Journal of Natural and Engineering Research

JNER, 2025, 1 (1): 30-37

Analysis of Attack Methodologies in IoT Networks and Examination of RT-IoT2022

Gözde Sarıaslan [1*]

[1] Department of Computer Engineering, Iskenderun Technical University, Hatay, Türkiye.

ABSTRACT

This study aims to analyze the monitoring of network traffic and the detection of security incidents arising from the widespread use of Internet of Things (IoT) devices, which, despite making daily life more convenient, also pose significant security risks. Methodologies such as DDoS, data exfiltration, spoofing, scanning, and brute-force attacks occurring within a network threaten both individual users and corporate systems. In this study, the RT-IoT2022 dataset derived from a real-time IoT infrastructure and containing both normal and malicious network behaviors consistent with real-world scenarios has been utilized. By using this dataset, the objective is to examine attack methodologies on IoT network traffic through machine learning techniques and to propose an effective detection model capable of identifying various types of attacks.

ARTICLE INFO

Received 23.11.2025,
Accepted 20.12.2025,
Publication Date 25.12.2025

Keywords:

IoT, Machine Learning, Network Traffic Security, RT-IoT2022

*Corresponding Author: Gözde SARIASLAN, E-mail: gozdesariaslan.lee24@iste.edu.tr

IoT Ağlarında Saldırı Metodolojilerinin Analizi ve RT-IoT2022 İncelemesi

ÖZET

Bu çalışma, günümüzde yaygın bir şekilde kullanılan nesnelerin interneti (Internet of Things, IoT) tabanlı cihazların hayatı kolaylaştırmasının yanı sıra güvenlik açısından ciddi riskleri barındırmasından kaynaklı bu ağ trafiğinin izlenmesi ve güvenlik olaylarının tespitini analiz etmeyi amaçlamaktadır. Ağ üzerinde gerçekleşen DDoS, bilgi sızdırma, spoofing, tarama ve brute-force gibi metodolojiler hem bireysel kullanıcıları hem de kurumsal sistemleri tehdit etmektedir. Bu çalışmada, RT-IoT2022, gerçek zamanlı bir IoT alt yapısında türetilmiş, hem normal hem de saldırgan ağ davranışlarını içeren gerçek dünya ile uyumlu bir veri seti kullanılmıştır. Bu veri seti kullanılarak IoT ağ trafiği üzerindeki saldırı metodolojilerini makine öğrenmesi teknikleri ile inceleyerek farklı saldırı türlerine karşı etkin bir tespit modeli önerilmesi hedeflenmektedir.

MAKALE BİLGİSİ

Received 23.11.2025,
Accepted 20.12.2025,
Publication Date 25.12.2025

Anahtar Kelimeler:

IoT, Makine Öğrenmesi, Ağ Trafiği Güvenliği, RT-IoT2022

GİRİŞ

IoT cihazlarının kullanımı gittikçe yaygınlaşmakta ve bu cihazlar akıllı ev uygulamalarından, endüstriyel kontrol sistemlerine kadar geniş bir yelpazeye yayılmaktadır. Bu yaygın kullanım beraberinde ciddi güvenlik risklerini getirmektedir. IoT cihazlarının genellikle düşük maliyetli, düşük işlem gücüne ve zayıf güvenlik yapısına sahip olması bu cihazları çeşitli saldırıların hedefi haline getirmiştir.

Geleneksel güvenlik çözümleri, sabit kural tabanlı yaklaşımlar IoT cihazlarından gelen büyük hacimli ağ trafiğini analiz etmekte yetersiz kalabilir. Bu yaklaşım ve çözümlerin yetersiz kaldığı noktada devreye yapay zeka ve makine öğrenmesi yöntemleri girmektedir. Bu yöntemler zayıf yapılandırılmış veri içindeki anormal örüntülerin tespit edilmesi ve saldırı sınıflandırması gibi görevlerde güçlü bir alternatif sunmaktadır.

Literatürde IoT ağ trafiği analizi ve saldırıların tespiti üzerine yapılan çalışmalar, gerçekçi veri kümeleri kullanılarak makine öğrenmesi modellerinin etkinliğini ortaya koymaktadır. Bu alanda yapılan çalışmalardan Elzaghmouri ve arkadaşları (2024), gerçek IoT ortamlarını temsil eden RT-IoT2022 veri seti üzerinde CNN, BLSTM, GRU ve dikkat mekanizmasını birleştiren hibrit bir

makine öğrenme mimarisi önermiş ve e %99.6'nın üzerinde doğruluk elde ederek çözümlerin yüksek tespit kapasitesini göstermiştir. Bu ve benzer çalışmalar RT-IoT2022 veri setinin farklı saldırı türlerini temsil etme kapasitesini ve yapay zekâ tabanlı saldırı tespit sistemlerinin IoT güvenliği için güçlü bir alternatif sunduğunu göstermektedir.

Bu çalışmada, RT-IoT2022, gerçek zamanlı bir IoT alt yapısında türetilmiş, hem normal hem de saldırgan ağ davranışlarını içeren gerçek dünya ile uyumlu bir veri seti kullanılarak IoT ağ trafiği üzerindeki saldırı metodolojilerinin makine öğrenmesi teknikleri ile incelenerek analiz edilmesi hedeflenmiştir. İlk olarak veri seti ön işlemeye tabi tutulacak, ardından sınıflandırma ve anomalilerin tespiti için çok katmanlı bir yöntem uygulanacaktır. Veri dengesi, öznitelik seçimi ve karşılaştırmalı algoritma performansı yönlerinden katkı sağlayarak IoT ağı üzerinde farklı saldırı türlerine karşı daha etkin bir tespit modeli önerilmesi hedeflenmektedir.

MATERYAL VE METOD

Veri Seti

Bu çalışmada, IoT ortamlarında hem normal ağ trafiği hem de saldırı altındaki ağ trafiğini içeren RT-IoT2022 veri seti kullanılmaktadır (Sharmila & Nagapadma, 2023). Bu veri seti; 123117 örnek ve 83 değişken içermektedir. Ayrıca veri kümesinde "Benign" (normal) trafik, DoS / DDoS, Recon, Spoofing ve Brute Force gibi saldırı türlerini kapsayan sınıflar yer almaktadır. Bu veri seti, IoT ağlarında gerçekçi bir test ortamı sunarak doğruluğu yüksek sonuçlar almamıza katkı sağlayacaktır.

Yöntemler

Ön İşleme (Pre-Processing)

RT-IoT2022 veri seti; hem sayısal hem kategorik değişkenler içermektedir. Bu nedenle kapsamlı bir ön işleme sürecine girmesi gerekmektedir. Bu aşamada ilk olarak kategorik değişkenler, modellemeye uygun biçimde sayısal formata dönüştürülecektir. Özellikle ağ protokolü ve service gibi nitelikler, label encoding veya embeddings aracılığıyla işlenecektir. Ardından veri kümesinde bulunabilecek aykırı değerler istatistiksel yöntemlerle belirlenerek temizleme ve yeniden ölçeklendirme yapılacaktır.

Öznitelik Seçimi ve Boyut İndirgeme

Veri setinin 80'den fazla değişken içermesi, hem hesaplama maliyetini artırmakta hem de modellerde gereksiz gürültüye neden olabilmektedir. Bu nedenle model eğitiminden önce en etkili özelliklerin belirlenmesi için öznitelik seçimi ve boyut indirgeme yöntemleri uygulanacaktır. Öncelikle Recursive Feature Elimination (RFE) kullanılarak sınıflandırma performansına katkısı düşük olan değişkenler elenecektir. Ayrıca literatürde RT-IoT2022 üzerinde yüksek başarı sağlayan çalışmalar dikkate alınarak en optimal öznitelik alt kümesi araştırılacaktır. Bu araştırma

ve çalışma ile daha yüksek performans sağlayan ve hesaplama yükünü azaltan bir özellik kümesi oluşturulması hedeflenmektedir.

Sınıflandırma ve Modelleme

Ön işleme (pre-processing) ve öznitelik seçimi aşamalarının ardından IoT saldırı tespitine yönelik kullanılmak üzere çeşitli makine öğrenmesi modelleri eğitilecektir. Makine öğrenmesi tarafında Random Forest (RF), Support Vector Machine (SVM) ve XGBoost gibi güçlü sınıflandırıcılar kullanılacaktır. Bu algoritmalar, saldırı türlerinin karar ağaçları, mesafe tabanlı yaklaşımlar, ayrım düzlemleri üzerinden ayrıştırılması için uygun bir temel sağlamaktadır. Otomatik özellik çıkarımı sağlayan autoencoder yapıları, CNN tabanlı modeller, zaman bağımlılıklarını yakalayan LSTM/GRU tabanlı ağlar test edilerek makine öğrenmesi modelleriyle karşılaştırılacaktır.

Değerlendirme Metrikleri

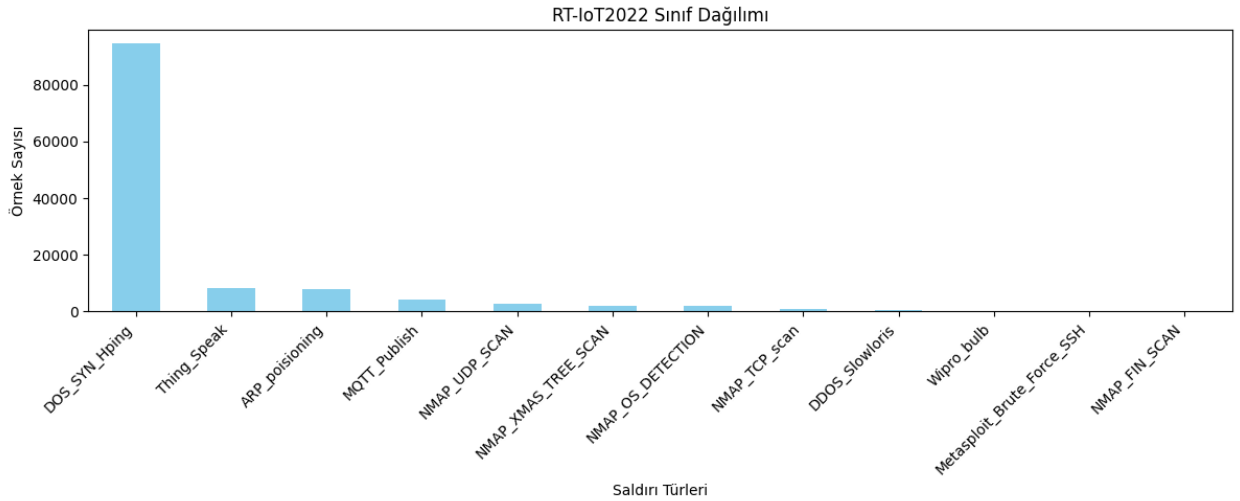
Model performansını bir bütün olarak ölçmek için çeşitli değerlendirme metrikleri kullanılacaktır. En temel ölçüt doğruluğun ardından kesinlik, duyarlılık ve F1 skoru hesaplanacaktır. Özellikle saldırı sınıflarının negatif oranının yüksek olması istenilmediğinden kaynaklı F1 skoru önemli bir kriter olacaktır. Sınıflandırma çıktılarının ayrıntılı analizi için karışıklık matrisi oluşturularak modellerin hangi saldırı türlerinde zorlandığı ve hangi sınıflarda yüksek başarı sağladığı tespit edilecektir. Model değerlendirmesi yapılırken IoT cihazlarının kısıtlı işlem gücü ve gerçek zamanlı gereksinimleri de dikkate alınarak modellerin uygulanabilirliği analiz edilecektir.

Model Karşılaştırması ve Analizi

Çalışmanın son aşamasında makine öğrenmesi modellerinin performansları karşılaştırmalı olarak analiz edilecektir. Öznitelik seçimi uygulanmış modeller ile uygulanmamış modeller ayrı değerlendirilerek özellik azaltma yöntemlerinin etkisi gözlenecektir. Ayrıca elde edilen bulgular, literatürde RT-IoT2022 veri seti üzerinde gerçekleştirilen önceki çalışmalarla karşılaştırılarak modelimizin güçlü yönleri, sınırlılıkları ve geliştirilmesi gereken yönleri tartışılacaktır. Bu sayede çalışma hem akademik hem de pratik uygulamalar açısından IoT saldırı tespitine yönelik kapsamlı bir değerlendirme sunacaktır.

SONUÇLAR ve TARTIŞMA

Bu çalışmada RT-IoT2022 veri seti kullanılarak makine öğrenimi tabanlı saldırı simüle edilerek saldırı tespit deneyleri gerçekleştirilmiştir. Deneysel çalışma kapsamında veri ön işleme, öznitelik seçimi ve modelleme adımları sonrasında Random Forest, SVM ve XGBoost sınıflandırıcıları eğitilmiş ve performansları karşılaştırılmıştır.



Şekil 1. RT-IoT2022 Sınıf Dağılımı

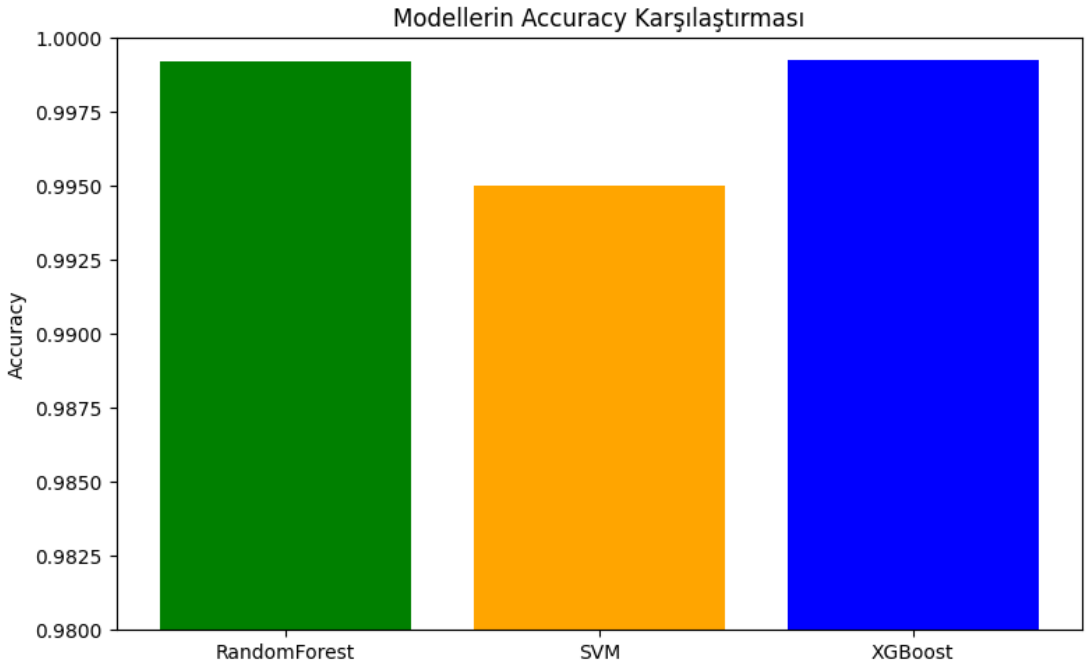
RT-IoT2022 sınıf dağılımı (Şekil 1), kullandığımız veri setinin oldukça dengesiz olduğunu göstermekte ve özellikle DOS_SYN_Hping sınıfının veri setinin büyük bölümünü oluşturduğunu göstermektedir. Bu nedenle dengesiz yapının model performansını etkilememesi için değerlendirme mektriklerinde accuracy tek başına yeterli olmayabileceği göz önünde bulundurulmuştur. Kullanılan diğer sınıflandırma performansları, modellerin sınıf dengesizliğine rağmen yüksek doğrulukla çalışabildiğini göstermiştir.

Eğitilen üç modelin doğruluk oranları oldukça yüksek seviyelere ulaşmıştır. Accuracy değerleriaşağıdaki şekildedir.

• Random Forest: %99.92

• SVM: %99.50

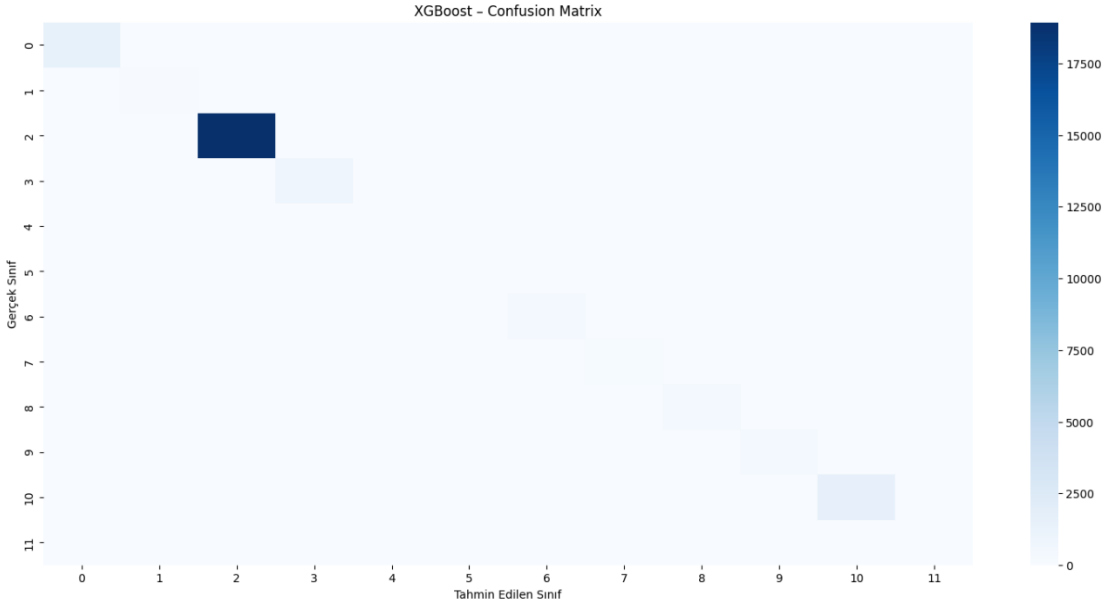
• XGBoost: %99.93



Şekil 2. Modellerin Accuracy Karşılaştırması

Model performansını gösteren karşılaştırma sonuçlarına (Şekil 2) göre; XGBoost modeli en yüksek doğruluk oranına sahip olarak en başarılı model olmuştur. RandomForest modeli bu modele yakın bir performans sergilerken SVM modelinin karmaşık ve çok boyutlu veride daha düşük performans gösterdiği gözlemlenmiştir.

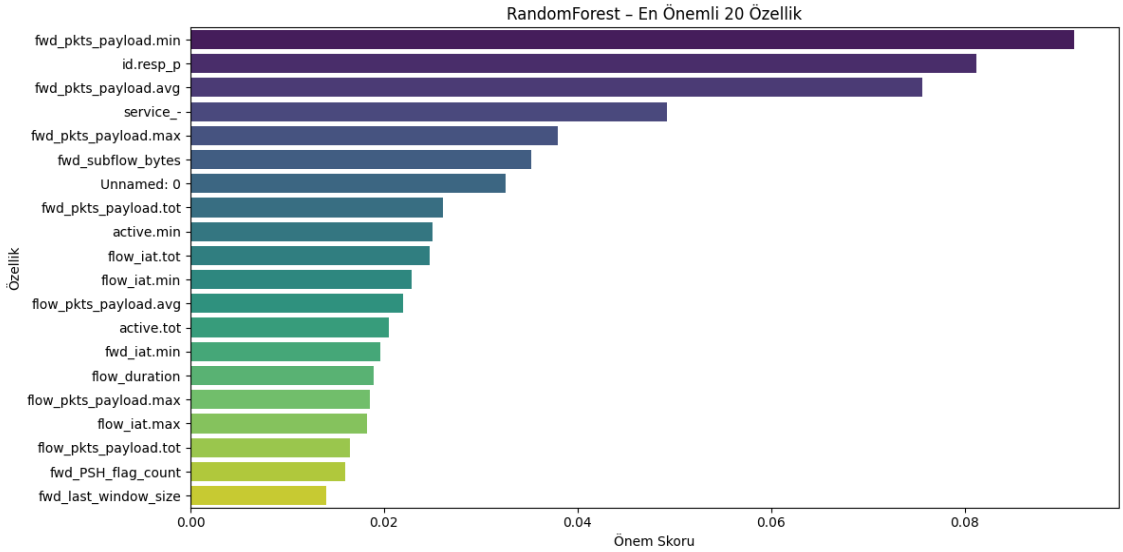
En yüksek doğruluğu elde eden XGBoost modeli için üretilen karışıklık matrisi, modelin tüm sınıfları yüksek hassasiyetle ayırt edebildiğini göstermektedir. Çok sayıda örneğe sahip sınıfları doğru tahmin edilebilmiştir. Düşük örnek sayısına sahip sınıflarda bile hatalı tahmin sayısı çok azdır. (Şekil 3)



Şekil 3. XGBoost Confusion Matrix

Bu bulgular, XGBoost modelinin sınıf dengesizliğine rağmen tutarlı bir performans sergilediğini göstermektedir. Bu model %99.93 doğruluk ile en iyi performansı göstererek IoT saldırı tespitinde güçlü bir yöntem olarak öne çıkmaktadır.

Random Forest modeli ile gerçekleştirilen özellik önem analizi sonucunda, saldırı tespitinde en etkili özelliklerin çoğunlukla; fwd paket yükü (payload) değerleri, yanıt portu, servis türü, akuş süreleri ve zamanlamaya dayalı istatistikler olduğu (Şekil 4) belirlenmiştir.



Şekil 4. Random Forest En Önemli 20 Özellik

Bu sonuçlar, veri seti yüksek oranda dengesiz olmasına rağmen modellerin yüksek doğruluk oranlarına ulaşabilmesinin, özellik zenginliğinin ve uygulanan ön işlemlerin etkiliği olduğunu göstermektedir. Modellerin hem yaygın hem de nadir saldırı türlerini başarılı bir şekilde ayırt edebildiğini ortaya koymaktadır.

Elde edilen başarı oranı literatürdeki birçok derin öğrenme tabanlı yönteme benzer veya daha yüksek seviyede olup, makine öğrenmesi yöntemlerinin daha hızlı ve etkin alternatif yöntemler sunabileceğini göstermektedir.

Yapay Zeka Desteği Bildirimi

Bu çalışmada, kodlama süreci ve metin anlatım netliğinin artırılması amacıyla yapay zekâ tabanlı araçlardan yararlanılmıştır. Kullanılan veri seti yazar tarafından sağlanmış olup, tüm bilimsel değerlendirme, analiz ve sonuçların sorumluluğu yazarlara aittir.

KAYNAKÇA

Sharmila, B. S., & Nagapadma, R. (2023). Quantized autoencoder (QAE) intrusion detection system for anomaly detection in resource-constrained IoT devices using RT-IoT2022 dataset. Cybersecurity, 6(1), 41.

Doshi, R., Apthorpe, N., & Feamster, N. (2018, May). Machine learning ddos detection for consumer internet of things devices. In 2018 IEEE security and privacy workshops (SPW) (pp. 29-35). IEEE.

Chen, T., & Guestrin, C. (2016, August). Xgboost: A scalable tree boosting system. In Proceedings of the 22nd acm sigkdd international conference on knowledge discovery and data mining (pp. 785-794).

Doğar, M. (2023). Detecting And Classifying Network Based Cyberattacks Using Machine Learning Techniques. Journal of Artificial Intelligence with Applications, 4(1), 20-23,

Elzaghmouri, B. M., Jbara, Y. H. F., Elaiwat, S., Innab, N., Osman, A. A. F., Ataelfadiel, M. A. M., ... & Abu-Zanona, M. (2024). A Novel Hybrid Architecture for Superior IoT Threat Detection through Real IoT Environments. Computers, Materials & Continua, 81(2).

Pehlivanoğlu, M. K., Kuyucu, A., Kaya, R., & Aydın, R. (2023). IoT Veri Kümelerinde Makine Öğrenmesi Tekniklerine Dayalı Saldırı Tespiti. Avrupa Bilim ve Teknoloji Dergisi, (52), 19-26.