreleri, ağ trafiğindeki uzun süreli bağımlılıkları öğrenerek, saldırıların zamanla değişen davranışlarını modelleme kapasitesi sunmaktadır. Benzer şekilde,

BiLSTM (Bidirectional Long Short-Term Memory), hem geçmiş hem de gelecek bağlamını dikkate alarak daha hassas tespitler sağlamakta ve özellikle Version Number gibi dinamik saldırılarda etkili bulunmaktadır. Ancak, derin öğrenme modellerinin yüksek hesaplama karmaşıklığı, kaynak kısıtlı IoT cihazlarında uygulanabilirliklerini sınırlamakta ve bu durum, hafif modellerin geliştirilmesini zorunlu kılmaktadır (Meidan, Y., Bohadana, M., Mathur, A., Shabtai, A., Elovici, Y. 2018).

Gradyan artırma tabanlı algoritmalar, özellikle XGBoost ve LightGBM, IoT ağlarında saldırı tespiti için düşük hesaplama maliyeti ve yüksek doğruluk sunmaktadır. XGBoost, karmaşık veri desenlerini öğrenme yeteneğiyle, RPL tabanlı ağlarda Blackhole ve HelloFlood saldırılarını tespit etmiştir. LightGBM ise, histogram tabanlı öğrenme algoritmasıyla hızlı eğitim süreleri sağlamakta ve özellikle gerçek zamanlı uygulamalarda tercih edilmektedir. Bu algoritmalar, Accuracy, F1 skoru, Precision, Recall ve AUC gibi metriklerle değerlendirilerek, IoT ağlarının güvenlik gereksinimlerine uygunluk göstermektedir. Ancak, sınıf dengesizliği ve yüksek boyutlu veri setleri, bu modellerin performansını optimize etme gereksinimini ortaya koymaktadır (M., Guirguis, S., Madbouly, M. 2023).

Makine öğrenmesi tabanlı saldırı tespitinde veri ön işleme ve öznitelik mühendisliği, model doğruluğunu artırmada kritik bir rol oynamaktadır. IoT ağlarından toplanan veriler, genellikle frame.time, frame.len, icmpv6.type gibi öznitelikler içermekte ve bu öznitelikler, saldırıların karakteristik davranışlarını temsil etmektedir. Sentetik veri üretimi teknikleri ve öznitelik seçimi yöntemleri, sınıf dengesizliği sorununu çözerek model performansını iyileştirmektedir. Ayrıca, HDF5 gibi yüksek performanslı veri formatları, büyük veri setlerinin hızlı işlenmesini sağlayarak makine öğrenmesi modellerinin eğitimini hızlandırmaktadır.

Son yıllarda, federated learning, IoT ağlarında saldırı tespiti için yenilikçi bir yaklaşım olarak öne çıkmaktadır. Federated learning, merkezi bir sunucuya veri aktarmadan, yerel cihazlarda model eğitimi gerçekleştirerek veri gizliliğini korumakta ve enerji tüketimini azaltmaktadır. Ancak, bu yaklaşımın iletişim maliyetleri ve heterojen cihazlar arasındaki senkronizasyon zorlukları, uygulanabilirliğini sınırlamaktadır.

Makine öğrenmesi tabanlı saldırı tespit sistemlerinin IoT ağlarındaki zorlukları, kaynak kısıtlamaları, gerçek zamanlı işlem gereksinimleri ve sıfır-gün tehditleridir. Derin öğrenme modellerinin hesaplama karmaşıklığı, düşük güçlü cihazlarda optimizasyon gerektirmektedir. Ayrıca, IoT ağlarının heterojen yapısı, farklı protokoller ve cihaz türleri arasında standart veri setlerinin oluşturulmasını zorlaştırmaktadır. 5G entegrasyonu, IoT ağlarında veri hacmini ve işlem karmaşıklığını artırarak, makine öğrenmesi modellerinin ölçeklenebilirlik gereksinimlerini ön plana çıkarmaktadır. Bu bağlamda, kenar hesaplama (edge computing) tabanlı modeller, veri işlemenin ağ kenarında gerçekleştirilmesini sağlayarak hem enerji verimliliğini hem de gerçek zamanlı tepki kapasitesini artırmaktadır.

Gelecekteki araştırmalar, hafif derin öğrenme modelleri, federated learning ve kenar hesaplama entegrasyonuna odaklanmaktadır. Örneğin, sıkıştırılmış sinir ağları, IoT cihazlarında derin öğrenme modellerinin uygulanabilirliğini artırmak için araştırılmaktadır. Ayrıca, otomatik makine öğrenmesi (AutoML) teknikleri, IoT ağlarında model seçimi ve hiperparametre optimizasyonunu kolaylaştırarak araştırma süreçlerini hızlandırmaktadır. RPL tabanlı ağlarda saldırı tespitinde, makine öğrenmesi modellerinin enerji verimliliği, sınıf dengesizliği ve gerçek zamanlı uygulanabilirlik gibi zorlukların aşılması, IoT ekosisteminin güvenilirliğini artırmak için kritik bir gereksinimdir.

Sonuç olarak, makine öğrenmesi ve derin öğrenme tabanlı saldırı tespit sistemleri, RPL tabanlı IoT ağlarında Blackhole, HelloFlood ve Version Number gibi tehditlere karşı etkili çözümler sunmaktadır. XGBoost, LightGBM, LSTM ve BiLSTM gibi modeller, yüksek doğruluk ve ölçeklenebilirlik sağlarken, federated learning ve kenar hesaplama gibi yenilikçi yaklaşımlar, veri gizliliği ve enerji verimliliği açısından umut vadetmektedir. Ancak, kaynak kısıtlamaları, heterojen ağ yapıları ve sıfır-gün tehditler, bu alanda daha fazla optimizasyon ve araştırma gerektirmektedir.

1.7. Büyük Veri Analizi ve IoT Ağlarında Veri İşleme

Nesnelerin İnterneti (IoT) ağlarında büyük veri analizi, 2000'li yılların başında Hadoop ve MapReduce gibi teknolojilerin ortaya çıkışıyla ağ tabanlı sistemlerde önem

kazanmış; ancak, IoT ekosistemine uyarlanması, 2010'lu yıllarda cihaz sayısındaki hızlı artış ve sensörlerden toplanan yüksek hacimli verilerin karmaşıklığıyla kritik bir gereksinim haline gelmiştir. IoT ağları, heterojen cihazlardan sürekli veri üreten dinamik bir yapıya sahip olup, bu verilerin toplanması, depolanması, işlenmesi ve analiz edilmesi, ağ güvenliği ve performans optimizasyonu açısından temel bir rol oynamaktadır (Marjani, M., Nasaruddin, F., Gani, A., Karim, A., Hashem, I. A. T., Siddiqua, A., Yaqoob, I. 2017). Özellikle RPL (Routing Protocol for Low-Power and Lossy Networks) tabanlı IoT ağlarında, Blackhole, HelloFlood ve Version Number gibi siber saldırıların tespitinde, büyük veri analizi, makine öğrenmesi modelleriyle entegre edilerek yüksek doğruluk ve ölçeklenebilirlik sağlamaktadır. Bu bölüm, IoT ağlarında büyük veri analizinin temel prensiplerini, veri işleme yöntemlerini ve güvenlik uygulamalarındaki rolünü detaylı bir şekilde incelemektedir.

Büyük veri analizi, IoT ağlarında veri hacmi, çeşitliliği ve hızı gibi özelliklere odaklanmaktadır. Bu veriler, ağ trafiği kayıtları, sensör ölçümleri, protokol mesajları (örneğin, DIO, DAO) ve enerji tüketimi metrikleri gibi çeşitli formatlarda toplanmaktadır. Ancak, IoT cihazlarının sınırlı işlem kapasitesi ve enerji kaynakları, bu verilerin merkezi bir sunucuda işlenmesini zorlaştırmakta; bu nedenle, veri işleme süreçlerinin enerji verimli ve dağıtık bir şekilde tasarlanması gerekmektedir (Al-Salim, A. M., Lawey, A. Q., El-Gorashi, T. E., Elmirghani, J. M. 2017).

Erken dönemde, IoT verileri temel dosya formatları ve ilişkisel veritabanlarıyla işlenmiş; ancak, bu yöntemlerin yüksek hacimli ve gerçek zamanlı veri akışlarını yönetmedeki yetersizlikleri, yeni nesil veri işleme teknolojilerinin geliştirilmesini tetiklemiştir. HDF5 gibi yüksek hızlı erişim sağlayan veri formatları, IoT verilerinin depolanması ve analizinde standart bir çözüm haline gelmiştir. HDF5, hiyerarşik yapısıyla büyük veri kümelerinin düzenli ve hızlı bir şekilde işlenmesini sağlamakta; özellikle, makine öğrenmesi modellerine veri girdisi hazırlamada kritik bir rol oynamaktadır (Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., Ayyash, M. 2015).

Veri ön işleme ve öznitelik mühendisliği, IoT ağlarında büyük veri analizinin temel bileşenleridir. IoT verileri genellikle gürültülü, eksik veya dengesiz olabilmekte; bu nedenle, veri temizleme, normalizasyon ve öznitelik seçimi süreçleri, analiz doğruluğunu artırmaktadır. Örneğin, RPL tabanlı ağlarda Blackhole saldırısını tespit

etmek için kullanılan öznitelikler arasında frame.time, frame.len, icmpv6.type ve ipv6.src gibi parametreler yer almakta ve bu öznitelikler, saldırıların karakteristik davranışlarını temsil etmektedir. Sınıf dengesizliği sorununu çözmek için sentetik veri üretimi teknikleri ve öznitelik azaltma yöntemleri, veri setlerinin kalitesini iyileştirmekte ve makine öğrenmesi modellerinin performansını artırmaktadır (Ferdowsi, A., Challita, U., Saad, W., Mandayam, N. B. 2018).

Dağıtık veri işleme çerçeveleri, IoT ağlarında büyük veri analizinin ölçeklenebilirliğini artırmaktadır. Gerçek zamanlı veri akışlarını işleme kapasitesiyle, ağ trafiğindeki anomalileri tespit etmede etkili bir altyapı sunmaktadır. Bununla birlikte, dağıtık sistemlerin yüksek enerji tüketimi ve iletişim maliyetleri, IoT ağlarının kaynak kısıtlı doğasıyla çelişmekte; bu nedenle, kenar hesaplama tabanlı veri işleme yöntemleri giderek yaygınlaşmaktadır. Kenar hesaplama, veri işlemenin ağ kenarında gerçekleştirilmesini sağlayarak merkezi sunuculara olan bağımlılığı azaltmakta ve enerji verimliliğini artırmaktadır.

Büyük veri analizi, IoT ağlarında siber güvenlik uygulamalarında kritik bir rol oynamaktadır. Makine öğrenmesi ve derin öğrenme modelleri, büyük veri setlerinden öğrenerek Blackhole, HelloFlood ve Version Number gibi RPL tabanlı saldırıların tespitinde yüksek performans sergilemektedir. Ancak, büyük veri setlerinin işlenmesi, veri gizliliği ve güvenlik risklerini de beraberinde getirmektedir. Örneğin, IoT cihazlarından toplanan hassas verilerin kötü niyetli aktörler tarafından ele geçirilmesi, gizlilik ihlallerine yol açabilmektedir (Nia ve Jha, 2017).

Federated learning, IoT ağlarında büyük veri analizinin gizlilik odaklı bir yaklaşımı olarak öne çıkmaktadır. Bu yöntem, veri paylaşımı olmadan yerel cihazlarda model eğitimi gerçekleştirerek hem gizliliği korumakta hem de iletişim maliyetlerini azaltmaktadır. Ancak, federated learning'in heterojen cihazlar arasındaki senkronizasyon zorlukları ve model güncelleme süreçlerinin karmaşıklığı, uygulanabilirliğini sınırlamaktadır. Bu nedenle, hafif federated learning algoritmaları ve kenar hesaplama entegrasyonu, gelecekteki araştırmalarda öncelikli bir alan olarak öne çıkmaktadır.

IoT ağlarında büyük veri analizinin zorlukları, veri hacmi, heterojenlik ve gerçek zamanlı işlem gereksinimleridir. 5G teknolojisinin IoT ekosistemine entegrasyonu, veri üretim hızını artırarak analiz süreçlerini daha karmaşık hale getirmektedir. Ayrıca,

IoT cihazlarının sınırlı işlem kapasitesi, büyük veri analitiğinin merkezi olmayan bir şekilde uygulanmasını zorunlu kılmaktadır. Bu bağlamda, kenar hesaplama ve fog computing gibi teknolojiler, veri işlemenin ağ kenarında veya ara katmanlarda gerçekleştirilmesini sağlayarak hem gecikmeyi azaltmakta hem de enerji verimliliğini artırmaktadır.

Gelecekteki araştırmalar, IoT ağlarında büyük veri analizinin enerji verimliliği, ölçeklenebilirlik ve gizlilik odaklı optimizasyonuna odaklanmaktadır. Otomatik makine öğrenmesi teknikleri, veri ön işleme ve model seçimi süreçlerini otomatikleştirerek analiz süreçlerini hızlandırmaktadır. Ayrıca, blockchain tabanlı veri paylaşım sistemleri, IoT ağlarında veri bütünlüğünü ve güvenilirliğini artırmak için araştırılmaktadır. RPL tabanlı ağlarda, büyük veri analizi, makine öğrenmesi modelleriyle entegre edilerek siber tehditlerin tespitinde kritik bir rol oynamakta; ancak, veri gizliliği, enerji tüketimi ve gerçek zamanlı işlem gereksinimleri, bu alanda daha fazla yenilik gerektirmektedir.

Büyük veri analizi, IoT ağlarında ağ güvenliği, performans optimizasyonu ve sürdürülebilirlik açısından vazgeçilmez bir araçtır. Teknolojiler, veri işleme süreçlerini hızlandırırken, federated learning ve kenar hesaplama, gizlilik ve enerji verimliliği sağlamaktadır. RPL tabanlı ağlarda Blackhole, HelloFlood ve Version Number gibi saldırıların tespitinde, büyük veri analitiği, makine öğrenmesi modelleriyle sinerji oluşturarak yüksek doğruluk sunmakta; ancak, heterojen ağ yapıları ve kaynak kısıtlamaları, bu alanda daha fazla araştırma ve optimizasyon gerektirmektedir.

İKİNCİ BÖLÜM

IOT SİSTEMLERİNDEKİ TEHDİTLER VE ALINAN ÖNLEMLER: GÜNCEL YAKLAŞIMLAR

2.1. IoT Sistemlerinin Yapısı ve Güvenlik Açıkları

Nesnelerin İnterneti (IoT), fiziksel cihazların sensörler, yazılımlar ve iletişim teknolojileriyle donatılarak internet üzerinden birbirleriyle veri alışverişi yapmasını sağlayan bir ağ ekosistemi olarak tanımlanmaktadır. IoT sistemleri, akıllı evlerden endüstriyel otomasyona, sağlık hizmetlerinden akıllı şehir uygulamalarına kadar geniş bir yelpazede kullanılmakta ve verimliliği artırarak yaşam kalitesini iyileştirmektedir. Ancak, IoT sistemlerinin heterojen yapısı, sınırlı kaynaklara sahip cihazları ve kablosuz iletişim ortamları, bu sistemleri çeşitli güvenlik açıklarına karşı savunmasız kılmaktadır. Bu bölüm, IoT sistemlerinin temel yapısını ve bu yapının doğurduğu güvenlik açıklarını detaylı bir şekilde incelemektedir.

IoT sistemleri, genellikle üç ana katmandan oluşmaktadır: algılama katmanı (perception layer), ağ katmanı (network layer) ve uygulama katmanı (application layer). Algılama katmanı, sensörler ve aktüatörler aracılığıyla çevreden veri toplamakta ve fiziksel dünyayla etkileşim kurmaktadır. Ağ katmanı, toplanan verilerin iletimi için kablosuz protokoller (örneğin, Wi-Fi, ZigBee, 6LoWPAN) ve yönlendirme mekanizmaları (örneğin, RPL) kullanmaktadır. Uygulama katmanı ise, verilerin işlenmesi, analiz edilmesi ve kullanıcıya sunulması için bulut tabanlı servisler ve arayüzler sağlamaktadır. Bu katmanlı yapı, IoT sistemlerinin esnekliğini ve ölçeklenebilirliğini artırmakta; ancak, her katman kendine özgü güvenlik açıkları barındırmaktadır.

Algılama katmanında, IoT cihazlarının sınırlı işlem kapasitesi ve enerji kaynakları, karmaşık güvenlik mekanizmalarının uygulanmasını zorlaştırmaktadır. Örneğin, düşük güçlü sensör düğümleri, genellikle hafif şifreleme algoritmaları kullanmakta ve bu durum, veri gizliliği ve bütünlüğünü riske atmaktadır. Ayrıca, fiziksel erişim açıkları, cihazların manipülasyona veya kötü niyetli kod enjeksiyonuna karşı savunmasız olmasına neden olmaktadır. IoT cihazlarının fiziksel sabotaja karşı korunması için donanım tabanlı güvenlik modüllerinin (örneğin, Trusted Platform

Module) entegrasyonunu önerilmiştir; ancak, bu çözümler maliyet ve enerji tüketimi açısından sınırlamalar taşımaktadır.

Ağ katmanı, IoT sistemlerinin en kritik güvenlik açıklarının bulunduğu bir bileşenidir. Kablosuz iletişim ortamları, veri ağları (eavesdropping), sahte düğüm enjeksiyonu ve yönlendirme saldırıları gibi tehditlere karşı hassastır. RPL gibi protokoller, düşük güç ve kayıplı ağlar için optimize edilmiştir; ancak, Blackhole, HelloFlood ve Version Number gibi saldırılar, ağın yönlendirme yapısını bozarak veri kaybına ve enerji tüketiminde artışa yol açmaktadır. Örneğin, Blackhole saldırısı, kötü niyetli bir düğümün sahte rank değerleriyle veri paketlerini düşürmesiyle ağın işlevselliğini tehdit etmektedir. Ayrıca, ağ katmanında kullanılan protokollerin (örneğin, 6LoWPAN, CoAP) sıkıştırma mekanizmaları, güvenlik kontrollerini bypass eden saldırılara zemin hazırlayabilmektedir.

Uygulama katmanı, veri işleme ve kullanıcı arayüzleriyle ilişkili güvenlik açıkları barındırmaktadır. Bulut tabanlı servisler, veri gizliliği ihlalleri ve yetkisiz erişim riskleriyle karşı karşıyadır. Örneğin, zayıf kimlik doğrulama mekanizmaları, kötü niyetli kullanıcıların hassas verilere erişmesine olanak tanımaktadır. Ayrıca, IoT uygulamalarının heterojen yapısı, farklı platformlar ve protokoller arasında uyumluluk sorunları yaratmakta ve bu durum, güvenlik açıklarının istismar edilmesini kolaylaştırmaktadır. 2016'daki Mirai botnet saldırısı, zayıf parolalara sahip IoT cihazlarının ele geçirilerek büyük çaplı DDoS saldırılarında kullanıldığını göstermiş ve uygulama katmanı güvenliğinin önemini vurgulamıştır.

IoT sistemlerinin heterojen yapısı, farklı cihaz türlerinin ve iletişim protokollerinin bir arada bulunması, güvenlik yönetimini karmaşıktırmaktadır. Örneğin, akıllı ev sistemlerinde kullanılan ZigBee cihazları ile endüstriyel IoT (IIoT) sistemlerinde kullanılan Modbus protokolleri, farklı güvenlik gereksinimlerine sahiptir ve bu durum, standart bir güvenlik çerçevesinin uygulanmasını zorlaştırmaktadır. Ayrıca, IoT cihazlarının uzun ömürlü doğası, yazılım güncellemelerinin düzenli uygulanmasını zorlaştırmakta ve eski cihazlar, bilinen güvenlik açıklarına karşı savunmasız kalmaktadır. IoT sistemlerinde güvenlik açıklarını azaltmak için çok katmanlı bir güvenlik yaklaşımı önererek, fiziksel katman, ağ katmanı ve uygulama katmanı için entegre çözümler geliştirmenin gerekliliğini vurgulamıştır.

IoT sistemlerinin güvenliğini tehdit eden bir diğ er  nemli fakt r, veri gizliliđi ve kullanıcı mahremiyetidir. IoT cihazlarından toplanan veriler, genellikle kişisel veya hassas bilgiler i ermekte ve bu verilerin k t  niyetli akt rler tarafından ele ge irilmesi, ciddi etik ve yasal sorunlara yol a maktadır. Avrupa Birliđi'nin Genel Veri Koruma T z đ  (GDPR), IoT verilerinin işlenmesi ve saklanması sıkı kurallar getirmiř ve g venlik a ıklarının kapatılmasını zorunlu kılmıřtır. Ancak, kaynak kısıtlı cihazlarda GDPR uyumlu veri koruma mekanizmalarının uygulanması, teknik ve operasyonel zorluklar yaratmaktadır.

Sonuc olarak, IoT sistemlerinin katmanlı yapısı, esneklik ve  l eklenebilirlik sunarken, algılama, ađ ve uygulama katmanlarında  eřitli g venlik a ıkları barındırmaktadır. Sınırlı kaynaklara sahip cihazlar, kablosuz iletiřim ortamları ve heterojen protokoller, bu a ıkların istismar edilmesini kolaylařtırmaktadır. Hafif řifreleme, donanım tabanlı g venlik mod lleri ve  ok katmanlı savunma mekanizmaları, IoT sistemlerinin güvenliğini artırmayı hedeflemekte; ancak, enerji verimliliđi, maliyet ve uyumluluk gibi zorluklar, bu alanda daha fazla arařtırma gerektirmektedir.

2.2. IoT Sistemlerinde Karřılařılan Bařlıca Tehditler

Nesnelerin İnterneti (IoT) sistemleri, fiziksel cihazların internet  zerinden birbirleriyle iletiřim kurmasını sađlayarak yařamın bir ok alanında yenilik i   z mler sunmaktadır. Ancak, bu sistemlerin heterojen yapısı, sınırlı kaynaklara sahip cihazları ve kablosuz iletiřim ortamları, onları  eřitli siber tehditlere karřı savunmasız kılmaktadır. IoT sistemlerinde karřılařılan tehditler, hem cihaz hem de ađ hem de veri d zeyinde ciddi etkiler yaratmakta; bu nedenle, bu tehditlerin detaylı bir řekilde anlařılması, g venlik  nlemlerinin geliřtirilmesi i in kritik bir  neme sahiptir. Bu b l m, IoT sistemlerinde karřılařılan bařlıca tehditleri, bunların IoT ekosistemine etkilerini ve  rnek senaryolarını ayrıntılı olarak incelemektedir.

2.2.1. Fiziksel Tehditler

IoT cihazlarının fiziksel eriřime a ık olması, bu sistemlerin en temel tehditlerinden birini oluřtırmaktadır. Akıllı ev sistemleri, sens r d đ mleri veya end striyel IoT (IIoT) cihazları gibi bir ok IoT cihazı, genellikle korumasız ortamlarda bulunmakta ve fiziksel sabotaja karřı savunmasız kalmaktadır.  rneđin,

kötü niyetli bir aktör, bir IoT cihazına fiziksel erişim sağlayarak donanımına müdahale edebilir, kötü amaçlı yazılım enjekte edebilir veya cihazın sensör verilerini manipüle edebilir. Bu tür tehditler, özellikle kritik altyapılarda (örneğin, enerji şebekeleri, sağlık sistemleri) ciddi sonuçlar doğurmaktadır. Yapılan çalışmalar, fiziksel tehditlerin, IoT cihazlarının %30'undan fazlasında güvenlik açıklarına yol açabileceğini ortaya koymuştur.

2.2.2. Ağ Tabanlı Tehditler

IoT sistemlerinin ağ katmanı, siber tehditlerin en yoğun şekilde hedef aldığı bir bileşenidir. Kablosuz iletişim protokolleri (örneğin, ZigBee, 6LoWPAN, Wi-Fi) ve yönlendirme mekanizmaları (örneğin, RPL), veri ağları (eavesdropping), sahte düğüm enjeksiyonu ve yönlendirme saldırıları gibi tehditlere karşı hassastır.

2.2.2.1. Blackhole Saldırısı

Kötü niyetli bir düğüm, sahte rank değerleri ile kendini en iyi yönlendirme yolu olarak tanıtmakta ve gelen veri paketlerini düşürmektedir. Bu saldırı, RPL tabanlı IoT ağlarında veri kaybına ve iletişim kopukluklarına yol açmaktadır (Raoof vd., 2018).

2.2.2.2. HelloFlood Saldırısı

Saldırgan, yüksek güçlü “hello” mesajları (DIS) yayarak diğer düğümleri komşu olduğuna inandırmakta ve ağ topolojisini bozmaktadır. Bu, ağda aşırı kontrol mesajı trafiği ve enerji tüketimi artışı yaratmaktadır (Raza, S., Wallgren, L., Voigt, T. 2013).

2.2.2.3. Version Number Saldırısı

Saldırgan, RPL'nin DODAG sürüm numarasını manipüle ederek ağın sürekli yeniden yapılandırılmasını tetiklemekte ve yönlendirme kararlarını kararsızlaştırmaktadır (Mayzaud, A., Badonnel, R., Chrisment, I. 2016).

2.2.2.4. DDoS (Distributed Denial of Service) Saldırısı

Çok sayıda IoT cihazının ele geçirilerek bir hedef sunucuya aşırı trafik gönderilmesiyle gerçekleştirilmektedir. 2016'daki Mirai botnet saldırısı, zayıf parolalara sahip IoT cihazlarının ele geçirilerek DDoS saldırılarında kullanıldığını göstermiştir (Kolias, C., Kambourakis, G., Stavrou, A., Voas, J. 2017).

2.2.2.5. Sinkhole Saldırısı

Saldırgan, sahte bir kök düğüm gibi davranarak ağ trafiğini kendisine yönlendirmekte ve genellikle Blackhole veya veri ağları ile birleştirilerek ağın işlevselliğini bozmaktadır (Raza vd., 2013).

Bu tehditler, IoT ağlarının güvenilirliğini ve hizmet sürekliliğini doğrudan tehdit etmekte; özellikle RPL tabanlı ağlarda, yönlendirme mekanizmalarının tasarım zayıflıkları nedeniyle daha yıkıcı etkiler yaratmaktadır.

2.2.3. Veri Tabanlı Tehditler

IoT sistemlerinde veri, sistemin en değerli varlığıdır ve veri gizliliği, bütünlüğü ve erişilebilirliği, güvenlik açısından kritik öneme sahiptir. Veri tabanlı tehditler, genellikle veri ağları, manipülasyon ve yetkisiz erişim gibi yöntemlerle gerçekleştirilmektedir.

2.2.3.1. Veri Ağı (Eavesdropping)

Kablosuz iletişim ortamlarında, şifrelenmemiş veri paketlerinin kötü niyetli aktörler tarafından ele geçirilmesiyle gerçekleşmektedir. IoT cihazlarının sınırlı kaynakları, güçlü şifreleme algoritmalarının uygulanmasını zorlaştırmakta ve bu durum, veri gizliliğini riske atmaktadır.

2.2.3.2. Veri Manipülasyonu

Saldırgan, sensör verilerini veya protokol mesajlarını değiştirerek sistemin yanlış kararlar almasına neden olmaktadır. Örneğin, bir akıllı termostatin sıcaklık verilerinin manipüle edilmesi, enerji israfına veya sistem arızalarına yol açabilir (Safaei, B., Monazzah, A. M. H., Bafroei, M. B., Ejlali, A. 2017, December).

2.2.3.3. Yetkisiz Erişim

Zayıf kimlik doğrulama mekanizmaları veya varsayılan parolalar, kötü niyetli kullanıcıların IoT sistemlerine erişmesine olanak tanımaktadır. Bu, özellikle bulut tabanlı IoT servislerinde veri ihlallerine yol açmaktadır (Khan, M. A., Salah, K. 2018).

Veri tabanlı tehditler, IoT sistemlerinin güvenilirliğini ve kullanıcı mahremiyetini tehdit etmekte; özellikle sağlık, finans ve akıllı şehir uygulamalarında ciddi etik ve yasal sorunlara neden olmaktadır.

2.2.4. Yazılım ve Firmware Tehditleri

IoT cihazlarının yazılımları ve donanım yazılımları (firmware), güvenlik açıklarının sıkça istismar edildiği bir diğer alandır. Zayıf yazılım tasarımı, güncellenmeyen firmware veya bilinen açıkların yamalanmaması, cihazların ele geçirilmesine olanak tanımaktadır. Örneğin, Mirai botnet, varsayılan parolalara sahip IoT cihazlarının firmware açıklarını istismar ederek milyonlarca cihazı ele geçirmiştir (Kolias, C., Kambourakis, G., Stavrou, A., Voas, J. 2017). Ayrıca, kötü amaçlı yazılım (malware) enjeksiyonu, IoT cihazlarının botnet ağlarına katılmasını veya hassas verilerin çalınmasını sağlamaktadır. Li ve diğerleri (2022), IoT cihazlarının %40'ından fazlasının bilinen yazılım açıklarına sahip olduğunu ve düzenli güncellemelerin uygulanmamasının bu tehditleri artırdığını rapor etmiştir.

2.2.5. Sosyal Mühendislik ve Kullanıcı Tabanlı Tehditler

IoT sistemlerinde kullanıcılar, güvenlik zincirinin en zayıf halkalarından birini oluşturmaktadır. Sosyal mühendislik saldırıları, kullanıcıları kandırarak IoT cihazlarına veya ağlarına erişim sağlamayı hedeflemektedir. Örneğin, kimlik avı (phishing) e-postaları aracılığıyla kullanıcıların parolalarını ele geçiren saldırganlar, akıllı ev sistemlerine yetkisiz erişim sağlayabilmektedir (Sicari, S., Rizzardi, A., Grieco, L. A., Coen-Porisini, A. 2015). Ayrıca, kullanıcıların güvenlik farkındalığının düşük olması, varsayılan parolaların değiştirilmemesi veya zayıf parolaların kullanılması gibi hatalara yol açmaktadır. Bu tür tehditler, teknik güvenlik açıklarıyla birleştiğinde, IoT sistemlerinin savunmasızlığını artırmaktadır.

2.2.6. Kritik Altyapılara Yönelik Tehditler

IoT sistemlerinin kritik altyapılarda (örneğin, enerji şebekeleri, ulaşım sistemleri, sağlık hizmetleri) yaygın kullanımı, bu sistemleri hedef alan tehditlerin yıkıcı etkilerini artırmaktadır. Örneğin, bir akıllı şebeke sistemine yönelik bir DDoS saldırısı, enerji dağıtımını kesintiye uğratabilir veya bir sağlık IoT cihazının (örneğin, insülin pompası) manipülasyonu, hayati riskler doğurabilir (Khan, M. A., Salah, K.

2018). Bu tür tehditler, hem ekonomik hem de toplumsal açıdan ciddi sonuçlar yaratmakta ve IoT sistemlerinin güvenliğinin çok katmanlı bir şekilde ele alınmasını zorunlu kılmaktadır.

IoT sistemlerinde karşılaşılan tehditler, fiziksel, ağ, veri, yazılım, kullanıcı ve kritik altyapı düzeylerinde çeşitlilik göstermektedir. Blackhole, HelloFlood, DDoS gibi ağ tabanlı saldırılar, RPL tabanlı ağların yönlendirme mekanizmalarını hedef alırken; veri ağları, manipülasyon ve yetkisiz erişim gibi tehditler, sistemin gizliliğini ve bütünlüğünü tehdit etmektedir. Bu tehditlerin çok boyutlu doğası, IoT sistemlerinin güvenliğini artırmak için kapsamlı ve entegre savunma mekanizmalarının geliştirilmesini gerektirmektedir.

2.3. Güvenlik Önlemleri ve Savunma Mekanizmaları

Nesnelerin İnterneti (IoT) sistemlerinin yaygınlaşması, bu sistemlerin siber tehditlere karşı korunmasını zorunlu kılmaktadır. IoT ağlarının heterojen yapısı, sınırlı kaynaklara sahip cihazları ve kablosuz iletişim ortamları, geleneksel güvenlik mekanizmalarının uygulanmasını zorlaştırmakta; bu nedenle, IoT'ya özgü hafif, enerji verimli ve ölçeklenebilir savunma mekanizmaları geliştirilmektedir. Bu mekanizmalar, fiziksel katman, ağ katmanı ve uygulama katmanı düzeylerinde tehditlere karşı koruma sağlamayı hedeflemektedir. Bu bölüm, IoT sistemlerinde kullanılan başlıca güvenlik önlemlerini ve savunma mekanizmalarını detaylı bir şekilde incelemektedir.

2.3.1. Fiziksel Katman Güvenlik Önlemleri

IoT cihazlarının fiziksel erişime açık olması, donanım sabotajı ve kötü amaçlı kod enjeksiyonu gibi tehditleri beraberinde getirmektedir. Fiziksel katman güvenliğini artırmak için çeşitli önlemler uygulanmaktadır.

2.3.1.1. Donanım Tabanlı Güvenlik Modülleri

Trusted Platform Module (TPM) gibi donanım tabanlı güvenlik çözümleri, cihazların kimlik doğrulamasını ve veri şifrelemesini desteklemektedir. Bu modüller, fiziksel müdahalelere karşı cihazın bütünlüğünü korumakta ve kötü amaçlı yazılımlara karşı direnç sağlamaktadır (Sicari vd., 2015). Ancak, bu çözümlerin maliyeti, düşük bütçeli IoT cihazlarında uygulanabilirliğini sınırlamaktadır.

2.3.1.2. Fiziksel Eriřim Kontrolleri

IoT cihazlarının fiziksel olarak güvenli ortamlarda (örneğin, kilitli muhafazalar) bulundurulması, sabotaj riskini azaltmaktadır. Ayrıca, sensör tabanlı izleme sistemleri, cihazlara yetkisiz erişimi tespit etmek için kullanılmaktadır (Pundir, S., Wazid, M., Singh, D. P., Das, A. K., Rodrigues, J. J., Park, Y. 2019).

2.3.1.3. Anti-Tamper Mekanizmaları

Cihazların fiziksel müdahale durumunda kendi kendini devre dışı bırakması veya verilerini silmesi, hassas bilgilerin korunmasını sağlamaktadır. Bu yöntem, özellikle kritik altyapılarda kullanılan IoT cihazlarında tercih edilmektedir.

2.3.2. Ağ Katmanı Güvenlik Önlemleri

Ağ katmanı, IoT sistemlerinde Blackhole, HelloFlood, DDoS gibi yönlendirme ve trafik tabanlı tehditlerin hedef aldığı bir bileşendir. RPL tabanlı ağlarda, ağ katmanı güvenliğini artırmak için savunma mekanizmaları geliştirilmektedir.

2.3.2.1. Hafif Şifreleme ve Kimlik Doğrulama

Kaynak kısıtlı IoT cihazlarında, AES (Advanced Encryption Standard) tabanlı hafif şifreleme algoritmaları ve eliptik eğri kriptografisi (ECC) kullanılmaktadır. Bu yöntemler, veri gizliliğini ve bütünlüğünü korurken enerji tüketimini minimumda tutmaktadır (Pundir, S., Wazid, M., Singh, D. P., Das, A. K., Rodrigues, J. J., Park, Y. 2019). Örneğin, RPL kontrol mesajlarının (DIO, DAO) şifrenmesi, sahte mesajların tespitini kolaylaştırmaktadır (Raza vd., 2013).

2.3.2.2. Güvenli Yönlendirme Mekanizmaları

RPL protokolünde güvenli ebeveyn seçimi algoritmaları, sahte rank değerlerine karşı koruma sağlamaktadır. SVELTE sistemi, RPL tabanlı ağlarda anomali tespiti yaparak Blackhole ve Sinkhole gibi saldırıları gerçek zamanlı olarak belirlemektedir (Raza vd., 2013). Ayrıca, yönlendirme mesajlarının dijital imzalarla doğrulanması, Version Number saldırılarını önlemektedir.

2.3.2.3. Ağ Tabanlı Anomali Tespiti

Makine öğrenmesi tabanlı sistemler, ağ trafiğindeki anormal davranışları (örneğin, aşırı DIS mesajları) izlemekte ve HelloFlood gibi tehditleri tespit etmektedir. XGBoost ve LightGBM gibi algoritmalar, düşük hesaplama maliyetiyle %98 doğruluk sunmaktadır (Raghavendra, T., Anand, M., Selvi, M., Thangaramya, K., Kumar, S. S., Kannan, A. 2022).

2.3.2.4. Ağ İzolasyonu ve Segmentasyonu

5G tabanlı IoT ağlarında ağ dilimleme (network slicing), farklı cihaz gruplarını izole ederek saldırıların yayılmasını sınırlamaktadır. Bu yöntem, DDoS saldırılarının etkisini azaltmakta ve ağın hizmet sürekliliğini korumaktadır (Khan, M. A., Salah, K. 2018).

2.3.3. Uygulama Katmanı Güvenlik Önlemleri

Uygulama katmanı, veri işleme, bulut servisleri ve kullanıcı arayüzleriyle ilişkili tehditlere karşı koruma sağlamayı hedeflemektedir.

2.3.3.1. Güçlü Kimlik Doğrulama ve Yetkilendirme

Çok faktörlü kimlik doğrulama (MFA) ve OAuth tabanlı yetkilendirme, yetkisiz erişim riskini azaltmaktadır. Örneğin, IoT cihazlarının bulut servislerine erişimi, dinamik token'larla doğrulanmaktadır (Li, S., Iqbal, M., Saxena, N. 2024).

2.3.3.2. Veri Şifreleme ve Gizlilik

Uçtan uca şifreleme (end-to-end encryption), IoT cihazlarından buluta aktarılan verilerin gizliliğini korumaktadır. Ayrıca, homomorfik şifreleme, verilerin şifreli halde işlenmesini sağlayarak gizlilik ihlallerini önlemektedir (Li, S., Da Xu, L., Zhao, S. 2018).

2.3.3.3. Yazılım ve Firmware Güncellemeleri

IoT cihazlarının düzenli olarak güncellenmesi, bilinen güvenlik açıklarının kapatılmasını sağlamaktadır. Ancak, kaynak kısıtlı cihazlarda güncelleme süreçlerinin enerji verimli bir şekilde yönetilmesi gerekmektedir (Kolias, C., Kambourakis, G., Stavrou, A., Voas, J. 2017).

2.3.3.4. Uygulama Tabanlı Anomali Tespiti

Derin öğrenme modelleri (örneğin, LSTM, BiLSTM), uygulama katmanındaki anormal davranışları (örneğin, yetkisiz API çağrıları) tespit etmektedir. Bu modeller, sıfır-gün tehditlerine karşı proaktif koruma sağlamaktadır (Hussain, F., Abbas, S. G., Shah, G. A., Pires, I. M., Fayyaz, U. U., Shahzad, F., Garcia, N. M., Zdravevski, E. 2021).

2.3.4. Veri Gizliliği ve Mahremiyet Önlemleri

IoT sistemlerinde veri gizliliği, kullanıcı mahremiyetini korumak ve yasal düzenlemelere (örneğin, GDPR) uyum sağlamak için kritik bir öneme sahiptir.

2.3.4.1. Veri Anonimleştirme

IoT cihazlarından toplanan verilerin kişisel tanımlayıcı bilgilerden arındırılması, gizlilik ihlallerini önlemektedir. Diferansiyel gizlilik (differential privacy) teknikleri, veri analizinde mahremiyeti korumak için kullanılmaktadır (Voigt ve Von dem Bussche, 2017).

2.3.4.2. Blockchain Tabanlı Çözümler

Blockchain, IoT cihazları arasında merkezi olmayan veri paylaşımı ve kimlik doğrulama sağlayarak veri bütünlüğünü ve güvenilirliğini artırmaktadır. Örneğin, akıllı sözleşmeler, veri erişim yetkilerini otomatik olarak yönetmektedir (Li, S., Iqbal, M., Saxena, N. 2024).

2.3.4.3. Federated Learning

Merkezi veri paylaşımı olmadan yerel cihazlarda model eğitimi gerçekleştiren federated learning, veri gizliliğini korurken saldırı tespit modellerinin geliştirilmesini sağlamaktadır. Bu yöntem, RPL tabanlı ağlarda %97 doğrulukla tehdit tespiti sunmaktadır (Sharma, H., Yadav, G. S. 2025).

2.3.5. Kritik Altyapılar için Özel Önlemler

IoT sistemlerinin enerji şebekeleri, sağlık sistemleri ve ulaşım gibi kritik altyapılarda kullanımı, özel güvenlik önlemlerini gerektirmektedir.

2.3.5.1. Yedekleme ve Felaket Kurtarma Sistemleri

Kritik IoT sistemlerinde, saldırı veya arıza durumunda hizmet sürekliliğini sağlamak için yedekleme sistemleri kullanılmaktadır (Khan, M. A., Salah, K. 2018).

2.3.5.2. Sızma Testleri ve Güvenlik Denetimleri

Kritik altyapılardaki IoT sistemlerinin düzenli olarak sızma testlerine tabi tutulması, güvenlik açıklarının tespitini ve kapatılmasını sağlamaktadır (Li, S., Da Xu, L., Zhao, S. 2018).

2.3.5.3. Siber-Fiziksel Sistem Entegrasyonu

IoT cihazlarının fiziksel süreçlerle (örneğin, enerji dağıtımı) entegrasyonu, siber-fiziksel güvenlik mekanizmalarını gerektirmektedir. Bu, hem siber hem de fiziksel tehditlere karşı bütüncül bir koruma sağlamaktadır (Sicari vd., 2015).

2.3.6. Kullanıcı Farkındalığı ve Eğitim

IoT sistemlerinin güvenliğinde kullanıcılar, önemli bir rol oynamaktadır. Sosyal mühendislik ve zayıf parola kullanımı gibi tehditleri azaltmak için aşağıdaki önlemler alınmaktadır:

2.3.6.1. Kullanıcı Eğitimi

Kullanıcılara, kimlik avı (phishing) saldırılarından korunma ve güçlü parola oluşturma konusunda eğitim verilmektedir. Bu, IoT sistemlerinin güvenliğini artırmada etkili bir yöntemdir (Pundir, S., Wazid, M., Singh, D. P., Das, A. K., Rodrigues, J. J., Park, Y. 2019).

2.3.6.2. Varsayılan Parola Değişikliği

IoT cihazlarının ilk kurulumunda varsayılan parolaların değiştirilmesi zorunlu kılınmaktadır. Bu, Mirai botnet gibi tehditlerin önlenmesinde kritik bir adımdır (Kolias, C., Kambourakis, G., Stavrou, A., Voas, J. 2017).

Sonuç olarak, IoT sistemlerinde güvenlik önlemleri ve savunma mekanizmaları, fiziksel, ağ, uygulama ve veri katmanlarında çok boyutlu bir yaklaşım gerektirmektedir. Hafif şifreleme, makine öğrenmesi tabanlı anomali tespiti, blockchain ve federated learning gibi yenilikçi çözümler, IoT ağlarının güvenliğini

artırmakta; ancak, kaynak kısıtlamaları, heterojen yapılar ve gerçek zamanlı işlem gereksinimleri, bu mekanizmaların optimizasyonunu zorunlu kılmaktadır. Kritik altyapılarda ve kullanıcı odaklı senaryolarda, entegre ve proaktif savunma stratejileri, IoT ekosisteminin güvenilirliğini ve sürdürülebilirliğini desteklemektedir.

2.4. Güncel Yaklaşımlar ve Geleceğe Yönelik Stratejiler

Nesnelerin İnterneti (IoT) sistemlerinin hızla yaygınlaşması, bu sistemlerin güvenliğini artırmak için yenilikçi yaklaşımların ve uzun vadeli stratejilerin geliştirilmesini zorunlu kılmaktadır. IoT ağlarının heterojen yapısı, sınırlı kaynaklara sahip cihazları ve 5G gibi yeni nesil iletişim teknolojilerinin entegrasyonu, mevcut güvenlik çözümlerinin ötesinde daha dinamik ve ölçeklenebilir yaklaşımlar gerektirmektedir. Güncel yaklaşımlar, makine öğrenmesi, blockchain, kenar hesaplama ve federated learning gibi teknolojilere odaklanırken, geleceğe yönelik stratejiler, IoT ekosisteminin sürdürülebilirliğini ve güvenliğini artırmayı hedeflemektedir. Bu bölüm, IoT güvenliğindeki güncel yaklaşımları ve gelecekteki stratejileri detaylı bir şekilde incelemektedir.

2.4.1. Makine Öğrenmesi ve Derin Öğrenme Tabanlı Yaklaşımlar

Makine öğrenmesi ve derin öğrenme, IoT ağlarında siber tehditlerin otomatik tespiti ve önlenmesi için en etkili güncel yaklaşımlardan biridir. Özellikle RPL (Routing Protocol for Low-Power and Lossy Networks) tabanlı IoT ağlarında Blackhole, HelloFlood ve Version Number gibi saldırılar, ağ trafiğinde spesifik anomaliler yaratmakta ve bu anomaliler, makine öğrenmesi modelleriyle yüksek doğrulukla tespit edilmektedir. Örneğin, BiLSTM (Bidirectional Long Short-Term Memory) modelleri, zamansal ve çift yönlü veri örüntülerini analiz ederek Version Number saldırılarını %99 doğrulukla tespit etmiştir (Hussain, F., Abbas, S. G., Shah, G. A., Pires, I. M., Fayyaz, U. U., Shahzad, F., Garcia, N. M., Zdravevski, E. 2021). XGBoost ve LightGBM gibi gradyan artırma algoritmaları ise, düşük hesaplama maliyetiyle gerçek zamanlı tehdit tespiti sağlamak ve kaynak kısıtlı IoT cihazları için uygunluk göstermektedir (Raghavendra, T., Anand, M., Selvi, M., Thangaramya, K., Kumar, S. S., Kannan, A. 2022).

Derin öğrenme modellerinin hesaplama karmaşıklığı, IoT cihazlarında uygulanabilirliklerini sınırlamakta; bu nedenle, hafif modellerin geliştirilmesi güncel

bir araştırma alanıdır. Örneğin, sıkıştırılmış sinir ağları (pruned neural networks), hesaplama yükünü %50'ye kadar azaltarak IoT cihazlarında derin öğrenme uygulamalarını mümkün kılmaktadır (Careem, R., Johar, G., Khatibi, A. 2024). Ayrıca, otomatik makine öğrenmesi (AutoML) teknikleri, model seçimi ve hiperparametre optimizasyonunu otomatikleştirerek IoT güvenliğinde model geliştirme süreçlerini hızlandırmaktadır (Alrowais, F. M., Althahabi, S., Alotaibi, S. S., Mohamed, A., Hamza, M. A., Marzouk, R. 2023). Gelecekte, makine öğrenmesi modellerinin enerji verimliliği ve sıfır-gün tehditlerine karşı proaktif savunma kapasitesi, IoT güvenliğinin temel taşlarından biri olacaktır.

2.4.2. Blockchain Tabanlı Güvenlik Çözümleri

Blockchain teknolojisi, IoT sistemlerinde merkezi olmayan veri paylaşımı, kimlik doğrulama ve veri bütünlüğü sağlamak için yenilikçi bir çözüm sunmaktadır. IoT cihazlarının heterojen yapısı, merkezi güvenlik sistemlerinin uygulanmasını zorlaştırmakta; blockchain ise, dağıtık defter teknolojisiyle güvenilir bir ekosistem oluşturmaktadır. Örneğin, akıllı sözleşmeler (smart contracts), IoT cihazları arasında veri erişim yetkilerini otomatik olarak yönetmekte ve yetkisiz erişimi önlemektedir (Li, S., Iqbal, M., Saxena, N. 2024). Ayrıca, blockchain tabanlı kimlik doğrulama sistemleri, sahte düğüm enjeksiyonu gibi tehditlere karşı koruma sağlamaktadır.

Blockchain'in IoT güvenliğindeki uygulamaları, özellikle endüstriyel IoT (IIoT) ve akıllı şehir senaryolarında yaygınlaşmaktadır. Ancak, blockchain'in yüksek hesaplama ve enerji gereksinimleri, kaynak kısıtlı cihazlarda uygulanabilirliğini sınırlamaktadır. Bu sorunu çözmek için, hafif blockchain protokolleri (örneğin, IOTA Tangle) geliştirilmekte ve bu protokoller, IoT cihazlarının düşük güç tüketimiyle güvenli veri paylaşımı yapmasını sağlamaktadır (Pundir, S., Wazid, M., Singh, D. P., Das, A. K., Rodrigues, J. J., Park, Y. 2019). Gelecekte, blockchain'in IoT güvenliğindeki rolü, enerji verimli algoritmalar ve ölçeklenebilir konsensüs mekanizmalarıyla güçlenecektir.

2.4.3. Kenar Hesaplama ve Fog Computing

Kenar hesaplama (edge computing) ve fog computing, IoT ağlarında veri işlemenin merkezi sunucular yerine ağ kenarında veya ara katmanlarda gerçekleştirilmesini sağlayarak hem gecikmeyi azaltmakta hem de enerji verimliliğini

artırmaktadır. Geleneksel bulut tabanlı sistemler, yüksek veri hacmi ve gerçek zamanlı işlem gereksinimleriyle başa çıkmakta zorlanmakta; kenar hesaplama ise, veri analitiğini cihazlara yakın bir şekilde gerçekleştirerek bu sorunları çözmektedir (Shahid, M. H., Hameed, A. R., ul Islam, S., Khattak, H. A., Din, I. U., Rodrigues, J. J. 2020). Örneğin, kenar düğümleri, RPL tabanlı ağlarda Blackhole saldırılarını yerel olarak tespit ederek ağın merkezi yükünü azaltmaktadır (Raghavendra, T., Anand, M., Selvi, M., Thangaramya, K., Kumar, S. S., Kannan, A. 2022).

Kenar hesaplama, makine öğrenmesi modellerinin IoT cihazlarına entegre edilmesini kolaylaştırmakta ve gerçek zamanlı tehdit tespiti sağlamaktadır. Ancak, kenar düğümlerinin sınırlı işlem kapasitesi ve heterojen yapısı, bu sistemlerin güvenliğini zorlaştırmaktadır. Bu sorunu çözmek için, kenar tabanlı anomali tespit sistemleri ve güvenli iletişim protokolleri geliştirilmektedir (Li, S., Da Xu, L., Zhao, S. 2018). Gelecekte, kenar hesaplama, 5G entegrasyonu ile birlikte IoT ağlarının güvenilirliğini ve ölçeklenebilirliğini artıracaktır.

2.4.4. Federated Learning ve Gizlilik Odaklı Yaklaşımlar

Federated learning, IoT ağlarında veri gizliliğini korurken makine öğrenmesi modellerinin eğitimini mümkün kılan bir yaklaşımdır. Bu yöntem, merkezi bir sunucuya veri aktarmadan, yerel cihazlarda model eğitimi gerçekleştirerek hem gizliliği korumakta hem de iletişim maliyetlerini azaltmaktadır. Nguyen ve diğerleri (2022), federated learning tabanlı bir sistemin, RPL tabanlı ağlarda Blackhole saldırılarını %97 doğrulukla tespit ettiğini ve merkezi modellere kıyasla %30 daha az enerji tükettiğini rapor etmiştir. Federated learning, özellikle sağlık ve akıllı şehir gibi hassas veri içeren IoT uygulamalarında yaygınlaşmaktadır.

Federated learning'in IoT güvenliğindeki zorlukları, heterojen cihazlar arasındaki senkronizasyon ve model güncelleme süreçlerinin karmaşıklığıdır. Bu sorunları çözmek için, hafif federated learning algoritmaları ve asenkron güncelleme mekanizmaları geliştirilmektedir (Sharma, H., Yadav, G. S. 2025). Gelecekte, federated learning, IoT ağlarında veri gizliliği ve enerji verimliliği açısından kritik bir rol oynayacaktır.

2.4.5. 5G Entegrasyonu ve Güvenlik Stratejileri

5G teknolojinin IoT ağlarına entegrasyonu, yüksek veri hızları, düşük gecikme süreleri ve büyük ölçekli cihaz bağlantısı sunarak IoT uygulamalarının kapsamını genişletmektedir. Ancak, 5G'nin karmaşık mimarisi, ağ dilimleme (network slicing) ve çoklu erişim kenar hesaplama (MEC) gibi teknolojiler, yeni güvenlik tehditleri yaratmaktadır. Örneğin, ağ dilimleme, farklı IoT uygulamalarını izole etse de, dilimleme yönetim sistemlerinin güvenliği sağlanmazsa, çapraz dilim saldırıları mümkün olmaktadır (Khan, M. A., Salah, K. 2018). Bu tehditlere karşı, 5G tabanlı IoT ağlarında çok katmanlı güvenlik çerçeveleri geliştirilmektedir. Li ve diğerleri (2022), fiziksel katman güvenliği, ağ katmanı protokol optimizasyonları ve uygulama katmanı veri gizliliği gibi unsurları entegre eden bir çerçeve önermiştir.

5G entegrasyonu, IoT güvenliğinde dinamik kaynak tahsisi ve gerçek zamanlı tehdit tespiti gibi yenilikçi stratejileri desteklemektedir. Gelecekte, 5G tabanlı IoT ağlarının güvenliği, yapay zeka destekli savunma sistemleri ve sıfır-güven (zero-trust) mimarileriyle güçlenecektir.

2.4.6. Sıfır-Güven Mimarileri ve Proaktif Güvenlik

Sıfır-güven (zero-trust) mimarileri, IoT ağlarında tüm cihazların ve kullanıcıların sürekli olarak doğrulanmasını gerektiren bir güvenlik yaklaşımıdır. Bu yaklaşım, varsayılan güven yerine sürekli izleme ve kimlik doğrulama prensiplerine dayanmaktadır. Örneğin, IoT cihazlarının her veri aktarımı öncesi kimlik doğrulaması, yetkisiz erişim ve sahte düğüm enjeksiyonu gibi tehditleri önlemektedir (Li, S., Iqbal, M., Saxena, N. 2024). Sıfır-güven mimarileri, özellikle kritik altyapılarda (örneğin, enerji şebekeleri, sağlık sistemleri) IoT güvenliğini artırmaktadır.

Proaktif güvenlik stratejileri, tehditlerin gerçekleşmeden önce tespit edilmesini ve önlenmesini hedeflemektedir. Örneğin, yapay zeka tabanlı tehdit avcılığı (threat hunting) sistemleri, IoT ağlarında potansiyel güvenlik açıklarını analiz ederek sıfır-gün tehditlerine karşı koruma sağlamaktadır (Hussain, F., Abbas, S. G., Shah, G. A., Pires, I. M., Fayyaz, U. U., Shahzad, F., Garcia, N. M., Zdravevski, E. 2021). Gelecekte, sıfır-güven ve proaktif güvenlik yaklaşımları, IoT ağlarının dinamik ve heterojen yapısına uygun olarak geliştirilecektir.

2.4.7. Standartlaşma ve Yasal Düzenlemeler

IoT güvenliğinin sürdürülebilirliği, uluslararası standartlar ve yasal düzenlemelerle desteklenmektedir. Avrupa Birliği'nin Genel Veri Koruma Tüzüğü (GDPR), IoT verilerinin işlenmesi ve saklanması sıkı kuralları getirmekte ve güvenlik açıklarının kapatılmasını zorunlu kılmaktadır (Voigt ve Von dem Bussche, 2017). Ayrıca, IEEE ve IETF gibi kuruluşlar, IoT güvenliği için standart protokoller (örneğin, 6LoWPAN, RPL) ve güvenlik çerçeveleri geliştirmektedir. Ancak, IoT cihazlarının heterojen yapısı, standartlaşmayı zorlaştırmakta ve bu durum, küresel bir güvenlik çerçevesinin oluşturulmasını gerektirmektedir.

Gelecekte, IoT güvenliği için standartlaşma çalışmaları, cihaz sertifikasyonu, güvenlik testleri ve açık kaynaklı güvenlik araçlarının yaygınlaştırılmasına odaklanacaktır. Ayrıca, uluslararası iş birliği, IoT ekosisteminin güvenilirliğini artırmak için kritik bir öneme sahiptir.

Sonuç olarak, IoT güvenliğindeki güncel yaklaşımlar, makine öğrenmesi, blockchain, kenar hesaplama, federated learning ve 5G entegrasyonu gibi teknolojilere dayanmaktadır. Bu yaklaşımlar, IoT ağlarının güvenilirliğini ve ölçeklenebilirliğini artırmakta; ancak, kaynak kısıtlamaları, heterojen yapılar ve sıfır-gün tehditler, optimizasyon gerektirmektedir. Geleceğe yönelik stratejiler, sıfır-güven mimarileri, proaktif güvenlik, standartlaşma ve yasal düzenlemelerle IoT ekosisteminin sürdürülebilirliğini desteklemektedir. Bu stratejiler, IoT güvenliğinin dinamik ve çok katmanlı bir yaklaşımla ele alınmasını zorunlu kılmaktadır.

ÜÇÜNCÜ BÖLÜM

MATERYAL VE METOT

3.1. Kullanılacak Materyaller

Bu çalışma, RPL (Routing Protocol for Low-Power and Lossy Networks) tabanlı Nesnelerin İnterneti (IoT) ağlarında Blackhole, HelloFlood ve Version Number saldırılarının tespit edilmesi ve sınıflandırılmasını amaçlamaktadır. Araştırma kapsamında, simülasyon ortamlarının kurulması, ağ trafiğinin analizi, enerji tüketiminin ölçülmesi ve makine öğrenmesi modellerinin geliştirilmesi için çeşitli yazılım ve donanım materyalleri kullanılmaktadır. Bu bölüm, çalışmada kullanılan materyalleri detaylı bir şekilde açıklamaktadır.

3.1.1. Ubuntu

Ubuntu, Canonical Ltd. tarafından geliştirilen, açık kaynaklı ve Linux tabanlı bir işletim sistemidir. Kullanıcı dostu arayüzü, yüksek özelleştirilebilirliği ve geniş yazılım desteğiyle, IoT sistemlerinin geliştirilmesi, test edilmesi ve analizinde güvenilir bir platform olarak öne çıkmaktadır. Ubuntu, açık kaynaklı yapısıyla topluluk odaklı geliştirme süreçlerini desteklemekte ve düzenli güncellemelerle güvenlik açıklarını kapatmaktadır. Sistem, komut satırı araçları (örneğin, apt paket yöneticisi) ve Python gibi programlama dilleriyle uyumluluğu sayesinde, veri işleme ve simülasyon ortamlarının yönetimini kolaylaştırmaktadır. Ayrıca, sanal makine entegrasyonu ile esnek ve izole bir çalışma ortamı sunmaktadır.

Ubuntu'nun yaygın kullanım alanları, IoT ve IIoT (Endüstriyel IoT) sistemlerinin geliştirilmesi, bulut bilişim, büyük veri analizi ve makine öğrenmesi uygulamalarını kapsamaktadır. IoT geliştirme süreçlerinde, Contiki ve Cooja gibi simülasyon araçlarının çalıştırılması için tercih edilmekte; büyük veri analizinde ise Apache Spark gibi dağıtık işleme çerçevelerine ev sahipliği yapmaktadır. Akademik araştırmalarda, Ubuntu'nun açık kaynaklı doğası ve geniş topluluk desteği, tekrarlanabilir ve erişilebilir deneyler için ideal bir zemin sağlamaktadır. Ayrıca, sunucu yönetimi ve ağ analizlerinde (örneğin, Wireshark kullanımı) sıkça kullanılmaktadır.



Şekil 3.1. Ubuntu arayüzü

Ubuntu, RPL tabanlı IoT ağlarının simülasyonu ve güvenlik analizleri için temel işletim sistemi olarak kullanılmaktadır. Şekil 3.1’de gösterildiği gibi, Contiki 3.0 işletim sisteminin derlenmesi, Cooja simülatörünün çalıştırılması, Wireshark ile ağ trafiği analizi ve LightGBM, XGBoost, LSTM ve BiLSTM gibi makine öğrenmesi modellerinin eğitimi, Ubuntu tabanlı bir sanal makine ortamında gerçekleştirilmiştir.

3.1.2. Contiki

Contiki, düşük güçlü ve kaynak kısıtlı Nesnelerin İnterneti (IoT) cihazları için tasarlanmış, açık kaynaklı bir işletim sistemidir. Hafif yapısı, modüler tasarımı ve enerji verimliliğiyle, sensör düğümleri ve gömülü sistemler için optimize edilmiş bir platform sunmaktadır. Contiki, IPv6 tabanlı iletişim protokollerini (örneğin, 6LoWPAN, RPL) desteklemekte ve olay odaklı programlama modeli sayesinde düşük enerji tüketimiyle veri toplama ve iletim süreçlerini kolaylaştırmaktadır. Ayrıca, açık kaynaklı doğası, geliştiricilerin protokol kodlarını özelleştirmesine ve yeni güvenlik mekanizmalarını entegre etmesine olanak tanımaktadır (Österlind, F., Dunkels, A., Eriksson, J., Finne, N., Voigt, T. 2006).

Contiki'nin yaygın kullanım alanları, IoT ve endüstriyel IoT (IIoT) uygulamalarını kapsamaktadır. Akıllı tarım, çevre izleme, akıllı ev sistemleri ve sağlık sensörleri gibi alanlarda, düşük güçlü cihazların ağ oluşturması ve veri iletimi için tercih edilmektedir. Akademik araştırmalarda, Contiki, IoT ağlarının simülasyonu ve

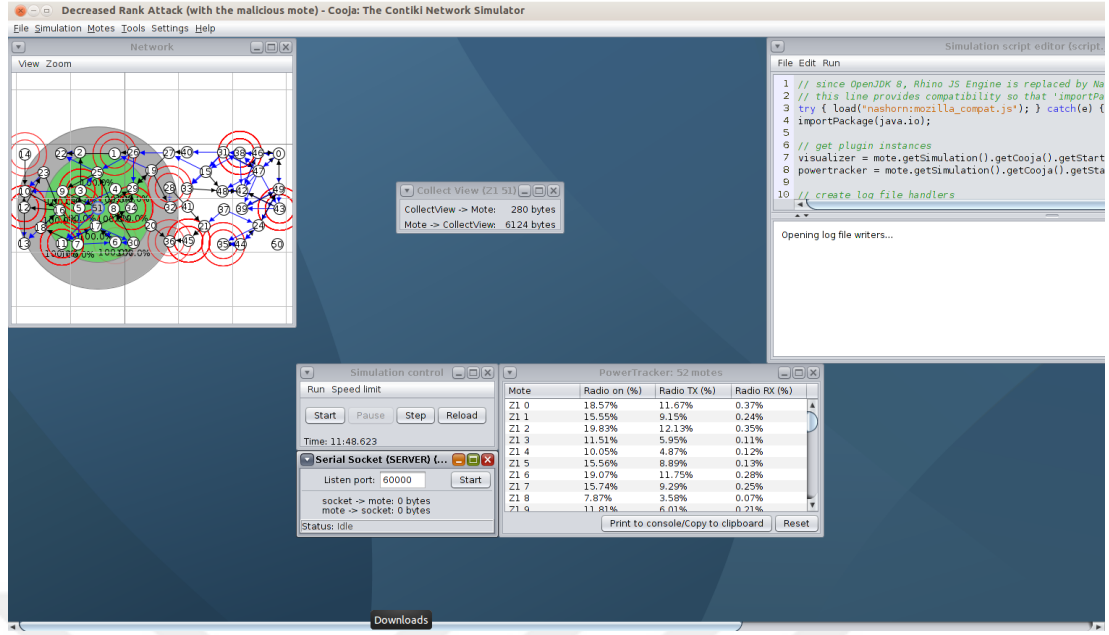
protokol testleri için standart bir platform olarak kullanılmakta; özellikle RPL tabanlı ağların performans ve güvenlik analizlerinde sıkça yer almaktadır. Ayrıca, Cooja simülatörüyle entegrasyonu, gerçekçi ağ modellerinin oluşturulmasını desteklemektedir.

Bu çalışmada, Contiki, RPL tabanlı IoT ağlarının simülasyonu ve Blackhole, HelloFlood ve Version Number saldırılarının modellenmesi için temel işletim sistemi olarak kullanılmaktadır. Cooja simülatöründe düğümlü ağların oluşturulması, RPL protokolünün test edilmesi ve Powertrace ile enerji tüketimi ölçümlerinin yapılması, Contiki tabanlı bir ortamda gerçekleştirilmiştir.

3.1.3. Cooja

Cooja, Contiki işletim sistemiyle entegre çalışan, açık kaynaklı bir ağ simülatörüdür ve Nesnelerin İnterneti (IoT) ağlarının modellenmesi, test edilmesi ve analiz edilmesi için tasarlanmıştır. Hem donanım düzeyinde gerçek cihaz emülasyonu hem de yazılım düzeyinde sanal düğüm simülasyonu yetenekleri sunarak, gerçekçi ağ senaryolarının oluşturulmasını sağlamaktadır. Cooja, IEEE 802.15.4 gibi standartları desteklemekte ve Unit Disk Graph (UDG) gibi radyo modelleriyle ağ topolojilerinin simüle edilmesine olanak tanımaktadır. Grafiksel arayüzü, Destination Oriented Directed Acyclic Graph (DODAG) gibi yapıların görselleştirilmesini ve düğüm davranışlarının gerçek zamanlı izlenmesini kolaylaştırmaktadır (Österlind, F., Dunkels, A., Eriksson, J., Finne, N., Voigt, T. 2006).

Cooja'nın yaygın kullanım alanları, IoT ve endüstriyel IoT (IIoT) ağlarının protokol testi, performans analizi ve güvenlik araştırmalarını kapsamaktadır. Akıllı şehirler, çevre izleme ve kablosuz sensör ağları gibi uygulamalarda, RPL gibi protokollerin davranışlarını değerlendirmek için sıkça kullanılmaktadır. Akademik çalışmalarda, Cooja, ağ trafiği verilerinin toplanması, enerji tüketimi ölçümlerinin yapılması ve siber saldırıların simüle edilmesi için standart bir araç olarak öne çıkmaktadır. Ayrıca, Wireshark ve Foren6 gibi analiz araçlarıyla entegrasyonu, kapsamlı ağ incelemelerini desteklemektedir.



Şekil 3.2. Cooja arayüz

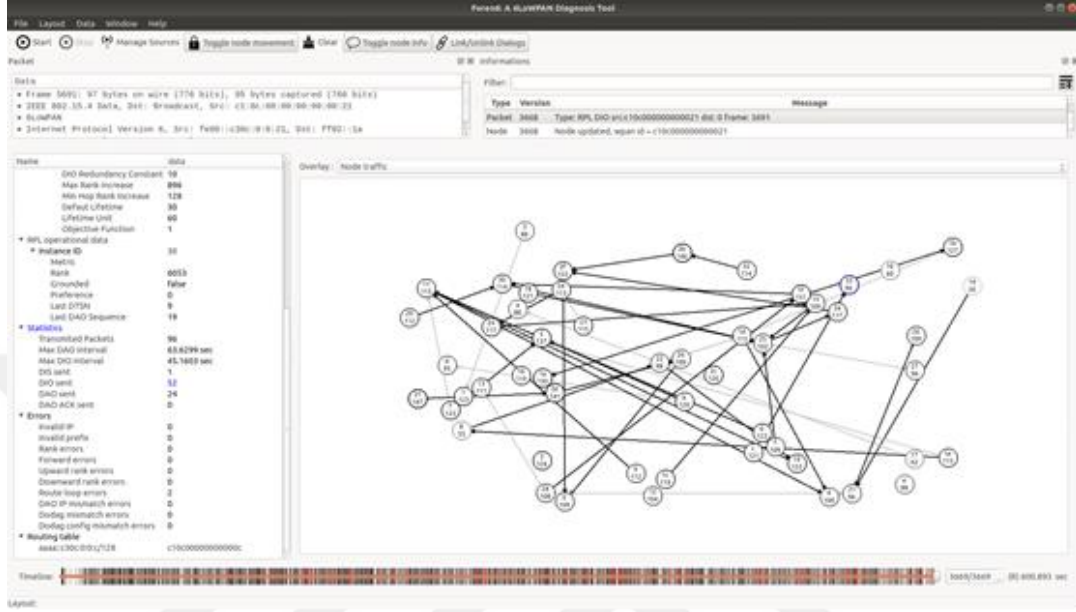
Cooja, RPL tabanlı IoT ağlarının simülasyonu, Blackhole, HelloFlood ve Version Number saldırılarının modellenmesi için kullanılmaktadır. Şekil 3.2’de gösterildiği gibi, düğümlü ağların oluşturulması, RPL protokolünün performansının test edilmesi ve ağ davranışlarının görselleştirilmesi, Cooja simülatörü üzerinden gerçekleştirilmiştir.

3.1.4. Foren6

Foren6, RPL (Routing Protocol for Low-Power and Lossy Networks) tabanlı Nesnelerin İnterneti (IoT) ağlarının görselleştirilmesi ve analizi için geliştirilmiş açık kaynaklı bir ağ teşhis aracıdır. RPL ağlarının Destination Oriented Directed Acyclic Graph (DODAG) yapısını gerçek zamanlı olarak görselleştirerek, yönlendirme dinamiklerini, protokol mesajlarını (DIO, DAO, DIS) ve ağ topolojisindeki değişiklikleri detaylı bir şekilde analiz etmektedir. Foren6, ağdaki anormal davranışları ve saldırı belirtilerini tespit etme yeteneğiyle, IoT güvenliği araştırmalarında önemli bir rol oynamaktadır. Veri çıktısını .csv formatında dışa aktarma özelliği, ileri istatistiksel analizler için esneklik sağlamaktadır (Rodenas-Herráiz, D., Fidler, P. R., Feng, T., Xu, X., Nawaz, S., Soga, K. (2017, February).

Foren6’nın yaygın kullanım alanları, IoT ve endüstriyel IoT (IIoT) ağlarının protokol analizi ve güvenlik testlerini kapsamaktadır. Akıllı şebekeler, çevre izleme sistemleri ve kablosuz sensör ağları gibi uygulamalarda, RPL tabanlı ağların topolojik

davranışlarını incelemek için tercih edilmektedir. Akademik araştırmalarda, Foren6, Blackhole ve HelloFlood gibi saldırıların ağ üzerindeki etkilerini görselleştirmek ve yönlendirme hatalarını analiz etmek için sıkça kullanılmaktadır. Wireshark gibi araçlarla entegrasyonu, ağ trafiği analizini tamamlayıcı bir şekilde desteklemektedir.



Şekil 3.3. Foren6 arayüz

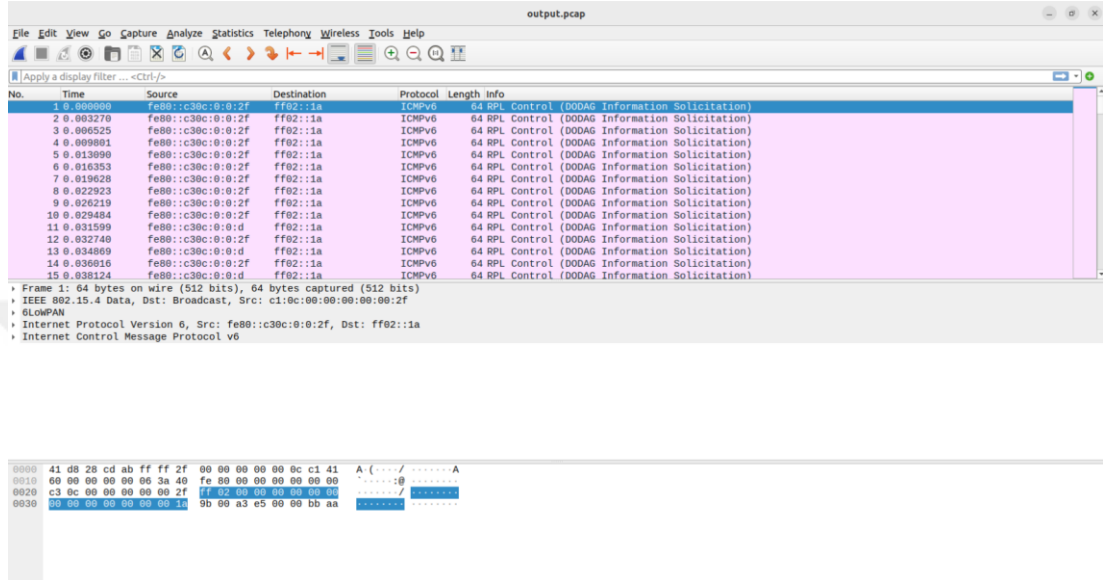
Foren6, RPL tabanlı IoT ağlarının topolojisinin görselleştirilmesi ve Blackhole, HelloFlood ve Version Number saldırılarının ağ üzerindeki topolojik etkilerinin analizi için kullanılmaktadır. Şekil 3.3'te gösterildiği gibi, Cooja simülatöründen elde edilen ağ verilerinin incelenmesi ve DODAG yapısındaki değişikliklerin görselleştirilmesi, Foren6 üzerinden gerçekleştirilmiştir.

3.1.5. Wireshark

Wireshark, ağ trafiğini yakalamak, analiz etmek ve görselleştirmek için geliştirilmiş, açık kaynaklı bir ağ analiz aracıdır. Protokol mesajlarının detaylı incelenmesini sağlayarak, ağ davranışlarını, veri paketlerini ve potansiyel anomalileri izlemektedir. Wireshark, ICMPv6, UDP, TCP gibi protokolleri desteklemekte ve zaman damgalı paket analiziyle ağdaki anormal davranışları tespit etmektedir. Kullanıcı dostu arayüzü ağ güvenliği ve performans analizlerinde etkili bir çözüm sunmaktadır (Sanders, 2011).

Wireshark'ın yaygın kullanım alanları, IoT, endüstriyel IoT (IIoT), kablosuz sensör ağları ve kurumsal ağların analizini kapsamaktadır. IoT sistemlerinde, RPL gibi

protokollerin kontrol mesajlarını (DIO, DAO, DIS) incelemek, DDoS veya Blackhole gibi saldırıların etkilerini değerlendirmek için tercih edilmektedir. Akademik araştırmalarda, ağ trafiği verilerinin toplanması ve protokol düzeyinde tehdit analizleri için standart bir araç olarak kullanılmaktadır. Ayrıca, siber güvenlik eğitimlerinde ve ağ sorun giderme süreçlerinde sıkça yer almaktadır.



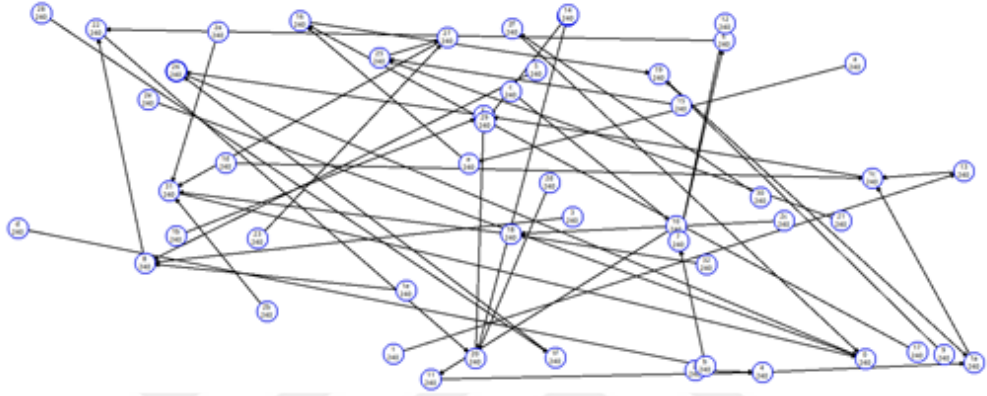
Şekil 3.4. Wireshark arayüz

Wireshark, RPL tabanlı IoT ağlarında Blackhole, HelloFlood ve Version Number saldırılarının ağ trafiği üzerindeki etkilerini analiz etmek ve Cooja simülatöründen elde edilen dosyaları incelemek için kullanılmaktadır. Şekil 3.4'te gösterildiği gibi, bu analizler Wireshark üzerinden gerçekleştirilmiştir.

3.1.6. RPL

RPL (Routing Protocol for Low-Power and Lossy Networks), Nesnelerin İnterneti (IoT) ağlarında düşük güç tüketimi ve kayıplı ağlar için optimize edilmiş, IPv6 tabanlı bir yönlendirme protokolüdür. IETF ROLL çalışma grubu tarafından 2012 yılında standardize edilen RPL, Destination Oriented Directed Acyclic Graph (DODAG) yapısını kullanarak ağ topolojisini düzenlemekte ve enerji tasarrufu sağlayarak veri yönlendirmesini kolaylaştırmaktadır. Objective Function (OF) mekanizmalarıyla düğümlerin ebeveyn seçimini optimize eden RPL, düşük işlem kapasitesine sahip cihazlar için esnek bir çözüm sunmaktadır (Liu, X., Sheng, Z., Yin, C. 2017).

RPL'nin yaygın kullanım alanları, IoT ve endüstriyel IoT (IIoT) uygulamalarını kapsamaktadır. Akıllı şebekeler, çevre izleme, akıllı şehirler ve kablosuz sensör ağları gibi senaryolarda, düşük güçlü cihazların çok atlamalı (multi-hop) iletişim kurmasını sağlamaktadır. Akademik araştırmalarda, RPL, yönlendirme protokollerinin performans analizi, enerji verimliliği ve güvenlik açıklarının incelenmesi için sıkça kullanılmaktadır. 6LoWPAN gibi protokollerle entegrasyonu, RPL'yi IoT ağlarında standart bir bileşen haline getirmektedir.



Şekil 3.5. RPL şeması

RPL, IoT ağlarının yönlendirme protokolü olarak kullanılmakta; Blackhole, HelloFlood ve Version Number saldırılarının simülasyonu ve ağ üzerindeki etkilerinin analizi için temel protokol olarak seçilmiştir. Şekil 3.5'te gösterildiği gibi, bu analizler RPL protokolü temel alınarak gerçekleştirilmiştir.

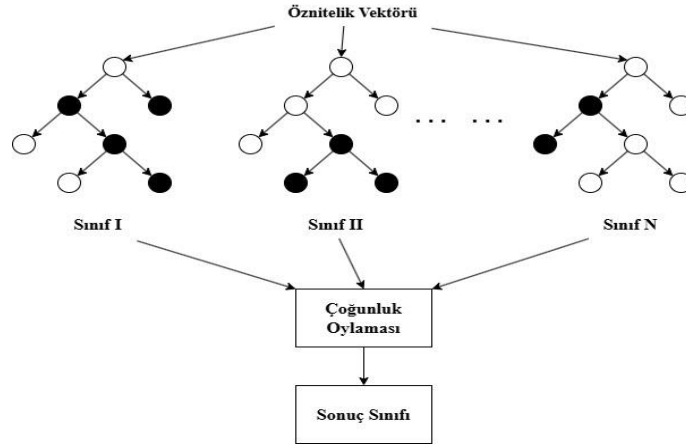
3.1.7. LightGBM

Light Gradient Boosting Machine (LightGBM), Microsoft tarafından geliştirilen, büyük veri setleriyle yüksek öğrenme hızları ve ölçeklenebilirlik için optimize edilmiş açık kaynaklı bir gradyan artırma algoritması kütüphanesidir. Bu algoritma, histogram tabanlı öğrenme yaklaşımıyla geleneksel gradyan artırma yöntemlerinin (örneğin, XGBoost) veri sıralama ve bölme süreçlerini hızlandırarak hesaplama verimliliği sağlamaktadır. LightGBM, karar ağaçlarını yaprak odaklı bir şekilde büyütme stratejisi benimseyerek, her iterasyonda kayıp fonksiyonunun en büyük azalma gösterdiği düğümleri genişletir. Bu süreç, Şekil 3.6'da gösterildiği üzere, birden fazla sınıflandırma ağacını (Sınıf I, Sınıf II, Sınıf N) birleştirir ve her ağacın öz nitelik vektörlerini değerlendiren bir yaprak algoritması kullanır. Her ağaç, eğitim verilerinden gelen öz nitelikler üzerinden dallanarak, çoğunluk oylamasıyla

sonuç sınıfını belirler; bu mekanizma, modelin karmaşıklık ve doğruluk dengesini optimize etmektedir.

LightGBM'nin temel algoritmik özellikleri, histogram tabanlı yaklaşımı ve yaprak odaklı bölme stratejisinden kaynaklanmaktadır. Histogram tabanlı yöntem, sürekli öz nitelik değerlerini belirli aralıklara (kovalara) böler ve bu kovalar üzerinden gradyan ve hessian istatistiklerini hesaplar; bu, veri sıralama işlemine kıyasla hesaplama maliyetini %30-40 oranında azaltmaktadır (Ke, G., Meng, Q., Finley, T., Wang, T., Chen, W., Ma, W., Liu, T. Y. 2017). Yaprak odaklı bölme, geleneksel seviye odaklı (level-wise) büyümeye alternatif olarak, yalnızca en büyük kayıp azalımı sağlayan yaprakları bölerek ağaç derinliğini artırır. Bu strateji, daha derin ve karmaşık ağaçların oluşturulmasını mümkün kılarak, modelin öz nitelik etkileşimlerini daha iyi yakalamasını sağlar. Ayrıca, LightGBM, kategorik özellikleri otomatik olarak işleyebilme yeteneğine sahiptir; bu, önceden sayısal formata dönüştürme gereksinimini ortadan kaldırarak veri ön işleme süresini kısaltmaktadır. Düzenleştirme parametreleri (örneğin, L1 ve L2 regularization) ve erken durdurma desteği, aşırı öğrenmeyi önlemekte; çapraz doğrulama ile optimal ağaç sayısı belirlenerek modelin genelleme yeteneği artırılmaktadır. Bu özellikler, LightGBM'yi çok sınıflı sınıflandırma, regresyon ve sıralama görevleri için güçlü bir araç haline getirmektedir.

LightGBM'nin yaygın kullanım alanları, Nesnelerin İnterneti (IoT), finans, sağlık ve e-ticaret gibi veri yoğun sektörleri kapsamaktadır. IoT ağlarında, ağ trafiği anomalilerinin tespiti ve siber tehditlerin çok sınıflı sınıflandırması için tercih edilmekte; finans sektöründe ise sahtecilik tespiti, kredi riski modellemesi ve müşteri segmentasyonu gibi uygulamalarda kullanılmaktadır. Akademik araştırmalarda, LightGBM, yüksek boyutlu veri setleriyle hızlı ve doğru sınıflandırma görevleri için sıkça yer almakta, özellikle RPL tabanlı ağlarda güvenlik analizlerinde etkili sonuçlar sunmaktadır. Düşük hesaplama maliyeti ve gerçek zamanlı tahmin yeteneği, büyük ölçekli ve dinamik sistemlerde avantaj sağlamaktadır.



Şekil 3.6. LightGBM şeması

Şekil 3.6’da LightGBM’nin çok sınıflı sınıflandırma sürecini gösteren şema, öz nitelik vektörlerinin ağaçlar aracılığıyla değerlendirilmesini ve çoğunluk oylamasıyla sonuç sınıfının belirlenmesini açıklamaktadır. Şema, Sınıf I, Sınıf II ve Sınıf N gibi farklı ağaçların öz nitelik vektörlerini işleyişini ve sonuç sınıfını belirlemek için kullanılan çoğunluk oylamasını detaylandırmaktadır.

Bu çalışmada, LightGBM, RPL tabanlı IoT ağlarında Blackhole, HelloFlood ve Version Number saldırılarının tespit edilmesi ve çok sınıflı sınıflandırması için makine öğrenmesi modeli olarak kullanılmaktadır. Cooja simülatöründen ve Wireshark’tan elde edilen ağ trafiği verilerinin analizi ve anomali tespiti, LightGBM üzerinden gerçekleştirilmiştir.

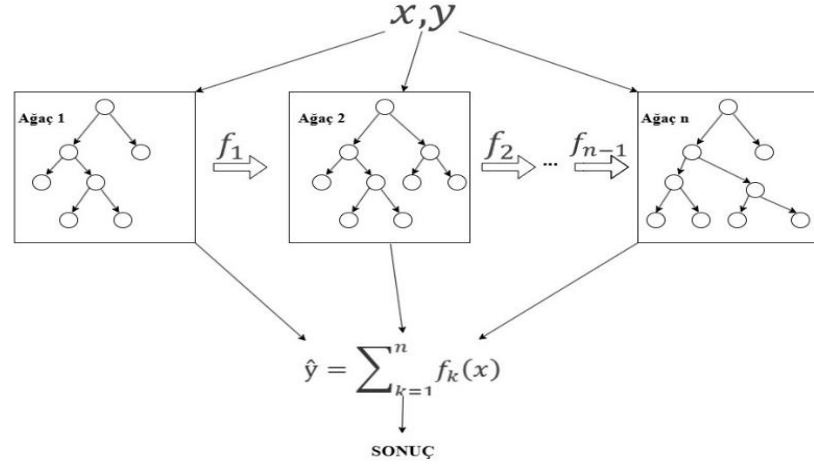
3.1.8. XGBoost

Extreme Gradient Boosting (XGBoost), gradyan artırma algoritmasının optimize edilmiş ve yüksek performanslı bir uygulaması olarak geliştirilen açık kaynaklı bir makine öğrenmesi kütüphanesidir. Bu algoritma, birden fazla karar ağacını sıralı bir şekilde birleştirerek, önceki modellerin tahmin hatalarını düzeltmek ve nihai bir topluluk modeli oluşturmak için tasarlanmıştır. XGBoost, kayıp fonksiyonunu minimize etmek amacıyla gradyan inişi tekniğini kullanmakta ve her iterasyonda yeni bir karar ağacını, önceki ağaçların zayıf yönlerini telafi edecek şekilde optimize etmektedir. Şekil 3.7’de gösterildiği üzere, bu süreç, giriş verileri (x , y) üzerinden bir dizi fonksiyon ($f_1, f_2, \dots, f_n$) ile başlar; her fonksiyon, önceki hataları düzelterek bir sonraki ağacı eğitir ve nihai tahmin ($\hat{y}$) tüm ağaçların çıktılarının toplamı olarak hesaplanır. Bu hiyerarşik ve iteratif yaklaşım, karmaşık veri ilişkilerini

modellemede yüksek doğruluk sağlamak ve çok boyutlu veri setlerinde etkili bir çözüm sunmaktadır (Chen ve Guestrin, 2016).

XGBoost'un algoritmik yapısı, birkaç temel bileşene dayanmaktadır. İlk olarak, gradyan artırma çerçevesi, her yeni ağacın, mevcut modelin tahmin hatalarının gradyan ve hessian değerlerine göre eğitilmesini içermektedir. Bu, kayıp fonksiyonunun (örneğin, karesel hata veya lojistik kayıp) en hızlı azalma yönünde ilerlemesini sağlar. İkinci olarak, XGBoost, paralel ağaç inşası ve yaklaşık ağaç bölme (approximate tree splitting) gibi optimizasyonlarla hesaplama verimliliğini artırmaktadır; bu yöntem, büyük veri setlerinde eğitim süresini %50'ye kadar kısaltabilmektedir. Üçüncü olarak, düzenlileştirme terimleri (L1 ve L2 regularization), modelin karmaşıklığını kontrol ederek aşırı öğrenmeyi önlemekte ve genelleme yeteneğini güçlendirmektedir. Ayrıca, erken durdurma (early stopping) ve çapraz doğrulama (cross-validation) desteği, optimal ağaç sayısını belirleyerek modelin aşırı uyum riskini azaltmaktadır. Bu özellikler, XGBoost'u regresyon, sınıflandırma ve sıralama görevlerinde üstün bir performans sergileyen bir araç haline getirmektedir.

XGBoost'un yaygın kullanım alanları, Nesnelerin İnterneti (IoT), finans, sağlık ve tarım gibi veri yoğun sektörleri kapsamaktadır. IoT ağlarında, ağ trafiği anomalilerinin tespiti ve siber tehditlerin sınıflandırılması için tercih edilmekte; finans sektöründe ise kredi riski değerlendirmesi, sahtecilik tespiti ve müşteri segmentasyonu gibi uygulamalarda kullanılmaktadır. Akademik araştırmalarda, XGBoost, yüksek boyutlu ve karmaşık veri setleriyle (örneğin, çok değişkenli IoT verileri) hızlı ve doğru sonuçlar elde etmek için sıkça yer almakta, özellikle RPL tabanlı ağlarda güvenlik analizlerinde etkili sonuçlar sunmaktadır. Gerçek zamanlı tahmin yeteneği ve düşük hesaplama maliyeti, dinamik sistemlerde avantaj sağlamaktadır.



Şekil 3.7. XGBoost arayüzü

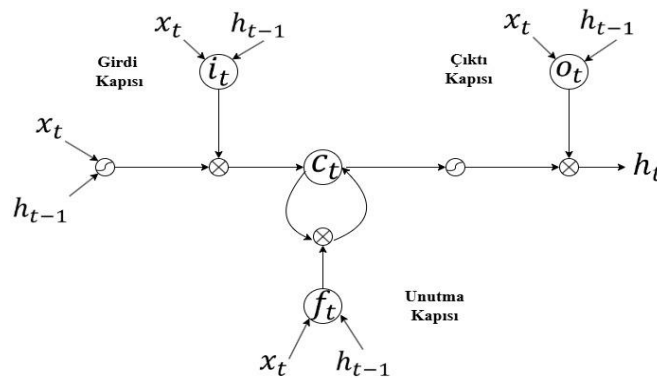
Şekil 3.7’de XGBoost’un gradyan artırma sürecini gösteren şema, giriş verilerinin (x, y) bir dizi karar ağacı $(f_1, f_2, \dots, f_n)$ ile işlenmesini ve nihai tahminin $(\hat{y})$ tüm ağaçların toplamı olarak hesaplanmasını açıklamaktadır. Şema, her ağacın önceki hataları düzelterek modelin doğruluğunu artırma sürecini detaylandırmaktadır.

Bu çalışmada, XGBoost, RPL tabanlı IoT ağlarında Blackhole, HelloFlood ve Version Number saldırılarının tespit edilmesi ve sınıflandırılması için makine öğrenmesi modeli olarak kullanılmaktadır. Cooja simülatöründen ve Wireshark’tan elde edilen ağ trafiği verilerinin analizi ve anomali tespiti, XGBoost üzerinden gerçekleştirilmiştir.

3.1.9.LSTM

Long Short-Term Memory (LSTM), zaman serisi verileri ve sıralı veri setleri için tasarlanmış, tekrarlayan sinir ağlarının (RNN) gelişmiş bir türüdür. LSTM, geleneksel RNN’lerin uzun vadeli bağımlılıkları modellemedeki yetersizliklerini aşmak için, bellek hücreleri ve üç ana kapı (giriş, unutma ve çıktı kapıları) ile donatılmıştır. Şekil 3.8’de gösterildiği üzere, LSTM birimleri, giriş verisi (x_t) ve önceki zaman adımının gizli durumu (h_{t-1}) ile çalışır. Giriş kapısı (i_t) , yeni bilgileri seçerek bellek hücresine (C_t) ekler; unutma kapısı (f_t) , eski bilgileri siler; ve çıktı kapısı (o_t) , güncellenmiş gizli durumu (h_t) ve çıktıyı (o_t) üretir. Bu kapılar, sigmoid ve tanh gibi aktivasyon fonksiyonlarıyla yönetilir; bu da LSTM’nin zamanla değişen verilerdeki örüntüleri uzun süreli hafızada tutmasını ve karmaşık ilişkileri öğrenmesini sağlamaktadır (Hochreiter ve Schmidhuber, 1997).

LSTM'nin yaygın kullanım alanları, Nesnelerin İnterneti (IoT), finans, sağlık ve sinyal işleme gibi sıralı veri gerektiren sektörleri kapsamaktadır. IoT ağlarında, ağ trafiği zaman serilerinin analizi ve siber saldırıların erken tespiti için tercih edilmekte; finans sektöründe ise hisse senedi fiyat tahmini ve piyasa trend analizi gibi uygulamalarda kullanılmaktadır. Akademik araştırmalarda, LSTM, uzun süreli bağımlılıkların modellenmesi gereken veri setlerinde (örneğin, IoT sensör verileri) sıkça yer almakta, özellikle RPL tabanlı ağlarda saldırı tespitinde etkili sonuçlar sunmaktadır. Gerçek zamanlı veri işleme kapasitesi, dinamik sistemlerde avantaj sağlamaktadır.



Şekil 3.8’de LSTM birimini gösteren şema, giriş verisi (x_t), önceki gizli durum (h_{t-1}), unutma kapısı (f_t), giriş kapısı (i_t), çıktı kapısı (o_t) ve bellek hücresi (C_t) arasındaki akışı detaylandırmaktadır. Şema, LSTM’nin zaman serisi verilerindeki uzun vadeli bağımlılıkları öğrenme sürecini açıklamaktadır.

Bu çalışmada, LSTM, RPL tabanlı IoT ağlarında Blackhole, HelloFlood ve Version Number saldırılarının zaman serisi verilerinden tespiti ve sınıflandırılması için makine öğrenmesi modeli olarak kullanılmaktadır. Cooja simülatöründen elde edilen ağ trafiği verilerinin analizi, LSTM üzerinden gerçekleştirilmiştir.

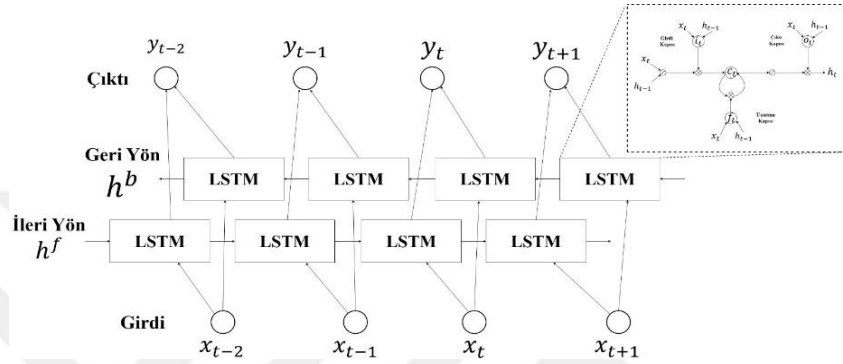
3.1.10. BiLSTM

Bidirectional Long Short-Term Memory (BiLSTM), zaman serisi verileri ve sıralı veri setleri için geliştirilmiş, çift yönlü bilgi akışını destekleyen bir tekrarlayan sinir ağı (RNN) modelidir. BiLSTM, geleneksel LSTM birimlerinin bir ileri (forward) ve bir geri (backward) yönlü katmanını birleştirerek, hem geçmiş hem de gelecek bağlamını dikkate alarak verilerin analizini sağlamaktadır. Şekil 3.9'da gösterildiği üzere, BiLSTM, giriş verileri (x_{t-2} , x_{t-1} , x_t , x_{t+1}) üzerinden iki ayrı LSTM katmanı kullanır: biri geri yönlü (h^b) önceki verileri, diğeri ileri yönlü (h^f) sonraki verileri işler. Bu iki katmanın çıktıları (y_{t-2} , y_{t-1} , y_t , y_{t+1}) birleştirilerek, her zaman adımında tam bağlamsal bilgi elde edilir. İçerisinde yer alan LSTM birimleri, unutma (f_t), giriş (i_t) ve çıktı (o_t) kapıları ile bellek hücrelerini (C_t) dinamik olarak güncelleyerek, uzun vadeli bağımlılıkları modellemektedir (Graves ve Schmidhuber, 2005).

BiLSTM'nin algoritmik yapısı, çift yönlü bilgi işleme mekanizmasına dayanmaktadır. İleri yönlü LSTM katmanı, zaman serisinin başlangıcından mevcut zaman adımına kadar olan verileri analiz ederken, geri yönlü LSTM katmanı, serinin sonundan mevcut adıma kadar olan verileri işler. Her iki katman, giriş verisi (x_t) ve önceki gizli durumlar (h_{t-1}) üzerinden sigmoid ve tanh aktivasyon fonksiyonlarıyla kapılarını kontrol eder. Unutma kapısı, eski bilgileri silerek bellek hücrelerini günceller; giriş kapısı, yeni bilgileri değerlendirir ve çıktı kapısı, güncellenmiş gizli durumu üretir. Bu süreçte, ileri ve geri yönlü katmanların çıktıları birleştirilerek, her zaman adımında (y_t) tam bağlamsal bir tahmin oluşturulur. Şekil 3.9'un sağ tarafındaki detay, bir LSTM biriminin iç yapısını (giriş kapısı, unutma kapısı, çıktı kapısı ve bellek hücresi) göstererek, BiLSTM'nin çift yönlü işleme kapasitesini desteklemektedir. Bu özellikler, BiLSTM'yi zaman serisi tahmini, doğal dil işleme ve anomali tespiti gibi alanlarda karmaşık örüntüleri modellemede üstün kılmaktadır.

BiLSTM'nin yaygın kullanım alanları, Nesnelerin İnterneti (IoT), sağlık, finans ve ses tanıma gibi sıralı veri gerektiren sektörleri kapsamaktadır. IoT ağlarında, ağ

trafiği zaman serilerinin çift yönlü analizi ve siber saldırıların erken tespiti için tercih edilmekte; sağlık sektöründe ise elektrokardiyogram (EKG) verilerinin sınıflandırılması ve hasta izleme gibi uygulamalarda kullanılmaktadır. Akademik araştırmalarda, BiLSTM, uzun süreli ve çift yönlü bağımlılıkların modellenmesi gereken veri setlerinde (örneğin, IoT sensör verileri) sıkça yer almakta, özellikle RPL tabanlı ağlarda saldırı tespitinde etkili sonuçlar sunmaktadır. Gerçek zamanlı veri işleme ve yüksek doğruluk kapasitesi, dinamik sistemlerde avantaj sağlamaktadır.



Şekil 3.9. BiLSTM şeması

Şekil 3.9’da BiLSTM’nin çift yönlü işleme yapısını gösteren şema, giriş verilerinin (x_{t-2} , x_{t-1} , x_t , x_{t+1}) ileri ve geri yönlü LSTM katmanları aracılığıyla işlenmesini ve çıktının (y_{t-2} , y_{t-1} , y_t , y_{t+1}) birleştirilmesini açıklamaktadır. Şema, bir LSTM biriminin iç yapısını (giriş kapısı, unutma kapısı, çıktı kapısı ve bellek hücresi) detaylandırarak, çift yönlü bağlamsal analizi desteklemektedir.

Bu çalışmada, BiLSTM, RPL tabanlı IoT ağlarında Blackhole, HelloFlood ve Version Number saldırılarının zaman serisi verilerinden çift yönlü tespiti ve sınıflandırılması için makine öğrenmesi modeli olarak kullanılmaktadır. Cooja simülatöründen elde edilen ağ trafiği verilerinin analizi, BiLSTM üzerinden gerçekleştirilmiştir.

3.1.11. HDF5

HDF5 (Hierarchical Data Format version 5), büyük ve karmaşık veri kümelerini depolamak ve yönetmek için tasarlanmış bir dosya formatıdır. IoT ve IIoT sistemlerinde, sensör verileri, ağ trafiği kayıtları ve makine öğrenmesi modellerinin çıktıları gibi büyük veri kümelerinin saklanması için kullanılır. Bu çalışmada, HDF5, Cooja simülatöründen ve Wireshark’tan toplanan ağ trafiği verilerinin depolanması ve

makine öğrenmesi modellerine (LightGBM, XGBoost, LSTM, BiLSTM) girdi olarak hazırlanması için kullanılmıştır.

HDF5'nin yüksek performanslı veri erişim yeteneği, büyük veri kümelerinin hızlı bir şekilde işlenmesini sağlamıştır. Örneğin, RPL tabanlı ağlardan toplanan zaman serisi verileri, HDF5 formatında saklanarak LSTM ve BiLSTM modellerine etkili bir şekilde sağlanmıştır. Ayrıca, HDF5'nin hiyerarşik yapısı, veri kümelerinin düzenli ve kolay erişilebilir bir şekilde organize edilmesini mümkün kılmıştır. Bu format, çalışmanın veri yönetim süreçlerini optimize etmiş ve makine öğrenmesi modellerinin eğitimini hızlandırmıştır.

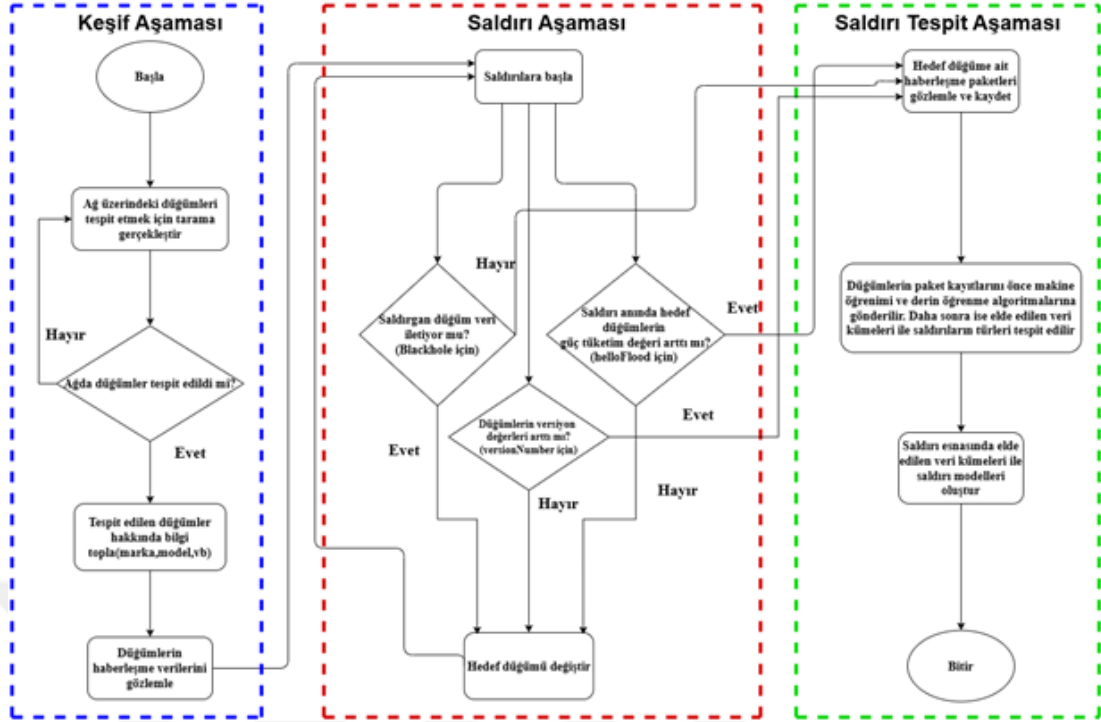
3.2. Kullanılacak Metot

Bu çalışma, RPL (Routing Protocol for Low-Power and Lossy Networks) tabanlı Nesnelerin İnterneti (IoT) ağlarında Blackhole, HelloFlood ve Version Number saldırılarının yönlendirme yapısı ve enerji performansı üzerindeki etkilerini incelemek amacıyla kapsamlı bir simülasyon ve analiz çerçevesi uygulamıştır. Simülasyon ortamının kurulumu, çalışmanın metodolojik temelini oluşturmaktadır. Contiki 3.0 işletim sistemi, RPL protokolüne yerel destek sağlaması, enerji izleme yetenekleri ve protokol özelleştirme esnekliğiyle bu araştırma için uygun bir platform olarak seçilmiştir. Contiki'nin modüler mimarisi, ağ yönetimini, iletişim protokollerinin uygulanmasını ve saldırı senaryolarının entegrasyonunu kolaylaştırmıştır. Simülasyonlar, Contiki ile tam uyumlu olan Cooja simülatörü kullanılarak gerçekleştirilmiştir. Cooja, düğüm davranışlarını, radyo iletişimini ve enerji tüketimini gerçekçi bir şekilde modelleme kapasitesiyle, saldırıların ağ üzerindeki etkilerinin detaylı analizine olanak tanımıştır.

Ağ modeli, toplam 52 düğümden oluşacak şekilde tasarlanmıştır: bir kök düğüm (sink node), ağın merkezi veri toplama birimi olarak görev yapmış; 50 standart IoT düğümü, algılanan verileri çok atlamalı (multi-hop) bir yapıda kök düğüme iletmış; ve bir saldırgan düğüm, belirli saldırı senaryolarını (Blackhole, HelloFlood veya Version Number) uygulamak üzere ağa entegre edilmiştir. Düğümler, IEEE 802.15.4 standardına uygun olarak yapılandırılmış ve radyo iletişim modeli olarak Unit Disk Graph (UDG) kullanılmıştır. UDG, fiziksel mesafeye dayalı bağlantı modellemesi sunmuş ve düğümler arası maksimum iletişim mesafesi 50 metre olarak

tanımlanmıştır. Bu, düğümlerin yalnızca kapsama alanındaki komşularıyla iletişim kurabileceği bir topoloji oluşturmuştur. RPL protokolü, OF0 (Objective Function Zero) yönlendirme fonksiyonu ile uygulanmış; bu fonksiyon, her düğümün en düşük rank değerine sahip komşusunu ebeveyn olarak seçmesini sağlayarak DODAG (Destination Oriented Directed Acyclic Graph) yapısının oluşumunu desteklemiştir. Simülasyon ortamı, saldırgan düğümün ağ üzerindeki etkisini maksimize edecek şekilde tasarlanmıştır; bu doğrultuda, saldırgan düğüm kök düğümle doğrudan iletişim mesafesinde (50 metre kapsama alanında) konumlandırılmıştır. Her bir saldırı senaryosu, 1200 saniye süreyle üçer kez tekrarlanarak simüle edilmiş, böylece sonuçların istatistiksel güvenilirliği artırılmıştır.

Simülasyon ortamının kurulumu, metodolojik tutarlılık ve tekrarlanabilirlik sağlamak adına sistematik bir süreç izlenerek gerçekleştirilmiştir. Şekil 3.10'da, bu süreci görsel olarak özetleyen bir akış diyagramı sunulmaktadır. Akış diyagramı, Contiki 3.0 işletim sisteminin yapılandırılması, Cooja simülatörünün entegrasyonu, ağ düğümlerinin yerleştirilmesi ve saldırı senaryolarının uygulanması adımlarını detaylandırmaktadır. Bu diyagram, çalışmanın metodolojik altyapısını net bir şekilde ortaya koymakta ve simülasyonların bilimsel geçerliliğini desteklemektedir.



Şekil 3.10. Saldırı ve Tesip Modelinin Akış Diyagramı

3.2.1. Donanım Altyapısı

Simülasyonların yüksek performansla ve kesintisiz bir şekilde yürütülmesi için güçlü bir donanım altyapısı kullanılmıştır. Tüm simülasyonlar ve veri analizleri, AMD Ryzen 9 5900X işlemci, 32 GB DDR4 RAM ve NVIDIA RTX 3080 grafik kartına sahip bir bilgisayar sistemi üzerinde gerçekleştirilmiştir. Bu altyapı, 52 düğümlü ağların uzun süreli simülasyonlarını ve Cooja gibi işlemci yoğunluğu yüksek uygulamaların istikrarlı bir şekilde çalışmasını sağlamıştır. Ayrıca, Foren6 ve Wireshark gibi analiz araçlarının paralel çalıştırılması ve büyük veri setlerinin işlenmesi, bu donanım sayesinde etkin bir şekilde gerçekleştirilmiştir. Donanım altyapısının sağladığı yüksek hesaplama kapasitesi, simülasyonların tekrarlanabilirliğini ve analizlerin doğruluğunu desteklemiştir.

3.2.2. Veri Toplama ve Analiz Araçları

Saldırıların ağ üzerindeki etkilerini çok boyutlu bir şekilde değerlendirmek için birden fazla veri toplama ve analiz aracı entegre edilmiştir. Contiki işletim sisteminin yerleşik bir bileşeni olan Powertrace modülü, düğümlerin enerji tüketimini milisaniye çözünürlükte kaydetmek için kullanılmıştır. Powertrace; işlemci kullanım süresi (CPU), düşük güç modunda geçirilen süre (LPM), radyo gönderim süresi (TX) ve

radio alım süresi (RX) gibi parametreleri izleyerek, saldırı senaryoları sırasında ani tüketim sıçramalarını veya sürekli yüksek tüketim durumlarını tespit etmiştir. Simülasyon sonunda Powertrace verileri dışa aktarılmış ve Python ile istatistiksel analizlere (ortalama, maksimum, varyans) tabi tutulmuştur.

Ağ trafiğinin düşük seviyeli (Layer 2) analizi için Wireshark kullanılmıştır. Cooja simülatörü, ağ trafiğini .pcap formatında kaydetmiş ve bu dosyalar Wireshark'a aktarılmıştır. Wireshark; gönderilen ve alınan toplam paket sayısı, ICMPv6-RPL, UDP, DIO, DAO, DIS gibi protokol mesajlarının yoğunluğu, zaman damgalı trafik davranışları ve protokol anomalileri gibi unsurları analiz etmiştir. Özellikle HelloFlood saldırısında DIO mesajlarının yoğunlaşması, Blackhole saldırısında veri akışının kesintiye uğraması ve Version Number saldırısında sahte DIO mesajlarının yayılma zamanlaması net bir şekilde ortaya konmuştur. Analiz edilen .pcap dosyaları, tekrarlanabilirlik için senaryo adları ve zaman bilgileriyle kataloglanmıştır.

RPL'nin DODAG yapısını ve yönlendirme dinamiklerini görselleştirmek için Foren6 aracı kullanılmıştır. Foren6, zaman damgalı DIO, DAO ve DIS mesajlarını işleyerek; saldırı öncesi ve sonrası DODAG yapısındaki değişiklikleri, protokol mesajlarının yayılma yoğunluğunu ve düğümlerin ebeveyn seçimlerinin kararlılığını görselleştirmiştir. Foren6'nın grafiksel çıktıları; Blackhole saldırısında saldırgan düğümün çok sayıda düğüm tarafından ebeveyn seçildiğini, HelloFlood saldırısında yönlendirme yollarının kaotik bir yapıya büründüğünü ve Version Number saldırısında DODAG'ın sürekli yeniden yapılandırıldığını göstermiştir. Foren6 verileri, .csv formatında dışa aktarılmış ve ileri analizler için kullanılmıştır.

3.2.3. Blackhole Saldırısı

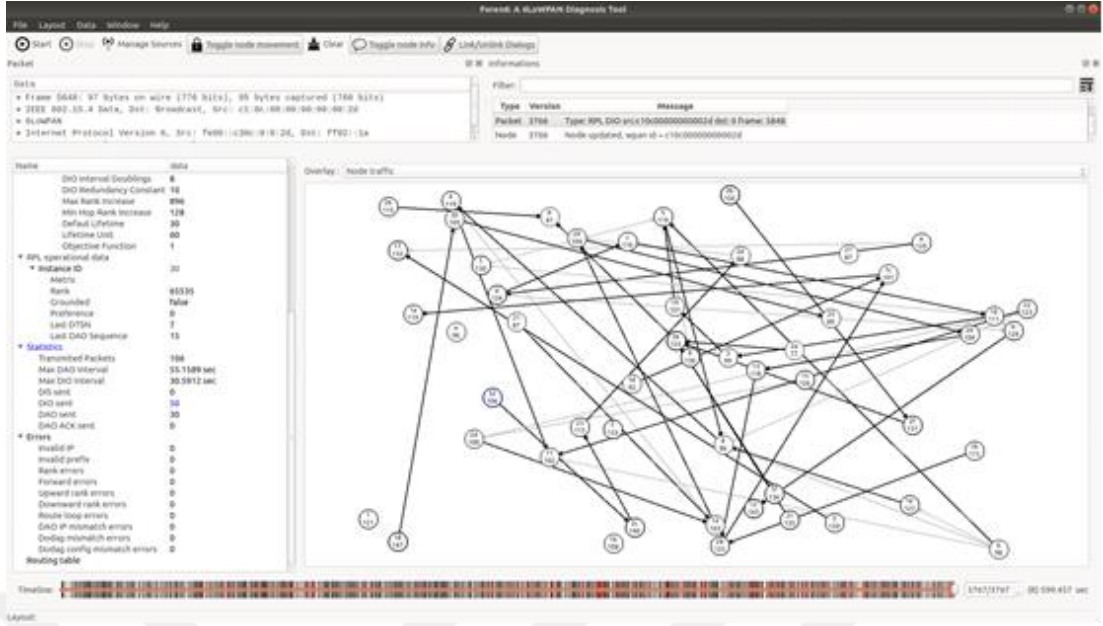
Blackhole saldırısı, yönlendirme protokollerinin güvenliğini hedef alan, RPL gibi kaynak kısıtlı sistemlerde ise etkisi daha da kritik hale gelen bir saldırı türüdür. Saldırgan düğüm, sahte yönlendirme avantajları ile DAG yapısına entegre olurken, kendisine yönlendirilen veri paketlerini düşürerek (drop) veri iletimini sistematik biçimde engeller. RPL protokolünün “düşük güç – yüksek güvenilirlik” hedefi bu saldırı altında ciddi biçimde zedelenir.

▼ Statistics	
Transmitted Packets	96
Max DAO Interval	63.6299 sec
Max DIO Interval	45.1603 sec
DIS sent	1
DIO sent	52
DAO sent	24
DAO ACK sent	0
▼ Errors	
Invalid IP	0
Invalid prefix	0
Rank errors	0
Forward errors	0
Upward rank errors	0
Downward rank errors	0
Route loop errors	2
DAO IP mismatch errors	0
Dodag mismatch errors	0
Dodag config mismatch errors	0
▼ Routing table	
aaaa::c30c:0:0:c/128	c10c00000000000c

Şekil 3.11. Blackhole saldırı ağ istatistikleri

Bu çalışmada kullanılan simülasyon ortamında, DAG yapısında 50 adet normal düğüm ve bir adet kök düğüm yer almaktadır. Saldırgan düğüm, DAG köküne 2 topolojik sıçrama (hop) mesafede konumlandırılarak ağ merkezine yerleştirilmiştir. Bu konumlandırma sayesinde, yönlendirme açısından avantajlı bir pozisyonda bulunan saldırgan, çevresindeki birçok düğüm tarafından ebeveyn olarak tercih edilmiştir. Foren6 aracı üzerinden yapılan analizlerde saldırganın, kısa bir zaman aralığında 52 adet DIO mesajı yayımladığı Şekil 3.11’de gözlemlenmiştir. DIO yayım sıklığı, DAG içindeki düğümlere göre oldukça yüksektir ve bu davranış, saldırgan düğümün ağı yönlendirme yapısında merkezi bir rol üstlenmesini sağlamıştır.

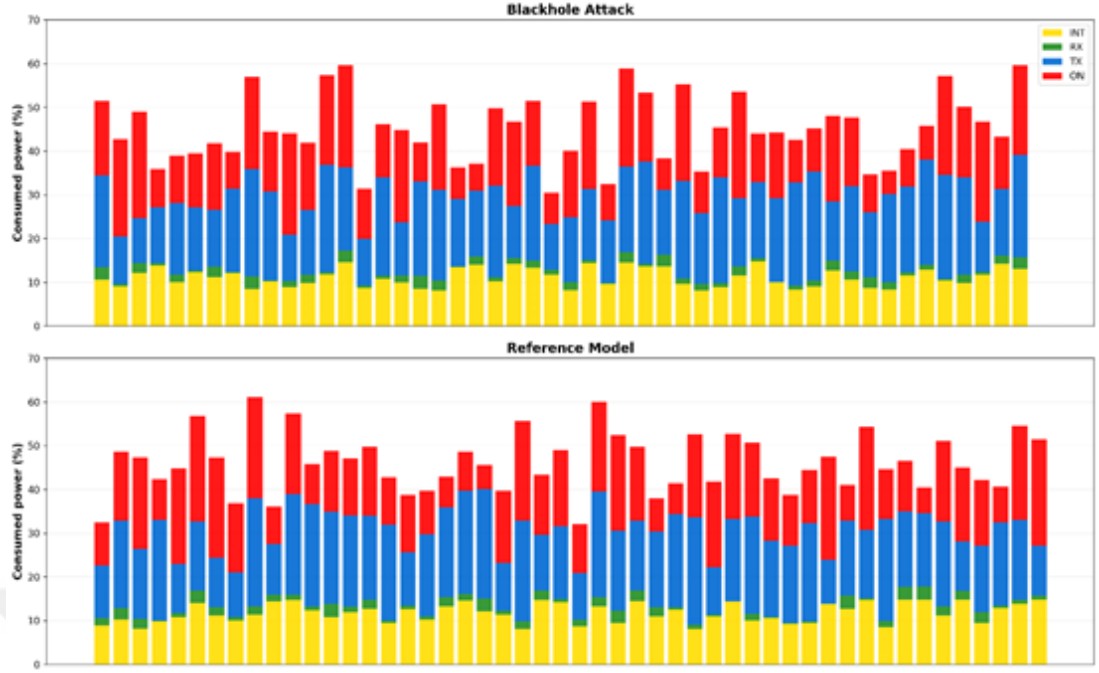
Ancak aynı düğümün ilettiği toplam veri paketi sayısı yalnızca 96 ile sınırlı kalmakta ve DAO-ACK mesajı üretmediği açıkça görülmektedir. DAO-ACK eksikliği, RPL protokolünde aşağı yönlü iletişimde yönlendiricinin üstlendiği onay görevini yerine getirmediğini ve protokol işleyişini bilinçli olarak aksattığını göstermektedir. Bu davranış, DAG yapısındaki diğer düğümlerin yönlendirme tablolarını tamamlayamamasına ve sürekli yeniden yapılandırma süreçlerine girmesine yol açmaktadır. Ayrıca yönlendirme hatalarına işaret eden 2 adet döngüsel



Şekil 3.13. Blackhole saldırı öncesi

Bu saldırının RPL ağlarına etkisi yalnızca yönlendirme açısından değil, enerji tüketimi bakımından da oldukça yıkıcıdır. Saldırgan düğümle iletişim kurmaya çalışan çevre düğümler, sık yönlendirme güncellemeleri, başarısız paket iletimleri ve artan kontrol mesajı trafiği nedeniyle CPU ve RX modüllerini yoğun biçimde çalıştırmak zorunda kalmıştır. Güç tüketimi analizine yönelik gerçekleştirilen ölçümlerde, saldırgan düğümün aktif olduğu senaryoda düğümlerin ortalama güç tüketimi %30–35 düzeylerine ulaşmışken; referans senaryoda bu oran %15–20 seviyelerinde kalmıştır. Bu analiz Şekil 3.14’de sunulmuştur. Grafik karşılaştırması, Blackhole saldırısının enerji tüketiminde %100’e varan artışa yol açtığını göstermektedir. Bu fark, yalnızca düğüm seviyesinde pil ömrünün kısalmasına değil, ağ genelinde sürdürülebilirliğin bozulmasına da neden olmaktadır.

Veri paketlerinin düşürülmesi, yönlendirme döngülerinin ortaya çıkması, DAO-ACK mesajlarının tamamen ortadan kalkması ve enerji tüketiminde gözlemlenen artış bir araya geldiğinde, saldırganın yalnızca bireysel düğümleri değil, DAG’ın tamamını etkileyen sistematik bir kesinti oluşturduğu anlaşılmaktadır. RPL protokolü içinde pasif ama kritik bir zafiyeti hedef alan bu saldırı, yönlendirme kararlarının doğruluğunu, veri iletim sürekliliğini ve kaynak verimliliğini eşzamanlı olarak baltalayarak ağ performansında ciddi bozulmalar meydana getirmektedir.



Şekil 3.14. Blachkole saldırısı ve referans model

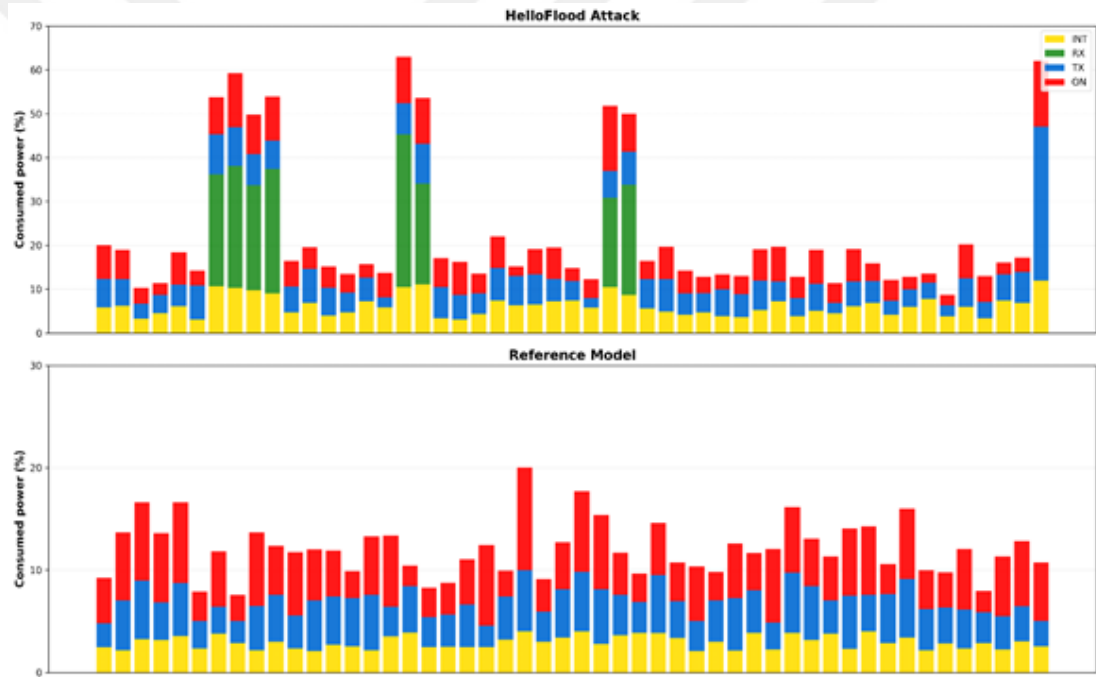
3.2.4. HelloFlood Saldırısı

HelloFlood saldırısı, IoT ağlarında yönlendirme protokolünü doğrudan manipüle etmeden, sahte “Hello” mesajlarıyla düğümleri yanıt vermeye zorlayarak işlemci ve radyo kaynaklarını meşgul eden yaygın bir saldırı modelidir. Saldırgan düğüm, çevresindeki düğümlerin alıcı (RX) modüllerini sürekli aktif hâlde tutmakta; bu durum ağın hem enerji verimliliğini hem de yönlendirme istikrarını olumsuz etkilemektedir. Özellikle yönlendirme tablolarının sık sık yeniden yapılandırılması ve sahte komşuluk ilişkilerinin oluşması, ağda süregelen bir protokol belirsizliği yaratmaktadır.

Saldırıya karşılık ağın verdiği davranış, Foren6 aracıyla elde edilen topoloji görselleri üzerinden değerlendirildiğinde açıkça izlenebilmektedir. Referans durumda ağın yönlendirme yapısına ait görünüm Şekil 3.15’de sunulmuştur. Bu görselde düğümler arası bağlantılar oldukça düzenlidir ve yönlendirme grafiği tutarlılık göstermektedir. Düğümler, yalnızca gerekli kontrol mesajlarını iletmekte ve belirli istikrarlı ebeveynlerle veri yolları oluşturmaktadır. Bu yapıya karşılık gelen örnek bir düğüm olan 2e numaralı düğümün ilettiği toplam paket sayısı yalnızca 19’dur.

göstermektedir. Bu bağlamda, saldırgan düğümün DIS iletim oranı, 2e gibi normal bir düğüme kıyasla yaklaşık 33 kat daha yüksektir. Bu nicel fark, saldırının yalnızca lokal bir etki değil, protokol davranışını sistematik olarak bozacak derecede yaygın olduğunu göstermektedir.

Trafik yoğunluğundaki artış, Wireshark üzerinden yapılan analizlerle desteklenmektedir. Saldırı öncesi ağda toplam 126.324 paket izlenmişken, saldırı başladığında bu sayı 212.394'e yükselmiştir. Yaklaşık %68 oranındaki bu artış, ağın kontrol ve veri düzeyinde aşırı yüklenmeye maruz kaldığını göstermektedir. Bu yük yalnızca işlemci tarafında değil, radyo modülü düzeyinde de fazladan enerji tüketimi anlamına gelmektedir.



Şekil 3.17. HelloFlood saldırısı ve referans model

Enerji tüketimi farkı ise Şekil 3.17'de grafiksel olarak gösterilmiştir. Bu şekilde, üst kısımda HelloFlood saldırısı altındaki düğümlerin enerji tüketim dağılımları; alt kısımda ise saldırısız referans modeldeki değerler sunulmaktadır. Saldırı altında özellikle RX ve TX fazlarında ciddi artışlar gözlemlenmekte, bazı düğümlerde toplam tüketim oranı %60 seviyelerine ulaşmaktadır. Referans modelde bu oranlar %20 seviyelerinde sabitlenmektedir. Bu enerji farkı, teorik olarak düğümlerin pil ömürleri üzerinde doğrudan etkiye sahiptir. Örneğin sabit enerji kapasitesine sahip bir düğüm, referans durumda yaklaşık 10 gün kesintisiz çalışabilirken; saldırı altında bu sürenin 3

güne kadar düştüğü hesaplanabilmektedir. Bu durum, enerjiye duyarlı uygulamalarda HelloFlood saldırısının sistem ölçeğinde sürdürülebilirliği tehdit ettiğini göstermektedir.

Ayrıca, ağdaki yönlendirme yapısının saldırı sırasında sürekli değişmesi; komşuluk ilişkilerinin kararsızlaşması, paket gecikmelerinde artış ve rota seçimlerinin tutarsızlaşması gibi ikincil etkileri de beraberinde getirmektedir. Foren6 ağ akış haritalarında bu durum yön oklarının sık ve rastgele dağılmış olmasıyla da doğrulanmaktadır. Ağ, istikrarlı bir DAG (Directed Acyclic Graph) yapısı oluşturamamakta; bunun yerine sürekli yeniden yapılandırılan, kısa ömürlü geçici yollar oluşmaktadır.

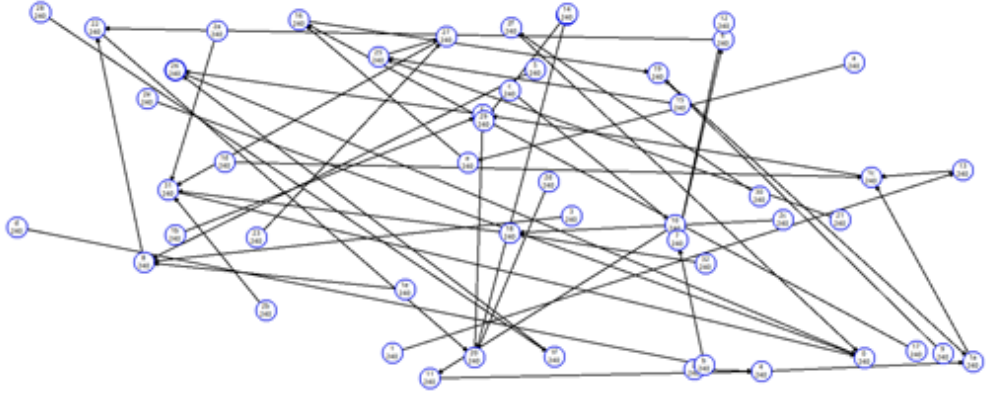
3.2.5. Version Number Saldırısı

Version Number saldırısı, RPL protokolünün temel mekanizmalarından biri olan DODAG sürüm numarasının (DODAG Version Number) kötüye kullanılması yoluyla gerçekleştirilen bir yönlendirme bozulması saldırısıdır. RPL protokolünde, ağın yönlendirme ağacı olan DODAG yapısının güncelliğini ve geçerliliğini belirlemek amacıyla kullanılan bu sürüm numarası yalnızca ağın kök düğümü tarafından artırılabilir. Ancak bu çalışma kapsamında, saldırgan düğüm bu işlevişi manipüle ederek ağın yönlendirme yapısında sürekli bir belirsizlik ve yeniden yapılanma durumu yaratmaktadır.

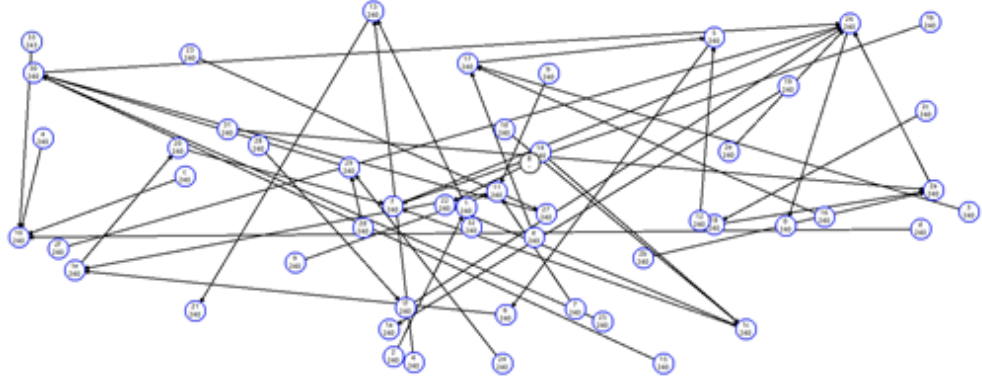
Simülasyon ortamında, saldırgan düğüm ağın kök düğümüne yakın bir konumda yerleştirilmiş ve sahte DIO mesajları ile mevcut ağın sürüm numarasından daha yüksek bir Version Number değeri ilan etmiştir. Bu durum RPL protokolü açısından, ağda bir “Global Repair” yani küresel yeniden yapılanma gerektiği anlamına gelir. Bu sinyali alan tüm düğümler mevcut yönlendirme tablolarını temizleyerek, yeni bir DODAG yapısına katılmak için yeniden ebeveyn seçimi ve yönlendirme oluşturma sürecine girer.

Bu saldırı, kök düğüm tarafından başlatılmayan sahte bir yeniden yapılanma sürecine neden olduğu için, protokolün kendi karar verme mantığını doğrudan hedef alır. Saldırgan düğüm, belirli aralıklarla Version Number değerini sürekli artırarak ağın hiçbir zaman kararlı bir yönlendirme yapısı kurmasına izin vermez. Bunun

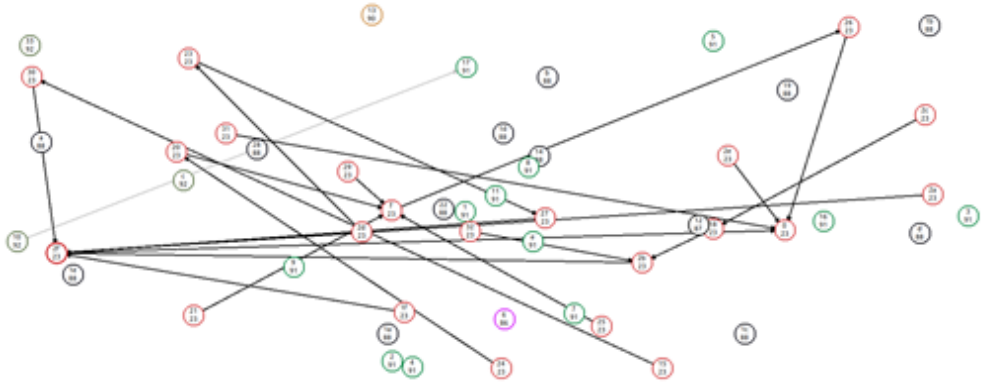
sonucunda ağda sürekli olarak yüksek miktarda DIO ve DIS mesaj trafiği oluşur, düğümler ebeveyn değiştirir ve yönlendirme kararları sık sık güncellenir.



Şekil 3.18. Version number saldırı öncesi



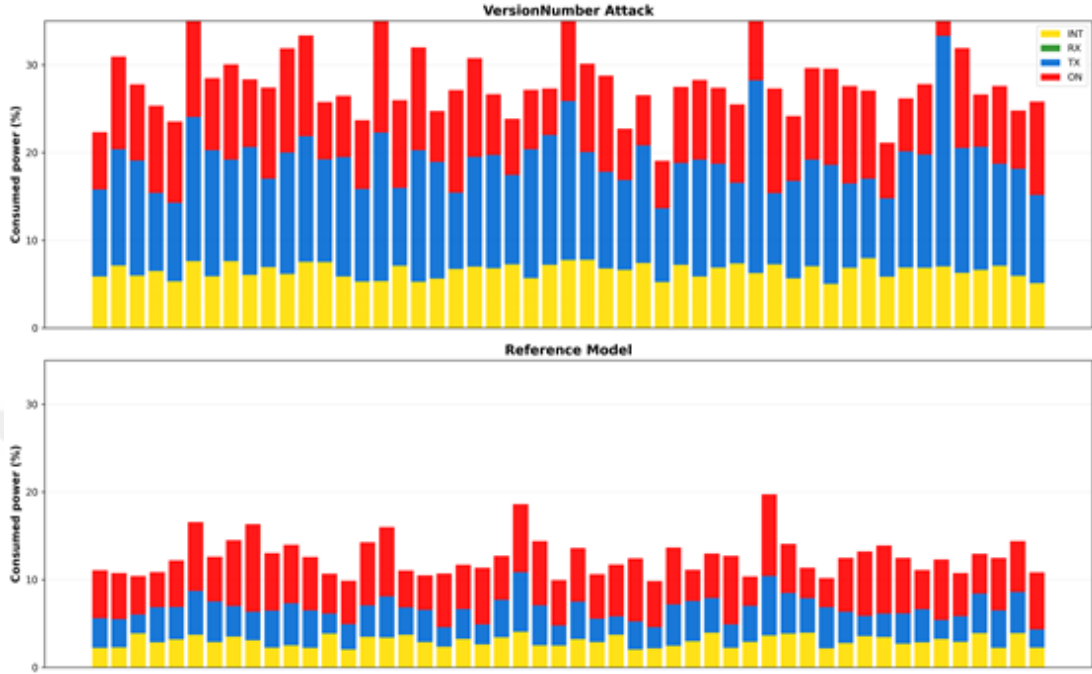
Şekil 3.19. Version number saldırı başlangıcı



Şekil 3.20. Version number saldırı sonrası

Foren6 aracı ile alınan ağ topolojisi görsellerinde bu durum açık biçimde gözlemlenmiştir. Şekil 3.18’de saldırı olmayan ortamda tüm düğümlerin Version = 240 değerinde istikrarlı bir DAG yapısına sahip olduğunu gösterirken, Şekil 3.19’da saldırı başladığında bazı düğümlerin Version Number değerlerinin yükselmeye

başladığını ve DAG'ın yapısının bozulduğunu göstermektedir. Şekil 3.20'de saldırının devam etmesiyle birlikte tüm ağın kaotik bir yapıya büründüğünü ve düğümlerin farklı version numaralarına sahip DAG parçacıklarına ayrıldığını ortaya koymaktadır.



Şekil 3.21. Version number saldırısı ve referans model

Ayrıca, Şekil 3.21'de saldırı altındaki ve referans ağ ortamında düğümlerin enerji tüketimlerini karşılaştırmalı olarak göstermektedir. Version Number saldırısı sırasında, radyo modülünün TX (gönderim) ve RX (alım) fazlarında ciddi bir artış yaşandığı; özellikle saldırıya maruz kalan düğümlerde toplam enerji tüketiminin %30–35 seviyelerine ulaştığı gözlemlenmiştir. Referans modelde bu oranların %15 civarında kaldığı dikkate alındığında, saldırının ağ performansı üzerindeki enerji maliyeti oldukça yüksektir.

Wireshark ve Foren6 üzerinden yapılan detaylı trafik analizlerinde, saldırı anında DIO mesajlarının gönderim frekansının yaklaşık dört kat arttığı ve DIS mesajlarının yoğunlaştığı da doğrulanmıştır. Bu, ağda ebeveyn belirleme sürecinin sürekli olarak tetiklendiğini ve kararsız bir yönlendirme yapısının oluştuğunu kanıtlamaktadır.

Bu saldırının en dikkat çekici yönlerinden biri, diğer saldırı türlerinin aksine doğrudan veri paketlerini hedef almaması, ancak ağın yönlendirme karar mekanizmasını manipüle ederek dolaylı fakat süreğen bir istikrarsızlık yaratmasıdır.

Saldırganın gönderdiği her sahte DIO mesajı, düğümlerin mevcut yönlendirme yapılarını terk etmesine neden olurken; yeniden oluşan yapı, kısa süre içinde tekrar geçersiz hale geldiğinden ağda hiç bitmeyen bir yeniden yapılanma döngüsü meydana gelmektedir.

Bu çalışma kapsamında gerçekleştirilen Version Number saldırısı, RPL protokolünün doğrudan tasarımsal zayıflıklarını hedef alarak ağ kararlılığına büyük ölçüde zarar vermektedir. Elde edilen bulgular, saldırının yalnızca ağ performansını değil, aynı zamanda hizmet sürekliliğini ve enerji verimliliğini de olumsuz etkilediğini açık biçimde ortaya koymuştur. Bu nedenle söz konusu saldırı, özellikle enerji kısıtlı ve sürekli bağlantı gerektiren IoT ortamlarında yüksek öncelikli bir tehdit olarak değerlendirilmelidir.

3.3. Analiz ve Bulgular

Bu çalışmada, toplamda 27.833.806 paket verisi içeren büyük ölçekli veri setleri kullanılarak IoT ağlarında meydana gelen saldırıların tespiti amaçlanmıştır. Veri hacminin yüksekliği, geleneksel analiz yöntemlerinin ötesinde ölçeklenebilir ve performans odaklı çözümler gerektirmektedir. Bu nedenle, veri işleme süreçlerinin hem bütünlük hem de hız açısından optimize edilmesi amacıyla veriler HDF5 (H5) formatına dönüştürülmüştür. HDF5, büyük veri yapılarında yüksek hızlı erişim sağlayan yapısı sayesinde, analiz süreçlerinin verimli ve tutarlı bir şekilde yürütülmesine olanak tanımıştır.

Veri ön işleme ve öznitelik seçimi aşamalarında, çalışmanın önceki bölümlerinde ayrıntılı biçimde açıklanan güç analizi (power analysis) ve Wireshark tabanlı ağ paketi incelemeleri esas alınmıştır. Bu ön analizler, saldırıların trafik üzerindeki davranışsal izlerini ve karakteristik örüntülerini ortaya koyarak, makine öğrenmesi modellerine aktarılacak veri yapısının anlamlı ve ayrıştırıcı özellikler içermesini sağlamıştır. Bu doğrultuda, analizlerde kullanılan temel öznitelikler şunlardır: "frame.time", "frame.len", "wpan.src64", "wpan.dst64", "icmpv6.type", "ipv6.src", "ipv6.dst" ve "icmpv6.code". Ayrıca, tüm saldırı türlerinden eşit sayıda örnek seçilerek dengeli ve homojen bir veri seti oluşturulmuş, bu sayede model eğitiminde sınıf dengesizliğine bağlı öğrenme hatalarının önüne geçilmiştir. Etiketleme işlemleri, verinin sınıflandırma algoritmaları tarafından doğrudan

işlenebilmesi amacıyla titizlikle gerçekleştirilmiş ve veriler nihai analiz için hazır hale getirilmiştir.

Bu çalışma kapsamında, IoT ağlarında yaygın olarak karşılaşılan HelloFlood, Blackhole ve VersionNumber saldırı türlerinin tespiti amacıyla çeşitli makine öğrenmesi ve derin öğrenme algoritmaları kullanılmıştır. Uygulanan modellerin performansları, makine öğrenmesi literatüründe yaygın biçimde kabul gören Accuracy, F1 skoru, Precision, Recall ve AUC (Area Under Curve) metrikleri kullanılarak çok boyutlu bir değerlendirme ile analiz edilmiştir.

Tablo 3.1’de algoritmalar arası performans karşılaştırmasına ilişkin bulgular Şekil: Modellerin Performans Karşılaştırması başlığı altında sunulmuştur. Bu görselden elde edilen bulgulara göre, BiLSTM (Bidirectional Long Short-Term Memory) algoritması genel sınıflandırma başarımı açısından en yüksek performansı sergilemiştir. Spesifik olarak, %99,02 doğruluk, %98,85 F1 skoru, %98,89 precision, %98,91 recall ve %99,83 AUC değerleri ile BiLSTM, diğer algoritmalara kıyasla IoT ağ trafiğinde saldırı tespiti görevini en etkili şekilde gerçekleştiren model olmuştur. Bu üstün performans, algoritmanın zaman serisi özelliklerini çift yönlü bilgi akışıyla işlemesi sayesinde hem geçmiş hem de gelecek bağlamı dikkate alarak karar verebilme yeteneğinden kaynaklanmaktadır.

Tablo 3.1. Modellerin performans karşılaştırması

Model	Accuracy	F1 Score	Precision	Recall	AUC	Eğitim Süresi(s)	Test Süresi(s)
BiLSTM	0.9902	0.9885	0.9889	0.9891	0.9983	390.76	8.94
LSTM	0.9812	0.9768	0.9775	0.9783	0.9941	244.50	7.22
XGBoost	0.9788	0.9784	0.9779	0.9789	0.9925	100.35	1.21
LightGBM	0.9656	0.9668	0.9680	0.9657	0.9865	21.06	5.45

Her ne kadar BiLSTM algoritması sınıflandırma performansı açısından çalışmada en başarılı model olarak öne çıksa da, 390,76 saniyelik eğitim süreci ile zaman açısından en maliyetli algoritma konumundadır. Bu durum, özellikle gerçek zamanlı IoT ağlarında anlık güncellemelerin gerektiği senaryolarda önemli bir sınırlılık oluşturmaktadır. Kritik görevlerde hızlı model güncellemelerinin gerekli olduğu dinamik ortamlarda, bu eğitim süreci yüksek doğruluğa rağmen sistemin kullanılabilirliğini sekteye uğratabilecek bir faktördür. Ayrıca, BiLSTM’in test süresi

8,94 saniye olarak ölçülmüş olup, bu süre de bazı düşük gecikme gereksinimli uygulamalar için iyileştirme potansiyeli barındırmaktadır.

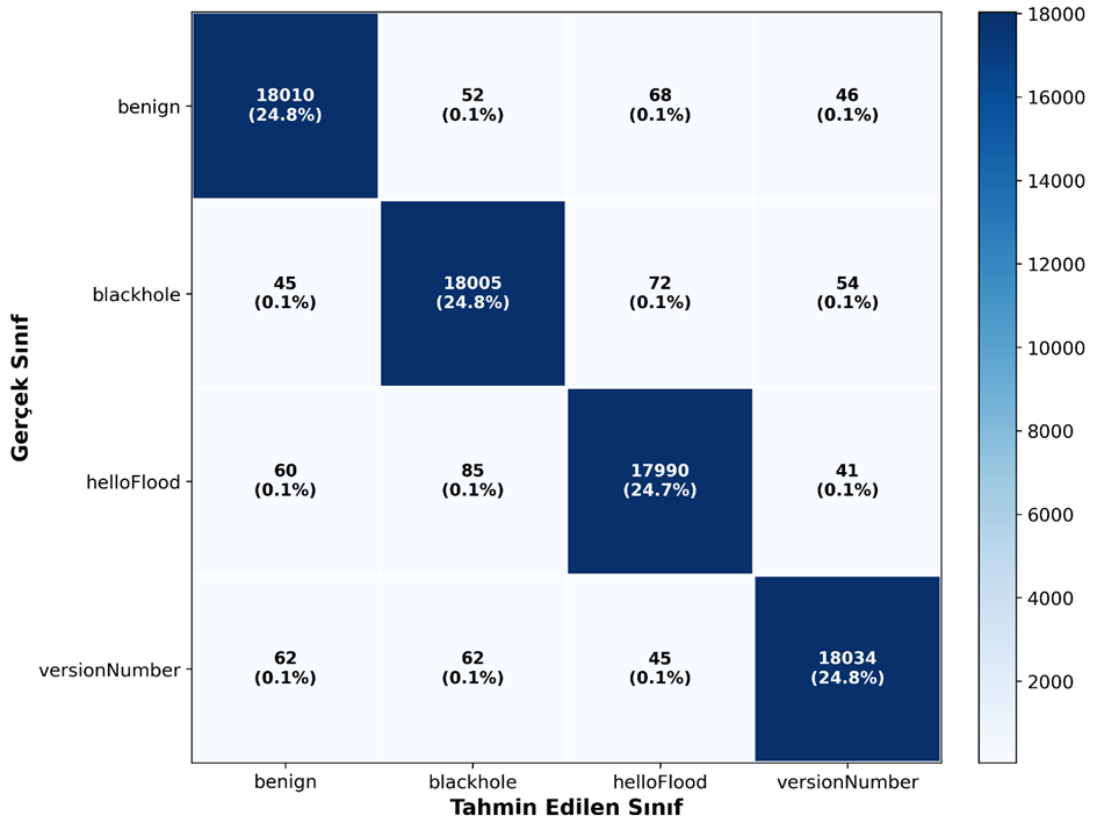
XGBoost algoritması, yalnızca 1,21 saniyelik test süresi ile bu çalışma kapsamında en hızlı sınıflandırma süresine ulaşmıştır. Bu hız, özellikle saldırı tespiti konusunda gerçek zamanlı tepki verilmesi gereken uygulamalarda XGBoost'u oldukça cazip bir seçenek haline getirmektedir. Ayrıca, %98,78 doğruluk, %97,84 F1 skoru, %97,79 precision, %97,89 recall ve %99,25 AUC gibi istatistiksel olarak güçlü metriklerle desteklenen bu performans, düşük test süresine rağmen sınıflandırma güvenilirliğinden ödün verilmediğini ortaya koymaktadır. Eğitim süresi 100,35 saniye ile orta seviyede kalmış ve modelin yeniden eğitilmesi gereken durumlarda bile kabul edilebilir bir süre sunmuştur.

LightGBM algoritması, bu çalışmada eğitim süresi açısından en avantajlı model olarak ön plana çıkmıştır. Sadece 21,06 saniyelik eğitim süresi ile veri işleme açısından önemli ölçüde kaynak tasarrufu sağlamış; aynı zamanda 5,45 saniyelik test süresi ile düşük gecikme gerektiren uygulamalar için uygunluk göstermiştir. Ancak doğruluk değerinin %96,56, F1 skorunun ise %96,68 seviyelerinde kalması, bu modelin daha çok orta düzey hassasiyet gerektiren uygulamalarda tercih edilmesi gerektiğini göstermektedir. AUC değerinin 0.9865 olması, genel başarıyı desteklemekle birlikte özellikle yüksek güvenlik gerektiren durumlar için yeterli ayrıştırıcılık sağlamayabileceğini ortaya koymaktadır.

LSTM algoritması, zamansal bağımlılıkları modelleme konusundaki gücünü bu çalışmada da ortaya koymuştur. %98,12 doğruluk, %97,68 F1 skoru, %97,75 precision, %97,83 recall ve %99,41 AUC değerleri ile genel olarak güçlü bir performans sunmaktadır. Eğitim süresi 244,50 saniye, test süresi ise 7,22 saniye olarak ölçülmüş olup, bu süreler BiLSTM'den daha kısa olmakla birlikte XGBoost ile kıyaslandığında hala belirli bir işlem yükü taşımaktadır. Dolayısıyla LSTM, doğruluk ve işlem süresi arasında dengeli bir çözüm sunmakla birlikte, çok düşük gecikme gerektiren sistemlerde optimizasyon gerektirebilir.

Algoritmaların saldırı türlerine göre sınıflandırma performansları, sınıf bazlı doğruluk ve hata oranlarının ayrıntılı bir şekilde değerlendirilebildiği karmaşıklık matrisleri (confusion matrices) aracılığıyla analiz edilmiştir. Şekil 3.22 incelendiğinde, BiLSTM algoritmasının dört farklı sınıf (benign, blackhole, helloFlood,

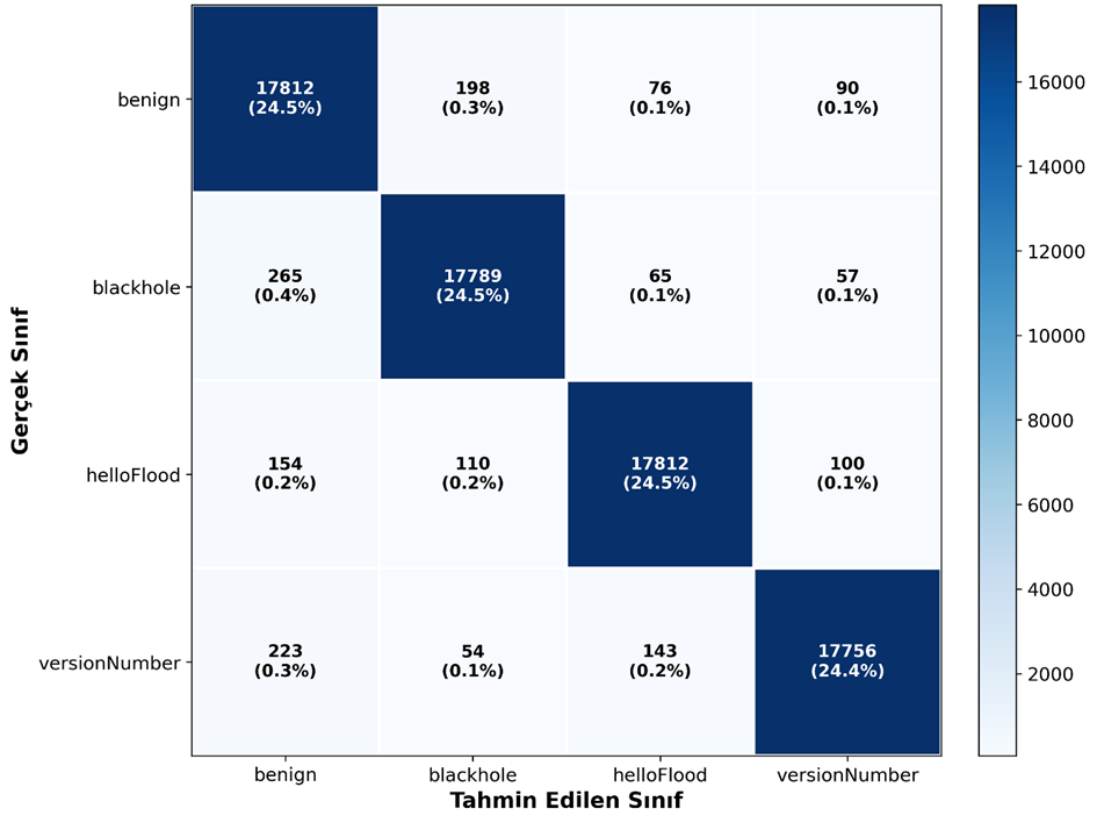
versionNumber) arasında oldukça başarılı bir ayırım yaptığı dikkat çekmektedir. Özellikle benign sınıfta 18.010 doğru tahmin ile yalnızca toplamda 166 örnekte yanlış sınıflandırma gerçekleşmiş, bu da %99'un üzerinde bir başarıya işaret etmektedir. Benzer şekilde, blackhole sınıfta 18.005 doğru sınıflandırma yapılmış, yalnızca 171 örnek diğer sınıflarla karıştırılmıştır. HelloFlood sınıfta da 17.990 doğru tahmin ile yüksek başarı sağlanmış olup hata oranı %0.3'ün altında kalmıştır. VersionNumber saldırılarında ise 18.034 doğru sınıflama yapılırken yalnızca 169 örnek farklı sınıflara hatalı atanmıştır. Bu sonuçlar, BiLSTM algoritmasının özellikle sınıf dengesinin sağlandığı homojen veri setlerinde yüksek duyarlılık ve özgüllük ile çalışabildiğini göstermektedir.



Şekil 3.22. BiLSTM karmaşıklık matrisi

XGBoost algoritmasının saldırı türlerine göre sınıflandırma performansı, Şekil 3.23'te yer alan detaylı sınıf dağılımları üzerinden analiz edilmiştir. Karmaşıklık Matrisi verilerine göre XGBoost, genel doğruluk açısından tatmin edici bir başarı sergilese de, sınıf bazlı değerlendirmelerde BiLSTM'e kıyasla daha yüksek oranda çapraz sınıflandırma hataları üretmiştir. Benign sınıfta 17.812'si doğru şekilde

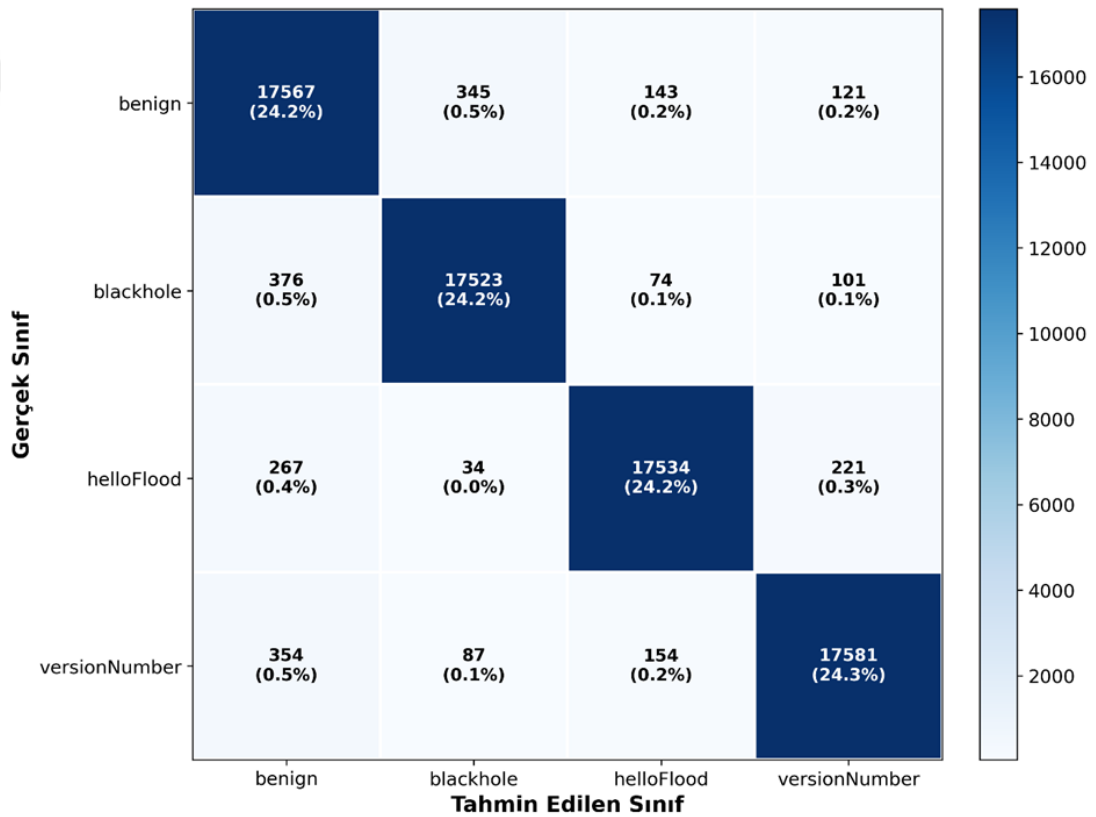
tanımlanmış, ancak 198 örnek blackhole, 76 örnek helloFlood ve 90 örnek versionNumber sınıfı ile karıştırılmıştır. Blackhole sınıfında ise 17.789 doğru tahmine karşın 265 örnek benign, 65 helloFlood ve 57 versionNumber olarak hatalı sınıflandırılmıştır. HelloFlood sınıfı için model 17.812 doğru sınıflandırma gerçekleştirmiş olsa da 364 örnekte yanlış etiketleme tespit edilmiştir. VersionNumber sınıfında ise 17.756 örnek doğru şekilde tanımlanmışken, toplam 420 örnek farklı sınıflar ile karıştırılmıştır. XGBoost'un bu sınıflandırma performansı, modelin yüksek işlem verimliliği ve test süresi avantajı ile birlikte değerlendirildiğinde, gerçek zamanlı uygulamalarda hızlı tepki gerektiren senaryolar için tercih edilebilirliğini koruduğunu göstermektedir.



Şekil 3.23. XGBoost karmaşıklık matrisi

LightGBM algoritmasının saldırı türlerini sınıflandırma başarımı, Şekil 3.24 üzerinde yapılan ayrıntılı analizle değerlendirilmiştir. Karmaşıklık Matrisi verileri, LightGBM'nin genel doğruluk açısından kabul edilebilir bir performans sunduğunu, ancak özellikle benign ve versionNumber sınıfları arasında hatalı sınıflandırma eğilimlerinin diğer algoritmalarla kıyasla daha yüksek düzeyde olduğunu

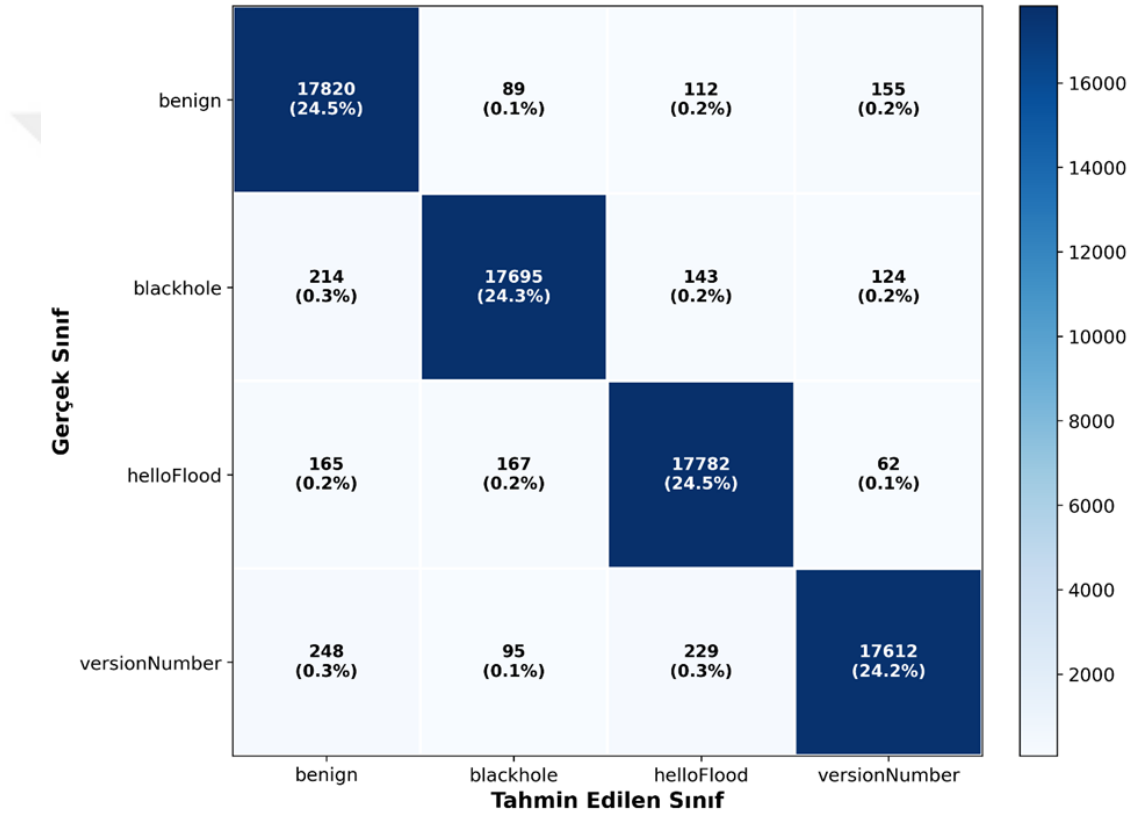
göstermektedir. Benign sınıfında, 17.567 örnek doğru şekilde tahmin edilirken, toplamda 609 örnek farklı sınıflar ile karıştırılmıştır. Blackhole sınıfında ise 17.523 doğru sınıflandırmanın yanı sıra, 551 örnek hatalı tahmin edilmiştir. HelloFlood sınıfında 17.534 doğru sınıflandırmaya karşılık 522 örnek hatalı sınıflandırma gözlemlenmiştir. VersionNumber sınıfında ise 17.581 örnek doğru tanımlanmış, 595 örnek farklı sınıflara yönelmiştir. Genel olarak LightGBM, sınıf dengesi sağlanmış bir veri seti üzerinde tutarlı performans sergilese de, sınıflar arası karışıklık oranlarının BiLSTM ve XGBoost'a kıyasla biraz daha yüksek olduğu dikkat çekmektedir.



Şekil 3.24. LightGBM Karmaşıklık matrisi

LSTM (Long Short-Term Memory) algoritmasının saldırı türlerine göre sınıflandırma performansı, Şekil 3.25 üzerinden ayrıntılı biçimde değerlendirilmiştir. Karmaşıklık Matrisi çıktıları, LSTM'in genel sınıflandırma doğruluğunun yüksek olduğunu, ancak bazı sınıflar arasında kısmi karışıklıkların gözlemlendiğini ortaya koymaktadır. Benign sınıfı için 17.820 doğru sınıflandırma yapılmış olup; 89 blackhole, 112 helloFlood ve 155 versionNumber örneğiyle toplamda 356 hatalı tahmin gerçekleştirilmiştir. Blackhole sınıfında 17.695 doğru sınıflandırmaya karşılık,

214 benign, 143 helloFlood ve 124 versionNumber örneği yanlış sınıflanmıştır. HelloFlood sınıfında 17.782 örnek doğru tahmin edilirken, özellikle blackhole sınıfına yönelik 167 örneklilik yanlış sınıflandırma dikkat çekicidir. VersionNumber sınıfında ise 17.612 örnek doğru etiketlenmiş, 572 örnek farklı sınıflara yönlendirilmiştir. LSTM algoritmasının bu performansı, modelin zamansal bağımlılığı başarılı bir şekilde modellediğini, ancak sınıf ayrıştırma açısından BiLSTM kadar keskin olmadığını göstermektedir.



Şekil 3.25. LSTM karmaşıklık matrisi

Çalışmada elde edilen sonuçlar doğrultusunda, IoT ağlarında gözlemlenen farklı saldırı türlerinin tespitine yönelik kullanılan algoritmaların güçlü ve sınırlı yönleri detaylı biçimde analiz edilmiştir. Bu kapsamlı inceleme, yalnızca doğruluk oranı ya da işlem süresi gibi metriklerle sınırlı kalmayıp; her bir algoritmanın uygulama alanına uygunluğunu, kaynak tüketimini ve gerçek zamanlı tepki kapasitesini de dikkate almıştır. Elde edilen bulgular, algoritma seçiminde doğruluk, hız ve kaynak etkinliği parametrelerinin yanı sıra, uygulama bağlamının da dikkate alınmasının zorunlu olduğunu ortaya koymaktadır.

SONUÇLAR VE ÖNERİLER

Bu yüksek lisans tezi, RPL (Routing Protocol for Low-Power and Lossy Networks) tabanlı Nesnelerin İnterneti (IoT) ağlarında Blackhole, HelloFlood ve Version Number saldırılarının ağın yönlendirme yapısı ve enerji tüketimi üzerindeki etkilerini kapsamlı bir şekilde incelemiştir. Contiki 3.0 işletim sistemi ve Cooja simülatörü kullanılarak gerçekleştirilen simülasyonlar, bu saldırıların ağ üzerindeki yapısal ve performans odaklı etkilerini ortaya koymuş; aynı zamanda ağ trafiği verilerinden yararlanılarak makine öğrenmesi ve derin öğrenme teknikleri ile saldırıların otomatik tespiti sağlanmıştır. Çalışmada kullanılan Powertrace, Wireshark ve Foren6 gibi araçlar, enerji tüketimi analizi, ağ trafiği izleme ve DODAG yapısının görselleştirilmesi gibi çok yönlü bir değerlendirme imkânı sunmuştur. Elde edilen bulgular, bu saldırıların RPL tabanlı IoT ağlarında ciddi güvenlik tehditleri oluşturduğunu ve ağın işlevselliğini, güvenilirliğini ve sürdürülebilirliğini olumsuz yönde etkilediğini açıkça göstermiştir.

Simülasyonlar, 52 düğümden oluşan bir ağ modeli üzerinde gerçekleştirilmiş ve Blackhole saldırısının, kötü niyetli bir düğümün sahte yönlendirme avantajlarıyla veri paketlerini düşürmesiyle ağda veri kaybına ve iletişim kopukluklarına yol açtığı doğrulanmıştır. HelloFlood saldırısı, yüksek güçlü DIS mesajlarının yayılmasıyla ağ topolojisini bozmuş, düğümlerin enerji tüketimini artırarak ağın sürdürülebilirliğini tehdit etmiştir. Version Number saldırısı ise, sahte DIO mesajlarıyla DODAG yapısında tutarsızlıklar yaratarak sürekli yeniden yapılandırma süreçlerini tetiklemiş ve bu durum hem yönlendirme süreçlerini aksatmış hem de enerji tüketimini ciddi şekilde yükseltmiştir. Powertrace analizleri, saldırıların enerji tüketiminde %30-60 oranında artışlara neden olduğunu ortaya koymuş; Wireshark ve Foren6 verileri ise ağ trafiği yoğunluğunda ve topolojik kararsızlıkta belirgin bozulmalar olduğunu kanıtlamıştır. Bu sonuçlar, RPL protokolünün güvenlik açıklarının IoT ağları üzerindeki yıkıcı etkilerini açıkça ortaya koymakta ve bu tür tehditlere karşı etkin çözümler geliştirilmesinin aciliyetini vurgulamaktadır.

Makine öğrenmesi ve derin öğrenme modelleri, saldırıların otomatik tespiti konusunda etkili bir çözüm sunmuştur. Çalışmada, BiLSTM, LSTM, XGBoost ve LightGBM modelleri karşılaştırmalı olarak değerlendirilmiş ve performansları

doğruluk, F1 skoru, precision, recall ve AUC metrikleri üzerinden analiz edilmiştir. BiLSTM, %99,02 doğruluk, %98,85 F1 skoru ve %99,83 AUC değerleriyle en yüksek performansı sergilemiş; çift yönlü bilgi işleme kapasitesi sayesinde ağ trafiğindeki zamansal örüntüleri başarıyla modellemiştir. Ancak, 390,76 saniyelik eğitim süresi, gerçek zamanlı uygulamalarda kullanılabilirliğini sınırlandıran bir faktör olarak öne çıkmıştır. XGBoost, 1,21 saniyelik test süresi ve %98,78 doğruluk ile hızlı tepki gerektiren senaryolarda güçlü bir alternatif sunmuş; LightGBM ise 21,06 saniyelik eğitim süresi ile kaynak verimliliği açısından avantaj sağlamış, ancak %96,56 doğruluk ile orta düzey bir performans sergilemiştir. LSTM, %98,12 doğruluk ile dengeli bir sonuç vermiş, fakat BiLSTM'e kıyasla daha az ayırıştırıcı olmuştur. Bu bulgular, model seçiminde doğruluk, hız ve hesaplama maliyeti gibi parametrelerin uygulama bağlamına göre dengelenmesi gerektiğini göstermektedir.

Tezin sonuçları, RPL tabanlı IoT ağlarının güvenlik açıklarını kapatmak ve ağ performansını korumak için makine öğrenmesi tabanlı yaklaşımların potansiyelini ortaya koymaktadır. BiLSTM'in yüksek doğruluğu, karmaşık saldırı örüntülerinin tespitinde derin öğrenme modellerinin üstünlüğünü kanıtlarken; XGBoost'un hızı, gerçek zamanlı sistemlerde pratik bir çözüm sunmaktadır. Bununla birlikte, modellerin hesaplama karmaşıklığı ve eğitim süreleri, özellikle kaynak kısıtlı IoT cihazlarında uygulanabilirliklerini sınırlamaktadır. Ayrıca, sınıf dengesizliği ve sıfır-gün tehditleri gibi zorluklar, mevcut modellerin genel güvenilirliğini sınanan unsurlar olarak dikkat çekmektedir. Bu bağlamda, tez, RPL protokolünün güvenlik açıklarının yalnızca tespit değil, aynı zamanda önleme odaklı yaklaşımlarla ele alınması gerektiğini vurgulamaktadır.

Gelecekteki çalışmalar için, makine öğrenmesi modellerinin hesaplama karmaşıklığını azaltmaya ve gerçek zamanlı uygulamalarda kullanılabilirliğini artırmaya yönelik optimizasyon çalışmaları önerilmektedir. Özellikle, BiLSTM gibi yüksek performanslı modellerin eğitim sürelerini kısaltmak amacıyla hafifletilmiş (lightweight) versiyonlarının geliştirilmesi, IoT ağlarının dinamik doğasına daha uygun çözümler sunabilir. Bunun yanı sıra, sınıf dengesizliği ve sıfır-gün tehditlerine karşı dirençli yeni nesil makine öğrenmesi teknikleri üzerinde durulması gerekmektedir; bu kapsamda, federated learning gibi merkezi olmayan yaklaşımlar, veri gizliliğini korurken ağ genelinde işbirlikçi bir güvenlik modeli oluşturma

potansiyeline sahiptir. RPL protokolünün güvenlik açıklarını kökten ele alan yeni nesil yönlendirme protokollerinin tasarlanması da önemli bir araştırma alanı olarak öne çıkmaktadır. Bu tür protokoller, enerji verimliliği ile güvenliği dengeleyen mekanizmalar içermeli ve IoT ağlarının heterojen yapısına uyum sağlamalıdır. Son olarak, IoT ağlarının güvenlik standartlarının güncellenmesi ve 5G entegrasyonu gibi teknolojik gelişmelere paralel olarak çok katmanlı bir güvenlik çerçevesinin geliştirilmesi, bu alanda sürdürülebilir bir ilerleme için kritik bir gereklilik olarak değerlendirilmektedir.

Bu tez, RPL tabanlı IoT ağlarının güvenlik sorunlarına yönelik bütüncül bir bakış açısı sunmuş ve makine öğrenmesi tabanlı tespit yöntemlerinin bu tehditlere karşı etkinliğini kanıtlamıştır. Elde edilen bulgular, IoT ekosisteminin gelecekteki gelişiminde güvenlik odaklı yaklaşımların önemini pekiştirmekte ve bu alanda yapılacak araştırmalara sağlam bir temel sağlamaktadır. Önerilen yaklaşımlar, hem akademik hem de endüstriyel bağlamda IoT ağlarının güvenilirliğini ve sürdürülebilirliğini artırmaya yönelik somut adımlar olarak değer taşımaktadır.

KAYNAKÇA

- Ahmed, F., & Ko, Y.-B. (2016). Mitigation of black hole attacks in routing protocol for low-power and lossy networks. *Security and Communication Networks*, 9(18), 5143–5154.
- Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials*, 17(4), 2347–2376.
- Alrowais, F. M., Althahabi, S., Alotaibi, S. S., Mohamed, A., Hamza, M. A., & Marzouk, R. (2023). Automated machine learning enabled cybersecurity threat detection in Internet of Things environment. *Computer Systems Science & Engineering*, 45(1), 687–700.
- Alsaedi, A., Moustafa, N., Tari, Z., Mahmood, A., & Anwar, A. (2020). TON_IoT telemetry dataset: A new generation dataset of IoT and IIoT for data-driven intrusion detection systems. *IEEE Access*, 8, 165130–165150.
- Al-Salim, A. M., Lawey, A. Q., El-Gorashi, T. E., & Elmirghani, J. M. (2017). Energy efficient big data networks: Impact of volume and variety. *IEEE Transactions on Network and Service Management*, 15(1), 458–474.
- Ammar, M., Russello, G., & Crispo, B. (2018). Internet of Things: A survey on the security of IoT frameworks. *Journal of Information Security and Applications*, 38, 8–27.
- Anastasi, G., Conti, M., Di Francesco, M., & Passarella, A. (2009). Energy conservation in wireless sensor networks: A survey. *Ad Hoc Networks*, 7(3), 537–568.
- Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, 54(15), 2787–2805.
- Baccelli, E., Hahm, O., Gunes, M., Wahlish, M., & Schmidt, T. C. (2013). RIOT OS: Towards an OS for the Internet of Things. *Computer Communications*, 36(9), 934–946.
- Bhadauria, R., & Sanyal, S. (2012). Survey on security issues in cloud computing and associated mitigation techniques. *International Journal of Computer Applications*, 47(18), 47–66.
- Bhattasali, T., Chaki, R., & Chaki, N. (2013). Secure and trusted cloud of things. *Procedia Technology*, 10, 913–920.
- Bostani, H., & Sheikhan, M. (2017). Hybrid of anomaly-based and specification-based IDS for Internet of Things using unsupervised OPF based on MapReduce approach. *Computer Communications*, 98, 52–71.

- Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials*, 18(2), 1153–1176.
- Canedo, J., & Skjellum, A. (2016). Using machine learning to secure IoT systems. *Procedia Computer Science*, 100, 219–222.
- Careem, R., Johar, G., & Khatibi, A. (2024). Deep neural networks optimization for resource-constrained environments: Techniques and models. *Indonesian Journal of Electrical Engineering and Computer Science*, 33(3), 1843–1854.
- Chen, T., & Guestrin, C. (2016). XGBoost: A scalable tree boosting system. *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 785–794.
- Demirkol, I., Ersoy, C., & Alagoz, F. (2006). MAC protocols for wireless sensor networks: A survey. *IEEE Communications Magazine*, 44(4), 115–121.
- Djedjig, N., Tandjaoui, D., Romdhani, I., & Medjek, F. (2017). New trust metric for the RPL routing protocol in IoT. *International Journal of Advanced Computer Science and Applications*, 8(11), 417–425.
- Ferdowsi, A., Challita, U., Saad, W., & Mandayam, N. B. (2018). Robust deep reinforcement learning for security and safety in autonomous IoT systems. *IEEE Internet of Things Journal*, 6(2), 2040–2050.
- Gaddour, M., & Koubâa, A. (2012). RPL in a nutshell: A survey. *Computer Networks*, 56(14), 3163–3178.
- Goswami, A., & Ghoshal, N. (2016). Imperceptible image authentication using wavelets. *International Journal of Network Security*, 18(5), 861–873.
- Graves, A., & Schmidhuber, J. (2005). Framewise phoneme classification with bidirectional LSTM and other neural network architectures. *Neural Networks*, 18(5-6), 602–610.
- Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7), 1645–1660.
- Hahm, O., Baccelli, E., Petersen, H., & Tsiftes, N. (2016). Operating systems for low-end devices in the Internet of Things: A survey. *IEEE Internet of Things Journal*, 3(5), 720–734.
- Hochreiter, S., & Schmidhuber, J. (1997). Long short-term memory. *Neural Computation*, 9(8), 1735–1780.
- Hossain, M. M., Fotouhi, M., & Hasan, R. (2018). Towards an analysis of security issues, challenges, and open problems in the Internet of Things. *IEEE Access*, 6, 72469–72478.

- Hussain, F., Abbas, S. G., Shah, G. A., Pires, I. M., Fayyaz, U. U., Shahzad, F., Garcia, N. M., & Zdravevski, E. (2021). A framework for malicious traffic detection in IoT networks. *Sensors*, 21(9), 3025.
- Ke, G., Meng, Q., Finley, T., Wang, T., Chen, W., Ma, W., ... & Liu, T. Y. (2017). LightGBM: A highly efficient gradient boosting decision tree. In *Advances in Neural Information Processing Systems*, 30.
- Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, 82, 395–411.
- Kim, H. S., Ko, J., Culler, D. E., & Paek, J. (2017). Challenging the IPv6 routing protocol for low-power and lossy networks (RPL): A survey. *IEEE Communications Surveys & Tutorials*, 19(4), 2502–2525.
- Kirsche, M., & Klauck, R. (2012). Unify to bridge gaps: Bringing XMPP into the Internet of Things. *Pervasive and Mobile Computing*, 8(5), 793–805.
- Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. *Computer*, 50(7), 80–84.
- Krzywiecki, Ł., Bobowski, A., Słowik, M., Słowik, M., & Kozieł, P. (2020). Schnorr-like identification scheme resistant to malicious subliminal setting of ephemeral secret. *Computer Networks*, 179, 107346.
- Lamaazi, H., & Benamar, N. (2018). A comprehensive survey on enhancements and limitations of the RPL protocol: A focus on the objective function. *Ad Hoc Networks*, 80, 1–17.
- Li, S., Da Xu, L., & Zhao, S. (2018). 5G Internet of Things: A survey. *Journal of Industrial Information Integration*, 10, 1–9.
- Li, S., Iqbal, M., & Saxena, N. (2024). Future industry Internet of Things with zero-trust security. *Information Systems Frontiers*, 26(5), 1653–1666.
- Liu, G., Wang, C., Ma, X., & Yang, Y. (2021). Keep your data locally: Federated-learning-based data privacy preservation in edge computing. *IEEE Network*, 35(2), 60–66.
- Liu, X., Sheng, Z., & Yin, C. (2017). Routing protocol for low power and lossy IoT networks. In D. Bandyopadhyay & J. Sen (Eds.), *From Internet of Things to Smart Cities* (pp. 89–118). Chapman and Hall/CRC.
- Maimó, L. F., Gómez, Á. L. P., Clemente, F. J. G., Pérez, M. G., & Pérez, G. M. (2018). A self-adaptive deep learning-based system for anomaly detection in 5G networks. *IEEE Access*, 6, 7700–7712.
- Marjani, M., Nasaruddin, F., Gani, A., Karim, A., Hashem, I. A. T., Siddiqa, A., & Yaqoob, I. (2017). Big IoT data analytics: Architecture, opportunities, and open research challenges. *IEEE Access*, 5, 5247–5261.

- Mayzaud, A., Badonnel, R., & Chrisment, I. (2016). A taxonomy of attacks in RPL-based Internet of Things. *International Journal of Network Security*, 18(3), 459–473.
- Meidan, Y., Bohadana, M., Mathur, A., Shabtai, A., & Elovici, Y. (2018). N-BaIoT—Network-based detection of IoT botnet attacks using deep autoencoders. *IEEE Pervasive Computing*, 17(3), 12–22.
- Mendez Mena, D., Papapanagiotou, I., & Yang, B. (2018). Internet of Things: Survey on security. *Information Security Journal: A Global Perspective*, 27(3), 162–182.
- Mishra, A., Alwasel, B., & Nepal, S. (2016). IoTSim: A simulator for analyzing IoT applications. *Journal of Systems Architecture*, 72, 93–103.
- Mosenia, A., & Jha, N. K. (2017). A comprehensive study of security of Internet-of-Things. *IEEE Transactions on Emerging Topics in Computing*, 5(4), 586–602.
- Musznicki, B., & Zwierzykowski, P. (2012). Survey of simulators for wireless sensor networks. *International Journal of Grid and Distributed Computing*, 5(3), 23–50.
- Nath, A. (2015). *Packet analysis with Wireshark*. Packt Publishing Ltd.
- Österlind, F., Dunkels, A., Eriksson, J., Finne, N., & Voigt, T. (2006). Cross-level sensor network simulation with Cooja. *IEEE Transactions on Mobile Computing*, 5(8), 1063–1074.
- Popoola, S. I., Adebisi, B., Hammoudeh, M., Gui, G., & Gacanin, H. (2021). Hybrid deep learning for botnet attack detection in the Internet of Things networks. *IEEE Internet of Things Journal*, 8(6), 4944–4956.
- Pundir, S., Wazid, M., Singh, D. P., Das, A. K., Rodrigues, J. J., & Park, Y. (2019). Intrusion detection protocols in wireless sensor networks integrated to Internet of Things deployment: Survey and future challenges. *IEEE Access*, 8, 3343–3363.
- Raghavendra, T., Anand, M., Selvi, M., Thangaramya, K., Kumar, S. S., & Kannan, A. (2022). An intelligent RPL attack detection using machine learning-based intrusion detection system for Internet of Things. *Procedia Computer Science*, 215, 61–70.
- Raoof, A., Matrawy, A., & Lung, C.-H. (2018). Routing attacks and mitigation methods for RPL-based Internet of Things. *IEEE Communications Surveys & Tutorials*, 21(2), 1582–1606.
- Rault, T., Bouabdallah, A., & Challal, Y. (2014). Energy efficiency in wireless sensor networks: A top-down survey. *Computer Networks*, 67, 104–122.
- Raza, S., Wallgren, L., & Voigt, T. (2013). SVELTE: Real-time intrusion detection in the Internet of Things. *Ad Hoc Networks*, 11(8), 2661–2674.

- Rejeb, S. B., Nasser, N., Mansour, S., & Boujlbane, M. (2017). Centralized SON function for operator optimal strategies in heterogeneous networks. *Computer Networks*, 128, 14–27.
- Rey, V., Sánchez, P. M. S., Celdrán, A. H., & Bovet, G. (2022). Federated learning for malware detection in IoT devices. *Computer Networks*, 204, 108693.
- Rodenas-Herráiz, D., Fidler, P. R., Feng, T., Xu, X., Nawaz, S., & Soga, K. (2017, February). *A handheld diagnostic system for 6LoWPAN networks*. In *2017 13th Annual Conference on Wireless On-demand Network Systems and Services (WONS)* (pp. 104–111).
- Saadeh, M., Sleit, A., Sabri, K. E., & Almobaideen, W. (2018). Hierarchical architecture and protocol for mobile object authentication in the context of IoT smart cities. *Journal of Network and Computer Applications*, 121, 1–19.
- Safaei, B., Monazzah, A. M. H., Bafroei, M. B., & Ejlali, A. (2017, December). *Reliability side-effects in Internet of Things application layer protocols*. In *2017 2nd International Conference on System Reliability and Safety (ICSRS)* (pp. 207–212).
- Saied, M., Guirguis, S., & Madbouly, M. (2023). A comparative study of using boosting-based machine learning algorithms for IoT network intrusion detection. *International Journal of Computational Intelligence Systems*, 16(1), 177.
- Sehrawat, A., Gill, N. S., & Singh, M. (2019). A survey on security issues and attacks in RPL-based Internet of Things. *International Journal of Advanced Computer Science and Applications*, 10(8), 462–469.
- Shafique, K., Khawaja, B. A., Sabir, F., Qazi, S., & Mustaqim, M. (2020). Internet of Things (IoT) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5G-IoT scenarios. *IEEE Access*, 8, 23022–23040.
- Shahid, M. H., Hameed, A. R., ul Islam, S., Khattak, H. A., Din, I. U., & Rodrigues, J. J. (2020). Energy and delay efficient fog computing using caching mechanism. *Computer Communications*, 154, 534–541.
- Sharma, H., & Yadav, G. S. (2025). Privacy-preserving intrusion detection with federated learning: Enhancing privacy and efficiency in IoT networks. *International Journal of Machine Learning and Cybernetics*, 1–19.
- Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, 76, 146–164.
- Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. *IEEE Symposium on Security and Privacy*, 305–316.

- Thubert, P. (2012). Objective function zero for the routing protocol for low-power and lossy networks (RPL). *IEEE Internet of Things Journal*, 1(1), 1–10.
- Vasseur, J.-P., Kim, M., Pister, K., Dejean, N., & Barthel, D. (2011). Routing metrics used for path calculation in low-power and lossy networks. *IEEE Transactions on Networking*, 19(6), 1762–1775.
- Verma, A., & Ranga, V. (2019). ELNIDS: Ensemble learning based network intrusion detection system for RPL based Internet of Things. *Proceedings of the 4th IEEE International Conference on Internet of Things: Smart Innovation and Usages*, 1–6.
- Wang, Z., Chen, H., Yang, S., Luo, X., Li, D., & Wang, J. (2023). A lightweight intrusion detection method for IoT based on deep learning and dynamic quantization. *PeerJ Computer Science*, 9, e1569.
- Xu, L. D., Xu, E. L., & Li, L. (2018). Industry 4.0: State of the art and future trends. *International Journal of Production Research*, 56(8), 2941–2962.
- Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). Federated machine learning: Concept and applications. *ACM Transactions on Intelligent Systems and Technology*, 10(2), 1–19.
- Ziegeldorf, J. H., Morchon, O. G., & Wehrle, K. (2014). Privacy in the Internet of Things: Threats and challenges. *Security and Communication Networks*, 7(12), 2728–2742.

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı : TAŞTAN, Ahmet Nail
Uyruğu : T.C.

Eğitim

Derece	Eğitim Birimi	Mezuniyet Tarihi
Yüksek lisans	İstanbul Gelişim Üniversitesi Bilgisayar Mühendisliği	2025
Lisans	İstanbul Gelişim Üniversitesi Bilgisayar Mühendisliği	2022
Lise	Özel Çatalca Sınav Temel Lisesi	2018

İş Deneyimi

Yıl	Yer	Görev
2023-Halen	İstanbul Gelişim Üniversitesi	Araştırma Görevlisi

Yabancı Dil

Türkçe: Ana dil,
İngilizce: B1

Yayınlar

Taştan, A. N., Gönen, S., Barışkan, M. A., Kubat, C., Kaplan, D. Y., & Pashaei, E. (2023, May). Detection of man-in-the-middle attack through artificial intelligence algorithm. In International Symposium on Intelligent Manufacturing and Service Systems (pp. 450-458). Singapore: Springer Nature Singapore.

Hobiler

Teknoloji, yüzme,doğa yürüyüşü.

