

**WI-FI DE-AUTHENTICATION SALDIRISINA
YÖNELİK MAKİNE ÖĞRENME TABANLI
TESPİT ve ÖNLEM ÖNERİSİ**

**2024
BİLGİSAYAR MÜHENDİSLİĞİ
BİTİRME PROJESİ TEZİ**

Ahmet Husrev ÇEKER

**WI-FI DE-AUTHENTICATION SALDIRISINA YÖNELİK MAKİNE
ÖĞRENME TABANLI TESPİT ve ÖNLEM ÖNERİSİ**

Ahmet Husrev Çeker

**Karabük Üniversitesi
Mühendislik Fakültesi
Bilgisayar Mühendisliği Bölümünde
Bitirme Projesi Tezi
Olarak Hazırlanmıştır.**

KARABÜK

Ocak 2024

Ahmet Husrev ÇEKER tarafından hazırlanan “WI-FI DE-AUTHENTICATION SALDIRISINA YÖNELİK MAKİNE ÖĞRENME TABANLI TESPİT ve ÖNLEM ÖNERİSİ” başlıklı bu projenin Bitirme Projesi Tezi olarak uygun olduğunu onaylıyorum.

Prof. Dr. İlhami Muharrem ORAK
.....

Bitime Projesi Danışmanı, Bilgisayar Mühendisliği Anabilim Dalı

...../...../2024

Bilgisayar Mühendisliği bölümü , bu tez ile, Bitirme Projesi Tezini onamıştır

Prof. Dr. Oğuz FINDIK
.....

Bölüm Başkanı

“Bu projedeki tüm bilgilerin akademik kurallara ve etik ilkelere uygun olarak elde edildiğini ve sunulduğunu; ayrıca bu kuralların ve ilkelerin gerektirdiği şekilde, bu çalışmadan kaynaklanmayan bütün atıfları yaptığımı beyan ederim.”

Ahmet Husrev ÇEKER

ÖZET

Bitme Projesi Tezi

WI-FI DE-AUTHENTICATION DoS SALDIRISINA YÖNELİK MAKİNE ÖĞRENME TABANLI TESPİT ve ÖNLEM ÖNERİSİ

Ahmet Husrev ÇEKER

Karabük Üniversitesi
Bilgisayar Mühendisliği
Bilgisayar Mühendisliği Bölümü

Tez Danışmanı:
Prof. Dr. İlhami Muharrem ORAK
Ocak 2024, 52 sayfa

Günümüzde kablosuz ağlar, kablolu ağlardan daha yaygın olarak kullanılmaktadır. Ancak, bir ağa kablosuz erişim sağlayan access point, router gibi cihazların birçoğu, de-authentication saldırılara karşı savunmasızdır. Bu tür kritik saldırıları önlemek için genellikle modern Wi-Fi standartlarına sahip pahalı ve güncel cihazlar kullanmak gerekmektedir, çünkü saldırganın kimliği tespit edilemez. Bu çalışmada, daha uygun maliyetli ve yeni bir ağ sistemine geçiş yapma imkanı olmayan bireyler veya işletmeler için, saldırının tespiti ve önlenmesi amacıyla bir yöntem önerilmektedir. Bu yöntem, makine öğrenmesi kullanarak saldırının tespit edilmesini ve trilaterasyon yöntemiyle saldırganın coğrafi konumunun belirlenmesini içermektedir.

Anahtar Sözcükler : Wi-Fi, De-Authentication Saldırısı, Makine Öğrenmesi, Trilaterasyon.

ABSTRACT

Senior Project Thesis

MACHINE LEARNING-BASED DETECTION AND PREVENTION PROPOSAL FOR WI-FI DE-AUTHENTICATION DoS ATTACK

Ahmet Husrev ÇEKER

**Karabük University
Faculty of Engineering
Department of Computer Engineering**

**Project Supervisor:
Prof. Dr. İlhami Muharrem ORAK
January 2024, 52 pages**

Today, wireless networks are more commonly used than wired networks. However, many devices that provide wireless access to a network, such as access points and routers, are directly vulnerable to a critical attack known as a de-authentication attack. Preventing this attack typically requires the use of expensive, modern devices with up-to-date Wi-Fi standards, as the identity of the attacker cannot be detected. This study proposes a method for detecting and preventing these attacks for individuals or companies that cannot afford to transition to a newer, more expensive network system or technology. The proposed method involves using machine learning to detect the attack and trilateration to determine the geographic location of the attacker.

Key Words : Wi-Fi, De-Authentication Attack, Machine Learning, Trilateration.

TEŞEKKÜR

Bu tez çalışmasının planlanması, araştırılmasında, yürütülmesinde, oluşumunda ilgi ve desteğini esirgemeyen, engin bilgi ve tecrübelerinden yararlandığım, yönlendirme ve bilgilendirmeleriyle çalışmamı bilimsel temeller ışığında şekillendiren sayın hocam Prof. Dr. İlhami Muharrem ORAK'a ve donanım gereksinimlerimizi ücretsiz sunduğu için sayın Sezer ÖZDEMİR ağabeye sonsuz teşekkürlerimi sunarım.

İÇİNDEKİLER

KABUL	ii
ÖZET	iv
ABSTRACT	v
TEŞEKKÜR	vi
İÇİNDEKİLER	vii
BÖLÜM 1: GİRİŞ	1
1.1. LİTERATÜR ARAŞTIRMASI: DE-AUTHENTICATION SALDIRISI ve MEVCUT TESPİT ve ÖNLEME YÖNTEMLERİ	1
1.1.1. DE-AUTHENTICATION SALDIRISI	2
1.1.2. MEVCUT TESPİT ve ÖNLEME YÖNTEMLERİ	4
1.2. PROJENİN AMACI	6
BÖLÜM 2: SALDIRININ TESPİTİ	7
2.1. SALDIRININ TESPİTİ İÇİN İZLENİLEN YOL VE ULAŞILAN SONUÇ	7
2.2. KULLANILAN VERİ SETİNİN RAPORU	8
2.2.1. VERİ SETİNİN DETAYI	9
2.2.2. VERİ SETİ TEMİZLİĞİ VE ÖN İŞLEME	10
2.2.3. ETİKETLEME VE ÖRÜNTÜ ANALİZİ	10
2.2.4. KARŞILAŞILAN PROBLEMLER	12
2.2.5. MODEL PERFORMANSININ DEĞERLENDİRİLMESİ VE MODEL SEÇİMİ	15

BÖLÜM 3: SALDIRGANIN TESPİTİ	16
3.1. YOL 1: TEK YÖNLÜ (UNIDIRECTIONAL) ANTEN İLE LOKASYON TESPİTİ	16
3.1.1. YÖNTEMİN DETAYLARI ve UYGULAMASI	18
3.1.2. SINIRLAMALAR ve UYGULAMA ALANLARI	19
3.2. YOL 2: ÜÇ FARKLI YERE KONUMLANDIRILMIŞ ACCESS POINT İLE LOKASYON TESPİTİ (TRİLATERASYON)	20
3.2.1. SİNYAL GÜCÜNDEN (RSSI) X ve Y DENKLEMLERİNİN ELDE EDİLMESİ	21
3.2.2. PYTHON İMPLEMENTASYONU	22
3.3. YOL 3: NTP (Network Time Protocol) PAKETLERİYLE LOKASYON TESPİTİ	23
 BÖLÜM 4: YAZILIM ve DONANIM MİMARİSİ	26
4.1. ROLLER	26
4.2. USE CASE DİYAGRAMLARI	27
4.2.1. AKTÖRLER	27
4.2.2. SİSTEM FONKSİYONLARI	28
4.3. ERD: ERD DİYAGRAMININ YAPISI	32
4.4. KULLANILAN DONANIM VE YAZILIMLAR	33
4.4.1. DONANIMLAR	33
4.4.2. YAZILIMLAR	34
4.5. PROJEDEN GÖRÜNTÜLER	34
 BÖLÜM 5: SONUÇ ve GELECEK ARAŞTIRMA YÖNLERİ	38
 KAYNAKLAR	39
 ÖZGEÇMİŞ	40

BÖLÜM 1

GİRİŞ

Kablosuz ağlar, günümüzde hem evlerde hem de işletmelerde yaygın olarak kullanılmaktadır. Ancak, bu ağlar, çoğu zaman de-authentication saldıruları gibi çeşitli güvenlik tehditlerine karşı da savunmasızdır. Zira hâlâ birçok cihaz hâlâ Protected Management Frames (PMF) teknolojisini desteklememektedir. Çünkü bu teknoloji, IEEE 802.11w protokolünü destekleyen bir cihaz gerektirmektedir [1]. De-authentication saldıruları, bir kablosuz ağdaki bir istemcinin ağdan bağlantısının kesilmesine ve saldırının çeşidine göre tekrar bağlanamamasına neden olan bir saldırı çeşididir. Bu saldırısı, bilgi güvenliğinin üç şartı olan, gizlilik (confidentiality), bütünlük (integrity), erişilebilirlik (availability) maddelerinin hepsini birden ihlal edebilme potansiyeli taşımakla birlikte, uygulaması da nispeten kolaydır. Bu saldırının tercih edilme sebeplerinin en başında, ağdaki access point, router ve benzeri cihazların parolalarını öğrenmek veya istemcileri ağdan mahrum bırakmak amacıyla DoS (Denial of Service) saldırısı şeklinde kullanımı gelir.

Bu makalede, de-authentication saldırularını tespit etmek ve önlemek için makine öğrenmesi ve coğrafi konum tespiti kullanımıyla bir çözüm önerilmektedir.

1.1. LİTERATÜR ARAŞTIRMASI: DE-AUTHENTICATION SALDIRISI ve MEVCUT TESPİT ve ÖNLEME YÖNTEMLERİ:

Bu bölümde, Wi-Fi ağlarında meydana gelen de-authentication saldırısını tanımlayacak, saldırıyla karşı geliştirilen çeşitli yöntemleri ve bu yöntemlerin avantajlarını ve dezavantajlarını ele alacağız.

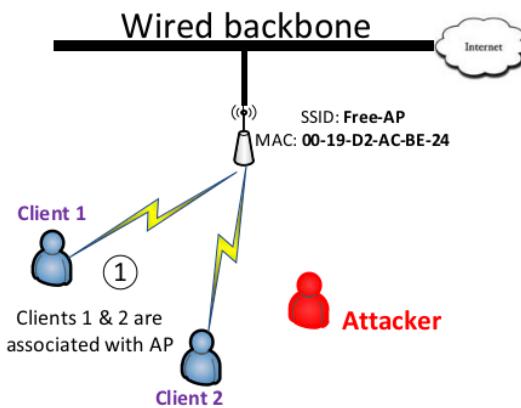
1.1.1. DE-AUTHENTICATION SALDIRISI:

De-authentication saldırısı, kablosuz ağlarda kullanılan bir güvenlik zafiyeti ve siber saldırı tekniğidir. Bu saldırı türü, ağa bağlı cihazların kısa veya uzun süreliğine hizmet dışı bırakılmasını hedefler. De-authentication saldıruları genellikle kablosuz iletişim protokollerindeki zayıflıkları veya güvenlik açıklarını istismar eder. Özellikle, WPA ve WPA2 gibi yaygın olarak kullanılan, bazense WPA3 gibi modern ve daha güvenli güvenlik protokollerindeki bazı zayıflıklar bu tür saldıruları mümkün kılar. Saldırganlar, hedef ağdaki bağlantıları keserek, kullanıcıların internet erişimini engelleyebilir veya hedef cihazları başka saldırılara açık hale getirebilirler. De-authentication saldırısı tek başına sadece ağa ulaşılabilirliği kısıtlasa da, farklı şekilde kullanımlarıyla birlikte ağır ulaşılabilirliğini kısıtlamasına ek olarak,ağın bütünlüğünü ve gizliliğini de tehdit etmektedir. Genelde, ağdaki access point'lere yapılacak Brute Force saldırısı ile ağdaki access point'lerin parolalarını elde etme amacıyla yapılan ön saldırıdır [2]. Bunun yanında Evil Twin saldırısına da kapı aralar [3] ve direkt olarak DoS (Denial of Service) saldırısı olarak kullanımı da mümkündür.

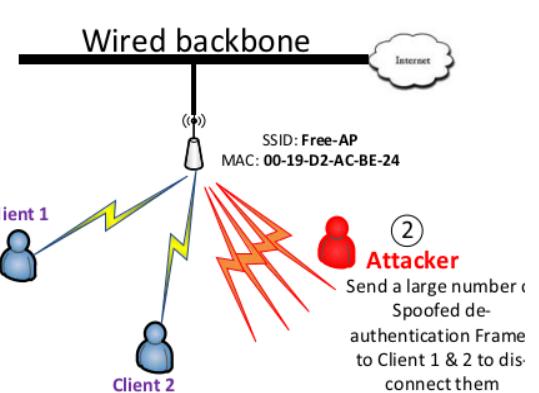
Temel olarak, saldırırganlar hedef ağa bağlı olan cihazları ağdan düşürmek için, istemcinin bağlı olduğu access point'e manipüle edilmiş de-authentication paketleri gönderirler. Bu paketler, hedef cihazlara ağ erişim izinlerinin iptal edildiğini bildiren sahte yönlendirmeler içerir. Normal şartlar altında, bir istemci, kablosuz olarak bağlı olduğu bir ağdan kopmak istediğiinde, bağlı olduğu access point'e de-authentication paketi gönderir. Böylece access point, bu istemcinin ağdan koptuğunu ve onunla daha fazla paket alışverişi yapmasına gerek kalmadığını anlar. Ve bu paket alışverişi, şifrelenmemiş bir şekilde yapılır. Dolayısıyla ağır içinde veya dışında olan bir başka cihaz bu paketi izleyebilir, içeriğini görebilir. Aynı zamanda bu paketin aynısını oluşturup, bu kopya paketin içeriğini değiştirebilir. De-authentication saldırısında ise yapılan şey basitçe; bu trafiğin şifrelenmemiş şekilde yapılıyor olmasından yararlanmaktadır. Saldırgan cihaz, kaynak adresi, hedef istemcinin MAC adresi olarak belirlenmiş, hedef adresi ise hedef istemcinin bağlı olduğu access point'in MAC

adresi olarak belirlenmiş bir de-authentication paketi oluşturur. Bu paketi yayınlar (broadcast). Paket, hedef access point veya router'a ulaştığında, hedef cihaz bu paketin istemcinin kendisinden geldiğini sanacak ve paketin kaynak adresinde yazan istemciyi ağdan düşürecektr. Böylelikle, saldırgan, paketin kaynak adresini değiştirerek hem kendi kimliğini gizlemiş olur hem de hedeflediği kurbanı ağdan, ağda hiçbir yetkisi olmamasına, ağa bağlı olmamasına rağmen düşürmüştür.

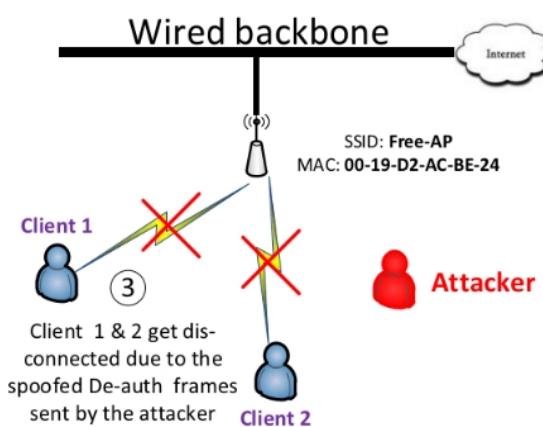
Bu saldırının önlenmesinin bu kadar zor olmasının sebebi, saldırganın kimliğinin hiçbir şekilde öğrenilemeyecek olmasıdır. Makalenin ileriki bölümlerinde saldırganın tespiti kimliği bilinmemesine rağmen nasıl yaptığımız anlatılacaktır.



Figür 1: Saldırısı öncesi senaryo. [4]



Figür 2: Saldırı esnası senaryo. [4]



Figür 3: Saldırı sonrası senaryo. [4]

1.1.2. MEVCUT TESPİT ve ÖNLEME YÖNTEMLERİ:

Yapılan incelemeler neticesinde, mevcut yöntemlerin çoğunun donanım ve yazılım güncellemesi, protokol modifikasyonu gerektirdiği belirlenmiştir.

Şifreleme Tabanlı Yöntemler:

Bu yöntemler, saldıruları önleme konusunda etkili olabilir, ancak istemci ve access point üzerinde firmware güncellemeleri gerektirirler. Letter-envelop protokolü, gizli bir anahtar kullanarak doğrulama sağlar, ancak Bellardo yöntemi gecikmelere neden olabilir. [4]

Protokol Modifikasyonu ve Güncelleme Tabanlı Yöntemler:

802.11w standarı zorunlu kimlik doğrulama sağlar, ancak hem istemci hem de access point üzerinde güncelleme gerektirir. Roaming istemcileri için association sorunlarına neden olabilir ve Bellardo yöntemi gecikmelere yol açabilir. [4]

Şifreleme Dışı Yöntemler:

Kolay uygulama avantajına sahiptir, ancak yanlış alarm riski yüksektir. Agarwal et al. metodunun, eşik değerine dayandığı ve karmaşık saldırılara karşı savunmasının zayıf olduğu tespit edilmiştir. [4]

Sequence Numarası Tabanlı Yöntemler:

Saldıruları önleme konusunda etkili olabilir, ancak sofistike saldırganlar tarafından tahminle kaçırılabilir. Xia et al. ve Anjum et al. yöntemleri, sequence number analizi kullanır ve yüksek saldırı yoğunluğunda güvenilmez olabilir. [4]

Makine Öğrenmesi veya Derin Öğrenme Tabanlı Yaklaşımlar:

Diğer yöntemlere göre daha başarılı bir saldırı tespiti sağlar, ancak saldırıyı önleme yeteneğine sahip değildir. [4, 14]

Genel Özeti ve Beklentiler:

Özet olarak, de-authentication saldırısını tespit etmek ve önlemek için mevcut metodolojilerin eksiklikleri aşağıdaki gibi tanımlanabilir:

- 1)** Kimliği doğrulanmamış paketlerin önlenmesini desteklemek için 802.11 protokol standartı içinde kimlik doğrulama ve paketlerin şifrelenmesinin uygulanması gereklidir.
- 2)** Hem istemci hem de access point cihazları için yazılım yamalarının dağıtılması gerekmektedir.
- 3)** En son 802.11 protokol standartlarını yükseltme (en azından 802.11w), dolayısıyla donanım değişikliği gerekmektedir.

Yukarıda belirtilen noktalardan, etkili bir de-authentication saldırı tespit tekniğinin aşağıdaki özelliklere sahip olması gereği sonucuna varılabilir:

- 1)** 802.11 protokol standardının değiştirilmeden kalması zorunludur.
- 2)** Çözüm hem eski hem de yeni ağlarda kolaylıkla kullanılabilir.
- 3)** Varsa donanım maliyetleri mümkün olduğunda düşük olmalıdır.
- 4)** Sistem, istemcinin temel işletim sistemine, uygulamasına bağlı olmamalı veya istemci yazılımının herhangi bir şekilde yamalanmasını gerektirmemelidir.
- 5)** Hafif bir çözüm olmanın ek avantajını sunduğu için doğası gereği kriptografik olmamalıdır. Zira kriptografik çözümler maliyet ve zahmeti artırır.

Mevcut yöntemlerin çoğu, 802.11 protokol standartında değişiklik yapmayı, donanım ve yazılım güncellemelerini gerektirmekte veya karmaşık saldırırlara karşı zayıf olabilmektedir. İdeal bir yöntem, şifreleme dışı, kolay uygulanabilir, donanım bağımsız ve saldırıyı önleme yeteneğine sahip olmalıdır. Bu bağlamda, önerilen projenin 802.11 protokol standartında değişiklik yapmadan, eski ve yeni ağlara kolayca uygulanabilir, düşük donanım maliyetine sahip, istemci bağımsız ve saldırıyı gerçek anlamda engelleyebilme yeteneğine sahip olması beklenmektedir.

1.2. PROJENİN AMACI

Siber saldırırlarda az bahsedilen ama bir o kadar etkili ve önlenmesi güç bir saldırı olan Wi-Fi de-authentication saldırısının makine öğrenmesi ile tespiti, saldırı tespit durumunda gerekli alarmların verilmesi, saldırganın kimliğinin tespit edilmesi mümkün olmadığından coğrafi konumunun tespiti edilmesi ve saldırının önlenmesine yönelik ilk adımın atılması, projenin amacıdır.

BÖLÜM 2

SALDIRININ TESPİTİ

Bu bölümde, saldırının tespitini yaparken izlenilen yollar izah edilecektir.

2.1. SALDIRININ TESPİTİ İÇİN İZLENİLEN YOL VE ULAŞILAN SONUÇ:

De-authentication saldırısının tespiti oldukça zordur. Bu zorluğun başlıca nedeni, istemcinin kablosuz ağdan ayrılmak istediğiinde bağlı olduğu access point'e de-authentication paketini kendisinin göndermesidir. Bu paketin kullanımı, normal şartlar altında gerekli ve yasal bir işlemidir. Saldırı esnasında da aynı paket, aynı yöntemle gönderildiğinden, bu paketin gerçekten istemciden mi yoksa bir saldırgandan mı geldiğini ayırt etmek gereklidir. Ancak bu şekilde, trafik akışının normal mi yoksa saldırısı kaynaklı mı olduğu tespit edilebilir.

Eğer de-authentication saldırısı, DoS (Denial of Service) saldırısı şeklinde gerçekleştiriliyorsa, tespiti daha kolay hale gelir. Bir istemci ağdan kendisi ayrılmak istediğiinde, access point'e art arda birçok de-authentication paketi göndermeyecektir. Ancak, DoS tipi de-authentication saldırısında bu paketler defalarca gönderilir. Yine de, sadece bu kriter kullanılarak DoS tipi de-authentication saldırısını tespit etmek, yüksek hata payına neden olabilir. Hata payının kabul edilebilir sınırları aşması, sistemin güvenilirliğini azaltır ve saldırısı durumunda "saldırı yok" sonucu vermek, sistemi ve kullanıcıları daha büyük bir tehdit altına sokar.

Bu nedenle, saldırısı tespitinde %99'lara varan başarı oranına ulaşabilecek yöntemler aramaktayız. Geleneksel yöntemler, de-authentication paketlerinin sayısı ve bu paketlerin gönderilme zamanını kullanarak saldırıyı tespit etmeye çalışır. Ancak bu yöntemler, yalnızca DoS tipi de-authentication saldırısını tespit etme potansiyeline sahiptir. Daha güvenilir ve kapsamlı bir çözüm için makine öğrenmesi modellerini kullanmayı tercih ettiğimizdir.

AWID 3 veri setini kullanarak bir makine öğrenmesi modeli eğittik. Model, test veri setinde %99 başarı oranına ulaştı; ancak gerçek dünyada test edildiğinde bu oran

%80'lere düştü. Bu sonuç, pratikte yetersizdi. Çözüm olarak, veri setimize yeni özellikler ekledik. Bu özellikler, "time_difference" ve "num_of_deauth_frames" olarak adlandırıldı.

"Time_difference" özelliği, iki de-authentication paketi arasındaki zaman farkını değil, de-authentication ile authentication paketleri arasındaki zaman farkını tutmaktadır. Normal şartlarda, bir istemci ağdan ayrılmak için de-authentication paketi gönderdiğinde hemen ardından authentication paketi göndermez. Ancak, bir saldırgan de-authentication paketi gönderdiğinde, istemci hemen tekrar authentication olmaya çalışır. Bu nedenle, time_difference değeri ne kadar az ise, trafiğin saldırısı trafigi olma olasılığı o kadar artar. [4]

"num_of_deauth_frames" özelliği ise, belirli bir zaman aralığında bir istemcinin gönderdiği de-authentication paketlerinin sayısını saklar. Bu değerin yüksek olması, paketin saldırısı paketi olma olasılığını artırır. Geleneksel yöntemlerde tek başına kullanılan bu özellik, bizim modelimizde ek bir özellik olarak yer almaktadır. [4]

Bu iki yeni özelliğin eklendiği veri setiyle eğitilen yeni makine öğrenmesi modeli, gerçek zamanlı testlerde %96 başarı oranına ulaşmıştır. Böylece, donanım ve protokol değişiklikleri gibi masraflı yükseltmeler yapmadan, ekonomik bir şekilde hedefimize ulaşarak saldırısı tespitini yüksek başarıyla gerçekleştirmiştir.

2.2. KULLANILAN VERİ SETİNİN RAPORU:

Çalışmaları yürütürken kullandığımız, elimizde bulunan, AWID 2 ve AWID 3 olmak üzere toplamda 27 GB boyutunda 2 adet veri seti bulunmaktadır. AWID 3 [5] veri seti, hem PCAP formatında hem de veri setini oluşturan taraf tarafından CSV formatına çevrilmiş haliyle elimizde bulunmaktadır. Biz, makine öğrenmesi modelimizi eğitirken CSV formatındaki son halini kullanacağız, zira sayısal özelliklere dayalı olması, yaygın kullanılıyor olması nedeniyle makine öğrenmesi modellerini eğitmek için CSV daha uygun bir formattır. Ek olarak CSV formatındaki hali bir takım ön

işlemlerden geçmiş, ham veri işlenmiş ve kullanıma daha uygun hale getirilmiştir. AWID3-CSV veri setini inceleyelim.

AWID3 veri seti, Wi-Fi IDS (Wireless Intrusion Detection System) konusunda çalışan araştırmacılarla yardımcı olmak amacıyla hazırlanmıştır.

2.2.1. VERİ SETİNİN DETAYI:

AWID 3, IEEE 802.1X Genişletilebilir Kimlik Doğrulama Protokolü (EAP) ortamında gerçekleştirilen çeşitli saldırıların izlerini yakalayarak ve inceleyerek, bilinen AWID2 veri kümесini önemli ölçüde tamamlamakta ve genişletmektedir. Ayrıca, 802.11 odaklı saldırıların, Korunan Yönetim Çerçevevleri (PMF) tarafından sunulan savunmaların aktif olduğu durumlarda gerçekleştirildiği göz önüne alındığında, WPA3 sertifikalı cihazlar için zorunlu olan IEEE 802.11w değişikliğinin dayanıklılığına dair, bildiğimiz kadarıyla ilk kapsamlı empirik çalışmayı sunmaktadır. Belirtilen her iki durumda da, AWID3'ün, saldırısı tespit sistemlerinin tasarımı ve değerlendirilmesinde önemli bir yardımcı olması beklenmektedir.

Daha uzun ömürlü ve kapsamlı bir veri seti sunmak amacıyla ve bir saldırının kablosuz MAC katmanından daha üst katmanlara doğru saldırısını tırmandırması perspektifi altında, IEEE 802.3 ağlarına özgü çeşitli saldırıları da dahil etti. Veri kümesi, ham açık metin pcap dosyaları şeklinde kamuya sunulduğundan, gelecekteki araştırmalar, belirli uygulama senaryosuna bağlı olarak herhangi bir özellik alt kümescini doğrudan kullanabilir. WiFi IDS konusuna çalışan araştırmacılarla daha fazla yardımcı olmak için, empirik olarak 254 özellik (253 genel özellik ve bir etiketleme amacıyla) manuel olarak çıkartılarak CSV formatında sunulmuştur. Bu "AWID3-CSV" veri kümlesi, pcap formatında verilen orijinal veri kümescini tamamlamaktadır. Çıkarılan özellikler, kaydedilen pcap dosyalarının hem MAC hem de uygulama katmanlarına yayılmakta olup, ilgili katmanlara göre ayrılmıştır.

[5]

2.2.2. VERİ SETİ TEMİZLİĞİ VE ÖN İŞLEME:

De-authentication saldırısı tespiti için kullanılan veri setinde, ilk 800,000 satırın de-authentication paketlerini içermediği tespit edilmiştir. Bu nedenle, veri setinin bu kısmının silinmesi gerektiği düşünülmüştür. Böylece, class imbalanced problemi ve veri setinin boyutu yarı yarıya azaltılabilir.

Veri setinin eski ve yeni durumları şu şekildedir:

- Eski:
 - 38,942 De-authentication paketi
 - 1,587,527 Normal paket
 - 1,626,469 Toplam paket
- Yeni:
 - 38,942 De-authentication paketi
 - 756,257 Normal paket
 - 795,199 Toplam paket

2.2.3. ETİKETLEME VE ÖRÜNTÜ ANALİZİ:

Veri setindeki etiketlerin nasıl belirlendiği anlaşılmaya çalışılmıştır. Modelin, satırların sırası karıştırıldığında bile %90'lara varan başarı oranı elde etmesi, etiketlemenin sadece de-authentication işlemi gerçekleşen her pakete dayanmadığını göstermiştir. Ayrıca, bunun açığa çıkardığı bir başka sonucu; etiketleme sırasında paketler arasında bir örüntüye bakılmamış ve paketler tek tek değerlendirilmiştir.

Attack	Normal traffic	Malicious traffic
Deauth	1,587,527	38,942

Figür 4: AWID 3 De-authentication Normal ve Zararlı Trafik Analizi [6]

Veri seti dökümantasyonu incelendiğinde, normal ve kötü niyetli trafik şeklinde bir tasnif yapıldığı anlaşılmıştır. Ancak, “wlan.fc.type_subtype” özelliği 12 olan

çerçeveeler filtrelendiğinde, veri setinde 38,942 değil, 170,000'den fazla satır bulunduğu görülmüştür. Bu durum, etiketleme sırasında sadece de-authentication paketi olup olmadığına bakılmadığını, başka kriterlerin de göz önünde bulundurulduğunu göstermiştir. Sonuç olarak ulaşılan sonuç, aşağıdaki filtrenin uygulanmış olduğunu:

Deauth

```
(wlan.fc.type_subtype==10 || wlan.fc.type_subtype==12) && wlan.fc.protected==0 && (frame.number >=1088022 && frame.number <=1626254)
```

Figür 5: Veri setinde sınıflandırma yaparken kullanılan tsharkfiltresi. [5]

Bu filtreden geçen her paket, de-authentication saldırısı paketi olarak etiketlenmektedir. Burada dikkat edilmesi gereken, her de-authentication paketinin de-authentication saldırısı paketi olmadığıdır. 2.1. başlıkta bu farka detayyla değinmiştik. Wlan.fc.type_subtype'ın değerinin 12 olması, o paketin de-authentication paketi olduğunu gösterir, ancak bir de-authentication saldırısı paketi olduğunu göstermez. Figürde görülen filtreyle etiketlenmiş veri setiyle modelimizi eğittiğimizde, yine 2.1. başlıkta bahsettiğimiz gibi, gerçek zamanlı yaptığımız testlerde, %80'e kadar düşen doğruluk oranları elde ettik. Bu sebeple, bu veri setine, kendi ürettiğimiz 2 adet özelliği daha sütun olarak ekledik. Detayı, 2.1. başlıkta anlatılmıştır.

Özellik Seçimi ve Model Eğitimi

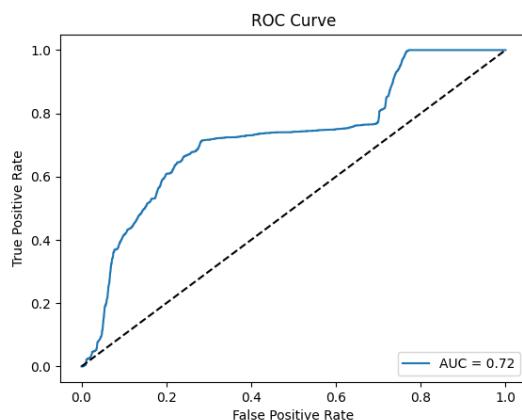
Makine öğrenmesi modelleri için veri setinde belirli özelliklerin türetilmesi ve seçilmesi önemlidir. Özellikle, paketler arasındaki zaman farkı (time_difference) ve belirli bir zaman diliminde gönderilen de-authentication paketlerinin sayısı (num_of_deauth_frames) gibi özellikler kullanılarak modelin başarısı artırılmıştır.

2.2.4. KARŞILAŞILAN PROBLEMLER:

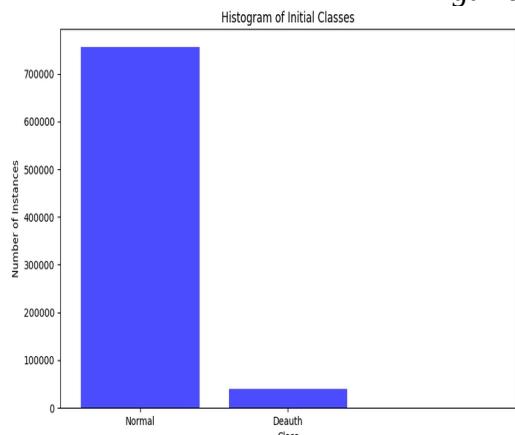
Class Imbalanced (Sınıf Dengesizliği) Problemi:

Class imbalanced problemi, makine öğrenmesi modellerinin bir sınıfın diğerine göre çok daha fazla sayıda örnek içерdiği veri setlerinde, nadir görülen sınıfları doğru bir şekilde tanımlamakta zorlanmasıdır. Bu durum, modelin yaygın olan sınıfı doğru tahmin etme eğilimi göstermesine ve nadir sınıfı göz ardı etmesine yol açarak dengesiz bir performans sergilemesine neden olur. Bu, de-authentication saldırısını tespit eden modellerde önemli bir zorluktur. Random Forest modeli, bu problemi oversampling veya undersampling yapmadan etkili bir şekilde çözmektedir. Farklı veri setleri üzerinde yapılan testlerde, modelin başarı oranı yüksek kalmıştır:

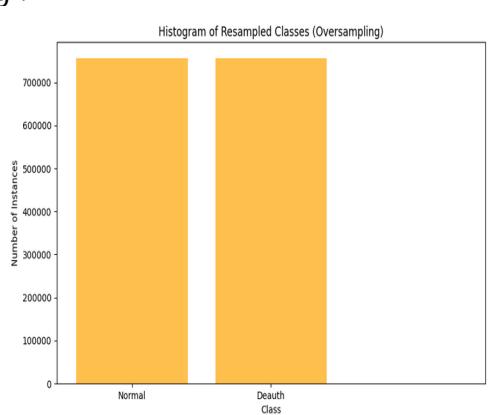
- Orijinal Test Setinde Doğruluk: 0.99997
- Oversampled Test Setinde Doğruluk: 0.99997
- Undersampled Test Setinde Doğruluk: 0.99987



Figür 6: Veri setine ait ROC Curve grafiği.



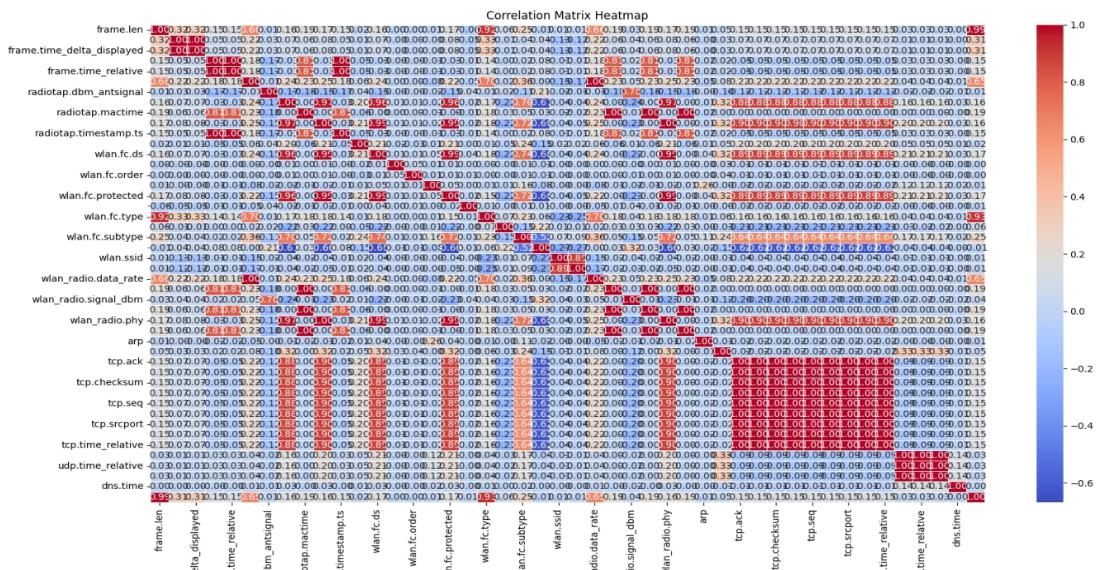
Figür 7: Veri setinin orjinal hali.



Figür 8: Veri setinin oversampled hali.

Korelasyon Analizi

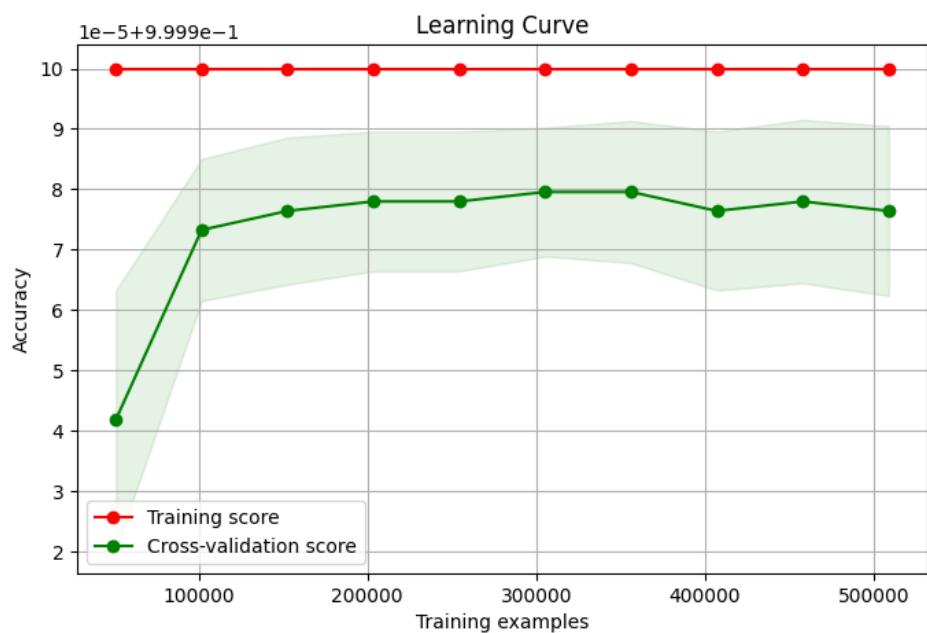
Veri setindeki özellikler arasında yüksek korelasyon bulunanları çıkartarak, model performansı iyileştirilmiştir. Örneğin, Naive Bayes modeli için korelasyonu 1 olan özellikler çıkarıldığında, doğruluk oranı 0.84'ten 0.95'e yükselmiştir. Ancak, class imbalanced problemi nedeniyle, model tüm örnekleri "normal" olarak sınıflandırarak yüksek doğruluk sağlamıştır, bu da modelin gerçekte kötü niyetli paketleri tespit edemediğini göstermektedir.



Figür 9: Veri setinde bulunan özelliklerin korelasyon matriksi.

Overfitting (Aşırı Uyum) Problemi:

SVM modeli, çeşitli veri setlerinde (temizlenmiş ve korelasyonu azaltılmış) %100 doğruluk oranı ile en iyi performansı göstermiştir. Ancak bu, overfitting probleminden dolayı elde ettiğimiz yaniltıcı bir sonuçtır. Daha önce de dediğimiz gibi, veri setinden ayırdığımız test setiyle cross validation yaparak başarı oranını test ettiğimizde, %100 doğruluk oranı verirken, bir anda gerçek zamanlı bir test yaptığımızda başarı oranı %80'lere kadar düşmektedir. Bu da, aşağıdaki öğrenme doğrusundan da görüldüğü üzere, modelde overfitting olduğunu gösterir:



Figür 10: SVM modeline ait, cross validation öncesi ve sonrası öğrenme eğrileri.

2.2.5. MODEL PERFORMANSININ DEĞERLENDİRİLMESİ VE MODEL SEÇİMİ:

Model Karşılaştırması

Farklı makine öğrenmesi modellerinin performansları karşılaştırılmıştır:

- Naive Bayes modeli, korelasyonu 1 olan özellikler çıkarıldığında, doğruluk oranı %84'ten %95'e çıkmıştır. Ancak class imbalanced problemine sahiptir.
- SVM modeli, çeşitli veri setlerinde (temizlenmiş ve korelasyonu azaltılmış) %100 doğruluk oranı ile en iyi performansı göstermiştir. Ancak bu, overfitting probleminden dolayı elde ettiğimiz yaniltıcı bir sonuctur, gerçek doğruluk oranı %80'dir.
- Random Forest, class imbalanced problemini, overfitting problemini çözdüğümüz ve veri setine yeni 2 türetilmiş özellik eklediğimizde en başarılı model olmuştur. Doğruluk oranı, %96'dır.

Sonuç olarak, modelimizi kendi ürettiğimiz veri setini kullanarak, Random Forest ile eğiterek, projenin saldırı tespiti bölümünü tamamladık.

BÖLÜM 3

SALDIRGANIN TESPİTİ

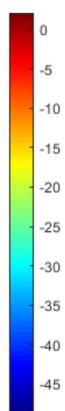
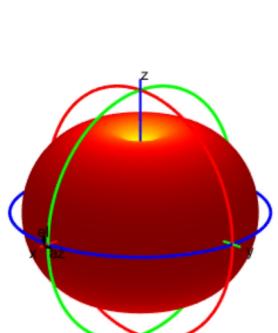
Önceki bölümde saldırının tespitinin zorluklarından ve karşılaşılan problemlerden bahsedilmişti. Ancak saldırın tespiti, saldırının tespitinden çok daha karmaşık ve zor bir süreçtir. Saldırgan, kimliğini tamamen gizlemektedir ve bu durum tespit sürecini oldukça zorlaştırır. Saldırganın kimliğini belirlemek, yazılımların ötesine geçmeyi ve radyo dalgalarının fiziksel yönünü kullanmayı gerektirir. Bu, aynı zamanda fiziksel bazı hesaplamalar yapmayı da içerir. Saldırganın kimliğini yalnızca coğrafi konumunu belirleyerek tespit edebiliriz. Ancak, bu çalışmanın kapsamı, tespit edilen lokasyonla ne yapılacağını içermez. Bu bölümde, yalnızca saldırın kullandığı cihazın ve kendisinin gerçek kimliğini tespit etme sürecinde atılması gereken ilk adım için üç farklı öneri sunulacaktır. Devamında tespit edilen coğrafi konum ile ne yapılacak, bu çalışmanın kapsamına dahil değildir.

Saldırganın coğrafi konumunu tespit etmenin üç farklı yolunu belirledik. Bunlardan ikisi sinyal gücüne dayanarak, diğeri ise özel bir paketin havada geçirdiği zamanı hesaplayarak gerçekleştirilir.

3.1. YOL 1: TEK YÖNLÜ (UNIDIRECTIONAL) ANTEN İLE LOKASYON TESPİTİ:

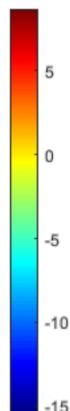
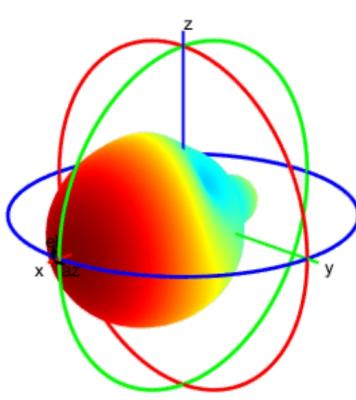
Bu bölümde, tek yönlü (unidirectional) anten kullanarak cihazların konumunu belirleme yöntemini ayrıntılı olarak ele alacağız. Tek yönlü antenler, belirli bir yönde güçlü sinyal iletimi ve alımı sağlayarak belirli bir hedefe odaklanma imkanı sunar. Bu özellikleri, uzun mesafelerde yüksek performans gerektiren uygulamalar için ideal hale getirir. Buna karşın, çok yönlü (omnidirectional) antenler sinyali 360 derece yayarak tüm yönlerde eşit sinyal gücü sağlar ve geniş kapsama alanı sunar.

Tek yönlü antenlerin yüksek kazançlı sinyal iletimi ve alımı sağladığı göz önüne alındığında, bu antenlerin x ekseni etrafında 360 derece sürekli olarak döndürülmesi ile bir cihazın x ve y eksenlerindeki konumunu tahmin etmek mümkündür. Bu yöntem, sinyal gücünden yola çıkarak mesafe hesabı yapma ilkesine dayanır, ancak hassas konum belirleme gereksinimleri için sınırlamaları olabileceği unutulmamalıdır. Sinyal gücü üzerinden yapılan mesafe hesaplamaları her zaman çok doğru sonuçlar vermeyebilir; çevresel faktörler ve çoklu yol (multipath) etkileri gibi etmenler bu hesaplamaları etkileyebilir.



Figür 11: Çok Yönlü (Omnidirectional) Anten İşima Örütüsü [7]

Figür 12: Çok Yönlü (Omnidirectional) Anten Örneği [7]



Figür 14: Tek Yönlü (Unidirectional) Anten Örneği [7]

Figür 13: Tek Yönlü (Unidirectional) Anten İşima Örütüsü [7]

3.1.1. YÖNTEMİN DETAYLARI ve UYGULAMASI:

Antenin Döndürülmesi: Tek yönlü anten, x ekseni etrafında 360 derece sürekli olarak döndürüldüğünde, belirli bir zaman diliminde (T1) antenin kapsama alanında bulunan cihazın yönü belirlenebilir. Bu, antenin her birim zaman diliminde kapsama alanının belirli bir açısal pozisyonda bulunması sayesinde mümkündür. Antenin her bir pozisyonda aldığı sinyal gücünü ölçülerek, T1 zamanı ile T2 zamanı arasındaki sinyal gücünü farkına bakılarak cihazın pozisyonundaki doğrultusunu tespit edilir.

Sinyal Gücü Ölçümleri: Antenin her bir açısal pozisyonunda, alınan sinyal gücünü (Received Signal Strength Indicator, RSSI) kaydedilir. Sinyal gücü, cihazın antene olan mesafesi ile ters orantılıdır; sinyal gücü azaldıkça mesafe artar ve tersi de geçerlidir. Bu nedenle, her bir açısal pozisyonda alınan RSSI değeri, cihazın antene olan mesafesini hesaplamak için kullanılır.

Mesafe Hesaplama: RSSI değerleri kullanılarak cihazın antene olan mesafesi hesaplanabilir. Bu hesaplama, aşağıdaki formül kullanılarak gerçekleştirilir:

$$\text{Mesafe} = 10^{\left(\frac{P_0 - RSSI}{10n}\right)}$$

Burada P0, referans mesafedeki (genellikle 1 metre) sinyal gücünü ve n ise ortamın yayılım katsayısını temsil eder. Bu formül, sinyal gücü kaybına dayalı olarak mesafeyi belirler.

Yön ve Mesafe Bilgilerinin Birleştirilmesi: Antenin döndürülmesi sırasında elde edilen yön ve mesafe bilgileri, cihazın x ve y eksenlerindeki kesin konumunu belirlemek için kullanılır. Bu bilgiler, bir koordinat sistemine yerleştirilir ve cihazın konumu şu şekilde hesaplanır:

$$x = d \cdot \cos(\theta)$$
$$y = d \cdot \sin(\theta)$$

Burada d mesafe ve θ ise antenin döndüğü açıdır.

Konum Belirleme: Antenin döndürülmesi ile elde edilen sinyal gücü ve mesafe verileri, cihazın x ve y koordinatlarının belirlenmesine olanak tanır. Bu yöntem, doğru ekipman ve kalibrasyon ile hassas konum belirleme sağlar. Ancak, çevresel faktörler ve çoklu yol etkileri gibi etmenlerin dikkate alınması önemlidir.

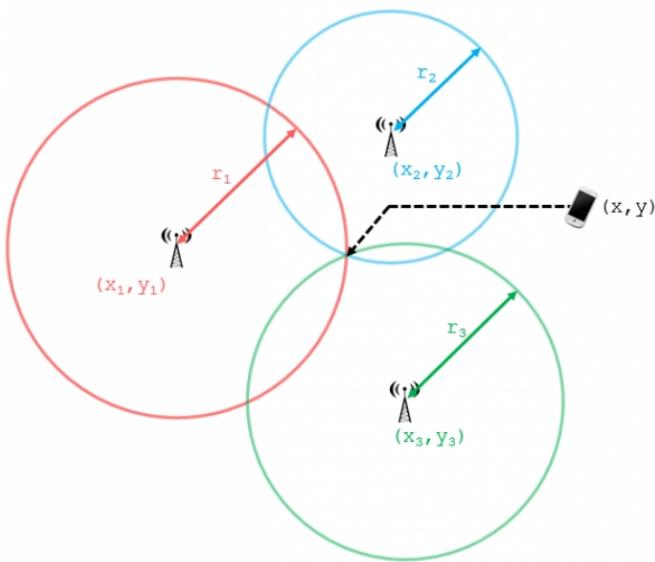
3.1.2. SINIRLAMALAR ve UYGULAMA ALANLARI:

Tek yönlü anten ile yapılan konum tespiti, doğru ekipman ve kalibrasyon ile yüksek hassasiyet sağlayabilir ve birçok uygulama alanında etkili bir çözüm sunabilir. Ancak, çevresel etkenler (örneğin, duvarlar, mobilyalar) ve çoklu yol (multipath) etkisi, sinyal gücünü ve dolayısıyla konum belirleme doğruluğunu etkileyebilir. Bu nedenle, sinyal gücün ölçümlerinin dikkatlice kalibre edilmesi ve çevresel faktörlerin dikkate alınması önemlidir. Ayrıca, antenin sürekli döndürülmesi ve sinyal gücünün her pozisyonda doğru bir şekilde ölçülmesi için hassas bir döndürme mekanizması ve doğru sinyal ölçüm cihazları gereklidir. Bu tür ekipmanlar, konum belirleme doğruluğunu artırırken, maliyet ve uygulama karmaşıklığını da artırabilir.

Sonuç olarak, tek yönlü anten ile yapılan konum tespiti, doğru ekipman ve kalibrasyon ile yüksek hassasiyet sağlayabilir ve birçok uygulama alanında etkili bir çözüm sunabilir. Ancak, bu yöntemin bazı olumsuz yanları da vardır. Çevresel etkenler ve çoklu yol (multipath) etkisi, sinyal gücünü ve dolayısıyla konum belirleme doğruluğunu olumsuz yönde etkileyebilir. Ayrıca, antenin sürekli döndürülmesi ve sinyal gücünün her pozisyonda doğru bir şekilde ölçülmesi için gereken hassas döndürme mekanizmaları ve doğru sinyal ölçüm cihazları, uygulama karmaşıklığını ve maliyetleri artırabilir. Bu nedenle, tek yönlü antenle yapılan konum tespiti her zaman ideal bir çözüm olmayabilir ve uygulanacak senaryoya bağlı olarak dikkatli değerlendirme gerektirir.

3.2. YOL 2: ÜÇ FARKLI YERE KONUMLANDIRILMIŞ ACCESS POINT İLE LOKASYON TESPİTİ (TRİLATERASYON):

Trilaterasyon, bir nesnenin coğrafi konumunu belirlemek için kullanılan bir tekniktir [8]. Bu yöntem, belirli bilinen konumlardan nesneye olan mesafeleri kullanarak nesnenin yaklaşık konumunu hesaplar.



Figür 15: 3 farklı baz istasyonu ve bir telefon ile trilaterasyon. [9]

Yukarıdaki diyagramda, üç farklı access point ve bir istemci cihazı (client) bulunmaktadır. Access point'ler (x_1,y_1) , (x_2,y_2) ve (x_3,y_3) koordinatlarında konumlanmıştır. Her bir access point'in, istemciye olan mesafesi sırasıyla r_1 , r_2 ve r_3 ile gösterilmektedir. Bu mesafeler, genellikle her access point'den gelen sinyal gücünü (RSSI) ölçülerek hesaplanır. Sinyal gücü, mesafe arttıkça zayıfladığı için, bu zayıflama oranı kullanılarak mesafe tahmini yapılabilir. Örneğin, bir access point'den gelen sinyal gücünü ölçülerek r_1 mesafesi hesaplanır. Aynı işlem access point'ler için de yapılır ve böylece r_2 ve r_3 mesafeleri de bulunur. Elde edilen mesafeler ve access point'lerin bilinen koordinatları kullanılarak, üç çemberin kesişim noktalarını hesaplanır ve istemcinin konumu tespit edilmiş olunur.

3.2.1. SİNYAL GÜCÜNDEN (RSSI) X ve Y DENKELMERİNİN ELDE EDİLMESİ:

Her bir çemberin merkezi bir access point'in koordinatlarında ve yarıçapı da o access point'den ölçülen mesafede olacak şekilde tanımlanır. Matematiksel olarak, her bir çember şu şekilde ifade edilir:

Step 1

The three equations for the three circles are as follows:

$$\begin{aligned}(x - x_1)^2 + (y - y_1)^2 &= r_1^2 \\(x - x_2)^2 + (y - y_2)^2 &= r_2^2 \\(x - x_3)^2 + (y - y_3)^2 &= r_3^2\end{aligned}$$

Step 2:

We can expand out the squares in each of these three equations:

$$\begin{aligned}x^2 - 2x_1x + x_1^2 + y^2 - 2y_1y + y_1^2 &= r_1^2 \\x^2 - 2x_2x + x_2^2 + y^2 - 2y_2y + y_2^2 &= r_2^2 \\x^2 - 2x_3x + x_3^2 + y^2 - 2y_3y + y_3^2 &= r_3^2\end{aligned}$$

Step 3:

Now let's subtract the second equation from the first:

$$(-2x_1 + 2x_2)x + (-2y_1 + 2y_2)y = r_1^2 - r_2^2 - x_1^2 + x_2^2 - y_1^2 + y_2^2$$

Likewise, we can now subtract the third equation from the second:

$$(-2x_2 + 2x_3)x + (-2y_2 + 2y_3)y = r_2^2 - r_3^2 - x_2^2 + x_3^2 - y_2^2 + y_3^2$$

Step 4:

Let's rewrite these two equations using A, B, C, D, E, F values. This would result in the following system of 2 equations:

$$\begin{aligned}Ax + By &= C \\Dx + Ey &= F\end{aligned}$$

Step 5:

The solution of this system is:

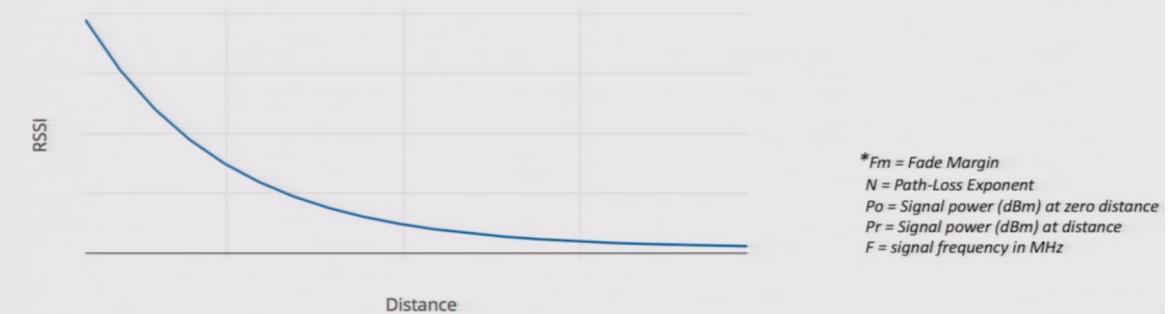
$$\begin{aligned}x &= \frac{CE - FB}{EA - BD} \\y &= \frac{CD - AF}{BD - AE}\end{aligned}$$

Figür 16: Trilaterasyon kullanarak x ve y eksenindeki konumları bulabilmek için gereken denklemin bulunması.

RSS based methods

- Distance can be calculated based on signal strength

$$d = 10^{[(P_0 - F_m - P_r - 10 \times n \times \log_{10}(f) + 30 \times n - 32.44) / 10 \times n]}$$



Figür 17: Sinyal gücünden (dB) mesafe hesaplama formülasyonu [10]

```
@classmethod
def __calculate_distance_by_dbm(cls, rssi: int, n=2, A=-30):
    """
    Calculate the distance from the RSSI value using the path-loss model.

    Parameters:
    rssи (dbm) (int): The received signal strength indicator (RSSI) in dBm.

    Returns:
    float: The estimated distance in meters.

    This function uses the following formula to convert RSSI to distance:
    d = 10^((A - RSSI) / (10 * n))
    where:
    - d is the distance in meters.
    - A is the RSSI value at a reference distance (typically 1 meter).
    - n is the path-loss exponent, which varies depending on the environment.
    """
    return 10 ** ((A - rssи) / (10 * n))
```

Figür 18: RSSI (dbm) değerinden mesafe yapan fonksiyonumuz. [13]

```

@classmethod
def set_antennas_pos(cls, xs, ys):
    cls.xs = xs
    cls.ys = ys

@classmethod
def __trilateration(cls, xs, ys, rs):
    return cls.__solve_equations(xs, ys, rs)

@classmethod
def __solve_equations(cls, xs, ys, rs):
    initial_guess = (0, 0)
    solution = root(cls.__equations, initial_guess, args=(xs, ys, rs), method='lm')
    return solution.x

@classmethod
def __equations(cls, vars, xs, ys, rs):
    x, y = vars
    eqs = np.empty(len(xs)) # Create empty NumPy array with space for 3 elements
    for i in range(3):
        eq = (x - xs[i])**2 + (y - ys[i])**2 - rs[i]**2
        eqs[i] = eq # Assign each equation value to the corresponding index in the array
    return eqs

```

Figür 19: Fonksiyonun devamı. [13]

YOL 3: NTP (Network Time Protocol) PAKETLERİYLE LOKASYON TESPİTİ:

NTP (Network Time Protocol) paketleri, ağ üzerindeki cihazların saatlerini yüksek hassasiyetle senkronize etmelerini sağlayan veri birimleridir [11]. Bir NTP paketi, temel olarak başlık alanı ve zaman damgası alanlarından oluşur. Başlık alanında, sürüm numarası, mod, stratum, poll ve precision gibi protokolün işleyişi için kritik bilgiler yer alır. Zaman damgası alanları ise kök gecikmesi, kök sapması, referans zaman damgası, başlangıç zaman damgası, alım zaman damgası ve iletim zaman damgası gibi, zaman senkronizasyonu ve veri alışverişini sürelerinin izlenmesini sağlayan detaylı zaman bilgilerini içerir. NTP paketleri, bu detaylı zaman bilgileri sayesinde sadece zaman senkronizasyonu sağlamakla kalmaz, aynı zamanda cihazların ağ üzerindeki konumlarının belirlenmesinde de kullanılabilir. Özellikle alım ve iletim zaman damgaları, ağdaki veri yolculuğunun sürelerini analiz ederek cihazların coğrafi konumlarının tespit edilmesine olanak tanır. Bu şekilde, NTP paketleri hem zaman yönetimi hem de lokasyon tespiti gibi kritik görevleri yerine getirerek ağ güvenliği ve yönetiminde önemli bir rol oynar.

Cryptosum	LI	VN	Mode	Strat	Poll	Prec	
				Root Delay			LI = leap indicator
				Root Dispersion			VN = version number
				Reference Identifier			Strat = Stratum (0-15)
				Reference Timestamp			Poll = poll interval
				Seconds (32), Fraction (32)			Prec = Precision
				Originate Timestamp			
				Seconds (32), Fraction (32)			
				Receive Timestamp			
				Seconds (32), Fraction (32)			
				Transmit Timestamp			
				Seconds (32), Fraction (32)			
				Ext. Field 1 Key Identifier (optional)			
				Ext. Field 2 Message Digest (optional)			
Authenticator (Optional)				Key/Algorithm Identifier			
				Message Hash (64 or 128)			

Figür 20: NTP (Network Time Protocol) Paketinin Yapısı [11]

Elimizde bulunan üç farklı access point'in belirli bir istemciye NTP paketi göndermesini sağladığımızda, istemci, access point'lere geri dönüş olarak bir NTP paketi gönderecektir. İstemciden gelen NTP paketinin iletim zaman damgası (transmit timestamp) ile alım zaman damgası (receive timestamp) arasındaki farkı hesapladığımızda, paketin iletilme süresini elde ederiz. Bu süreyi kullanarak, aradaki mesafeyi hesaplayabiliriz. Mesafenin hesaplanması formülü:

x: Mesafe (distance)

$$x = v \times t$$

v: Hız (bu durumda ışık hızı, c)

$$\text{distance} = c \times \Delta t$$

t: Süre (time delta)

Süreyi (time delta) hesaplama formülü:

Client	Connection	Server
Timestamp 1		Timestamp 2
Timestamp 4		Timestamp 3

$\text{Delay} = |(t4 - t1) - (t3 - t2)|$

Figür 21: NTP paketinin sakladığı süreler.

[11]

Figür 22: Time delta'yı elde etmemizi sağlayan formül.

[11]

İşik hızının sabit olduğu göz önüne alındığında, paketin iletilme süresini hesapladığımızda istemci ile access point arasındaki mesafeyi de belirleyebiliriz. Bu işlemi üç farklı access point için yaptığımızda, trilaterasyon yöntemiyle üç çemberin kesişiminden istemcinin x ve y koordinatlarını tespit edebiliriz. Ancak burada önemli bir problem bulunmaktadır: İşik hızında hareket eden bir cisim havada geçirdiği süreyi ölçmek için nanosaniye düzeyinde hassasiyet gerekmektedir [12]. Çünkü ışık hızında hareket eden bir cisim, özellikle bu kadar kısa mesafelerde milisaniye cinsinden ölçülemeyecek kadar hızlı hareket eder. Bu nedenle, time_delta'nın milisaniye değil, nanosaniye cinsinden olması tercih edilir. Bu çözüm, çok daha hassas ölçümler yapabilen kurumsal veya sanayi tipi, pahalı ek cihazlarla (örneğin NTP sunucuları veya FPGA based Wi-Fi stack) kullanıldığında çok daha hassas sonuçlar elde edilir.

Ek olarak, bu yöntemde saldırgan cihazın konumunu tespit edebilmek için saldırgan cihaza paket gönderip ondan paket almamız gerekmektedir. Ancak, saldırganın MAC adresini bilmemiğimizden ona paket gönderemeyiz. Bu nedenle, bu yöntem tek başına problemimizi çözmek için yeterli değildir. Ancak, bu yöntem 3.1. ve 3.2. yöntemlerle birlikte kullanıldığında, kimliğini bilmediğimiz bir cihazın konumunu hassas bir şekilde ölçübileceğimiz bir yöntem daha ortaya çıkar.

BÖLÜM 4

YAZILIM VE DONANIM MİMARİSİ

Bu bölümde, projemizin [13] yazılım ve donanım mimarisinden bahsedilecektir.

4.1. ROLLER:

Saldırgan (hacker):

Monitor modda access point'lere manipüle edilmiş de-authentication paketi gönderen herhangi bir access point'e associate ve authenticate olmamış bir client.

Access Point (Erişim Noktası):

Diğer Wi-Fi cihazlarının kablolu bir ağa veya kablosuz ağa bağlanmasını sağlayan bir ağ donanım cihazı.

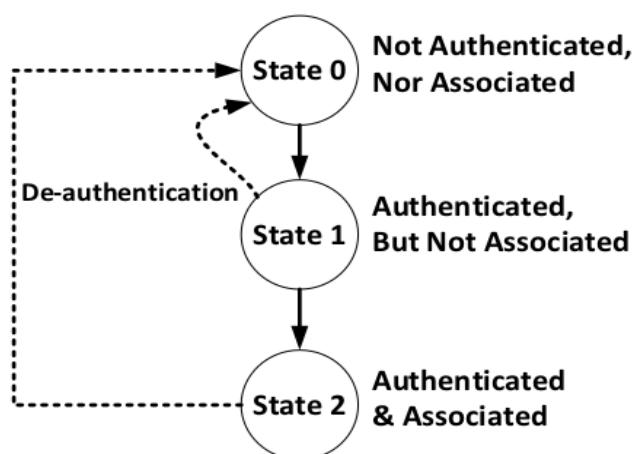
Client (İstemci):

Durum 0: İstemcinin kimliği doğrulanmadı (unauthenticated) veya ilişkilendirilmedi (unassociated).

Durum 1: İstemci kimliği doğrulandı ancak ilişkilendirilmedi.

Durum 2: İstemci kimliği doğrulandı ve ilişkilendirildi. İstemci artık AP ile veri alışverişi gerçekleştirebilir.

(Bir de-authentication paket alındığında (saldırıya uğrandığında), istemcinin o anda içinde bulunduğu durumdan (Durum 1 veya Durum 2) bağımsız olarak doğrudan Durum 0'a geçtiği unutulmamalıdır).



Figür 23: Bir Wi-Fi istemcisinin muhtemel durumları [4]

Intrusion Detection System (IDS): Kötü niyetli kullanıcıların sistemlere veya ağlara yetkisiz erişimini tespit eder. IDS'lerin birincil görevleri ana bilgisayarları ve ağları izlemek, bilgisayar sistemi etkinliğini değerlendirmek, uyarılar üretmek ve şüpheli davranışlara yanıt vermektedir, gerekiyse saldırıyı önlemektir.

Admin (Yönetici): Saldırının tespiti halinde IDS tarafından üretilen alarmların kendisini uyaracağı kişi(ler).

4.2. USE CASE DİYAGRAMLARI:

4.2.1. AKTÖRLER:

Network Admin (Ağ Yönetcisi):

Sistemi kuracak, çalıştıracak, yönetecek, bakımını yapacak, açıp kapatacak ve saldırının tespiti halinde haber alacak, gerekirse aksiyon alacak kişi.

Client (İstemci):

Herhangi bir, saldırından etkilenen veya etkilenmeyen istemcidir.

Access Point:

Erişim noktası, yani router, modem gibi cihazlar. Saldırıya uğrayan istemciler, access point'lere bağlıdır. Saldırıyı önlerken kullanılan yöntem access point'ler ile Attacker Client arasındaki bağlantıyı kesmeye yönelik olması planlanmaktadır.. (bkz: jammer)

Anten:

MU'ya bağlı, istenilen access point'in veya istemcinin anlık fiziksel konumunu bulmaya ve ağı taramaya yardımcı olan aygit(lar).

IDS (Anomali Tespit Sistemi):

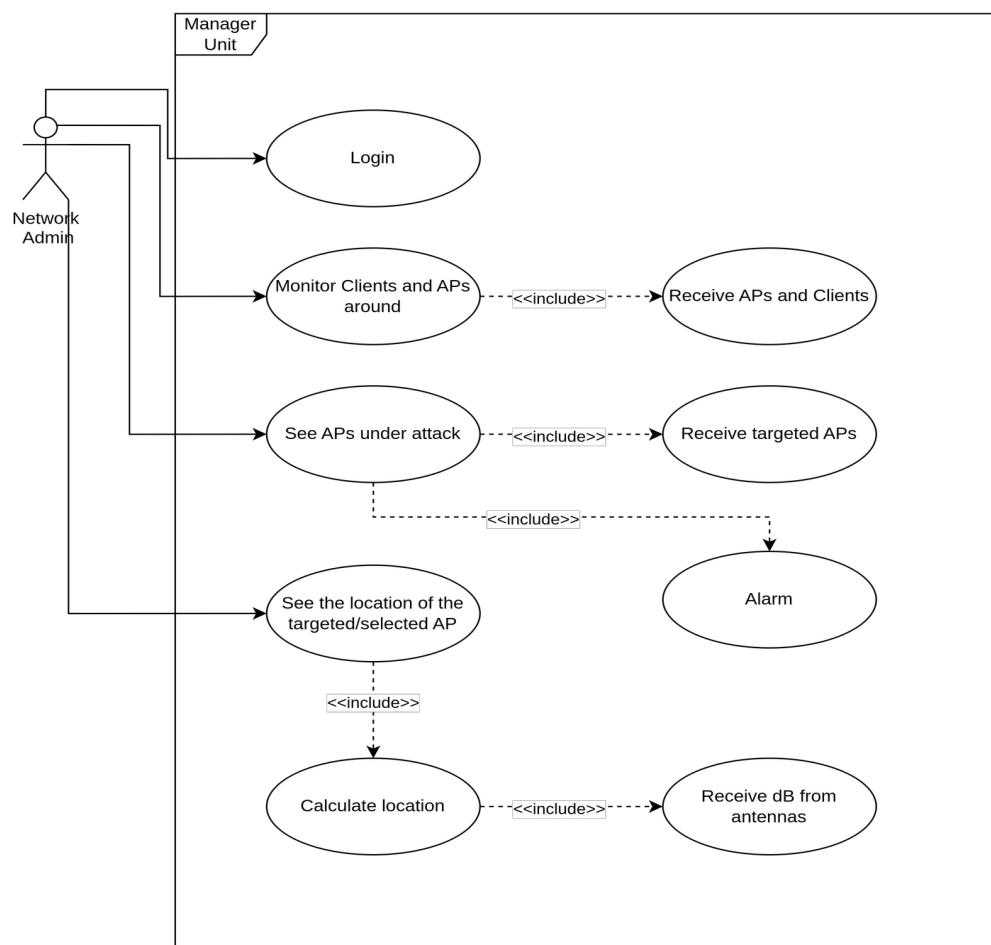
Saldırı tespitini yapacak makine öğrenmesi algoritmasını çalıştırın ve konum tespiti hesaplamaları yapan sistem.

Manager Unit (MU): Yönetim birimi. Network Admin'e kullanıcı arayüzü sunan, diğer modüllerini ve aygıtları birbiriyle haberleştiren, hesaplama işlemlerini yapan ana sunucu, sistem.

Wi-Fi Card Interface (WCI): MU ile antenler arasındaki iletişim kuracak MU'ya bağlı kartın arayüzü.

4.2.2. SİSTEM FONKSİYONLARI:

Manager Unit (MU) Fonksiyonları:



Figür 24: Manager Unit Modülü Use Case Diagramı

Login:

Sistemi sadece giriş yapabilenler kullanabilir. Güvenlik sağlamak maksadıyla bu fonksiyon kullanıcıya zorunlu kılmıştır.

Monitor Clients and APs around:

Civardaki AP ve Client'ları izleme.

See APs under attack:

Hangi AP veya Client üzerinde saldırı olduğunu görme.

See the location of the targeted/selected AP/Client:

Seçilen herhangi bir AP veya Client'in yaklaşık coğrafi konumunu öğrenme.

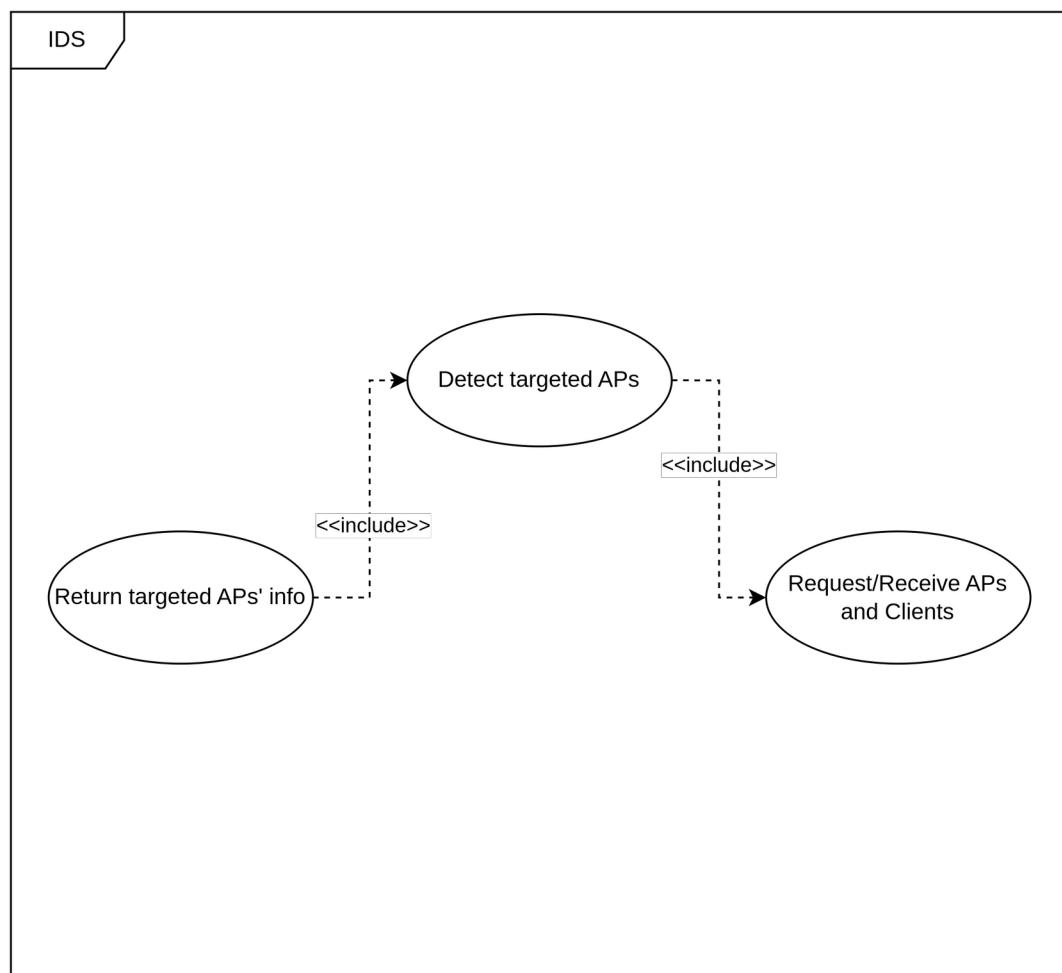
Alarm:

Saldırı tespit edildiğinde Network Admin'i uyarma.

Calculate location:

Antenlerden alınan sinyal gücü bilgisiyle istenilen Client ya da AP'nin yaklaşık coğrafi konumunu hesaplama.

IDS Fonksiyonları:

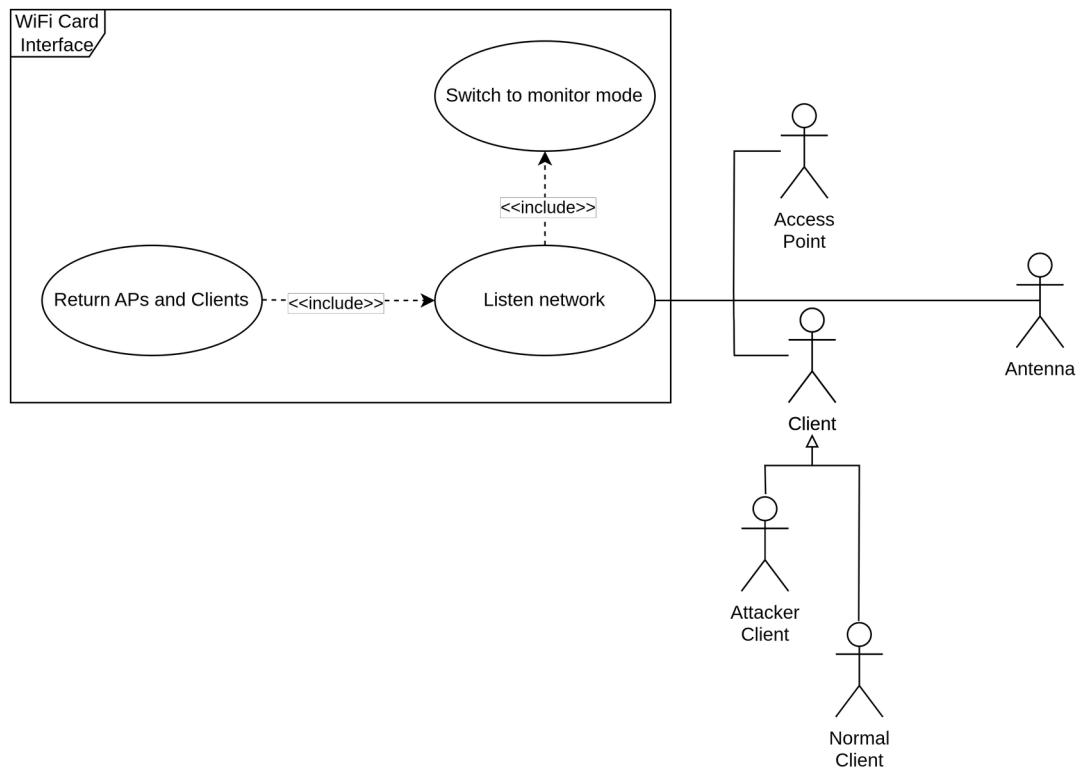


Figür 25: IDS Modülü Use Case Diagramı

Detect Targeted APs:

Saldırıgın tarafından hedef alınan AP'leri tespit et.

Wifi Card Interface:



Figür 26: WiFi Card Interface Modülü Use Case Diagramı

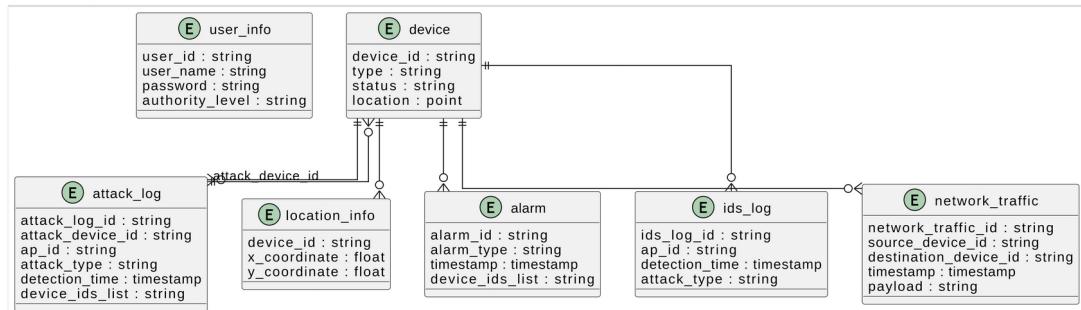
Listen Network:

Anten'in sinyal aldığı tüm aygıtların ağ trafiğini dinle.

Switch to monitor mode:

Wifi Card'ı monitör moda al. (Ağı dinlemek için gereklidir.)

4.3. ERD: ERD DİYAGRAMININ YAPISI:



Figür 27: Projenin ER Diyagramı.

Tablolar:

user_info: Network admin ve diğer yetkili kullanıcıların giriş bilgilerini içerir. (user_id, user_name, password, authority_level)

device: AP'ler, istemciler, saldırgan istemciler ve diğer cihazları temsil eder. (device_id, type, status, location)

attack_log: Saldırı ve saldırılara ilişkin bilgileri kaydeder. (attack_log_id, attack_device_id, ap_id, attack_type, detection_time, device_ids_list)

location_info: Her cihazın yaklaşık fiziksel konumunu içerir. (device_id, x_coordinate, y_coordinate)

alarm: Oluşturulan alarmları kaydeder. (alarm_id, alarm_type, timestamp, device_ids_list)

ids_log: Saldırı tespiti ile ilgili bilgileri içerir. (ids_log_id, ap_id, detection_time, attack_type)

network_traffic: Ağ trafiği dinleme ve kaydetme amacıyla kullanılır. (network_traffic_id, source_device_id, destination_device_id, timestamp, payload) İlişkiler:

İlişkiler:

device tablosu, location_info, attack_log, alarm, ids_log ve network_traffic tablolarına bir-çok ilişki ile bağlıdır. Bu, her cihazın birden fazla konum bilgisi, saldırısı, alarm, saldırısı tespiti ve ağ trafiği kaydı olabileceğini gösterir.

attack_log tablosu, device tablosuna foreign key ilişkisi ile bağlıdır. Bu, bir saldırının hangi cihaza etki ettiğini takip etmek için kullanılır.

4.4. KULLANILAN DONANIM VE YAZILIMLAR:

Bu bölümde, projede kullanılan donanım ve yazılımlardan bahsedilecektir.

4.4.1. DONANIMLAR:

Access Point/Router’lar:

2 adet AirTies 2.4 GHz 125 Mbps ADSL2+ 1 LAN Port (Model: RT-205)
(Harici 2 antenli)

1 adet tp-link 2.4 GHz 300 Mbps VDSL/ADSL 4 LAN Port Router (Model: VN020-F3)
(Harici 2 antenli)

Network Interface Kartları:

1 adet Ethernet controller: Realtek Semiconductor Co., Ltd. RTL8111/8168/8411
PCI Express Gigabit Ethernet Controller (rev 10)

1 adet Network controller: Intel Corporation Wi-Fi 6 AX200 (rev 1a)

Bilgisayar:

Lenova ThinkPad E14 Gen 2 (Ubuntu 22.04)

4.4.2. YAZILIMLAR:

Programlama Dilleri:

Python 3.10, Bash, Java Script

Framework'ler:

Django

Teknolojiler:

- AirTools (kendi yazdığımız kütüphane)
- Aircrack-ng tools (ağın taranması ve WiFi card interface kontrolü gibi işlevler),
- NumPy, Pandas, Keras (makine öğrenmesi modellerinin eğitimi),
- Weka (makine öğrenmesi modellerinin testi),
- OpenWrt (Access Point'lerin konfigurasyonu)
- subprocess, Xterminal

...

4.5. PROJEDEN GÖRÜNTÜLER:

The screenshot shows a web-based administration panel titled "Wi-Fi Deauth IDS Admin Panel". The top navigation bar includes links for Home, Start Scan, and Contact. Below the header, it displays the current time as "June 22, 2024, 12:38 p.m." and the number of attacked devices as "96". The main content area is titled "Devices" and contains a table listing 10 entries of attacked devices. Each entry includes the Mac Address, Signal Power (dBm), GeoLocation (x, y), Attack count, and Date.

Mac Address	Signal Power (dBm)	GeoLocation (x, y)	Attack	Date
ff:ff:ff:ff:ff:ff	[-33, -33, -33]	[152.34637689760373, 157.47597479571547]	1	May 31, 2024 16:13:55.752048821 +03
5e:f2:46:cc:a7:2a	[-32, -32, -32]	[152.34794164404695, 157.47524742911656]	0	May 31, 2024 16:13:35.872984991 +03
01:25:9e:ee:ee:ee	[-84, -84, -84]	[470.3658478702948, -161.36646983187188]	1	May 31, 2024 15:53:49.297086150 +03
1c:bf:c0:7d:95:bd	[-25, -25, -25]	[152.34843183048838, 157.47669403178997]	0	May 31, 2024 15:45:54.807185633 +03
2a:07:bd:20:55:a1	[-25, -25, -25]	[152.34843183048838, 157.47669403178997]	0	May 31, 2024 15:27:15.953913885 +03
40:5b:d8:d9:fa:e9	[-26, -26, -26]	[152.34836885379505, 157.4766610100197]	1	May 31, 2024 15:27:12.283748515 +03
32:61:47:0c:c4:65	[-25, -25, -25]	[152.34843183048838, 157.47669403178997]	0	May 31, 2024 15:23:54.975189609 +03
26:15:63:87:ab:d5	[-27, -27, -27]	[152.34828159366336, 157.47662033775202]	1	May 31, 2024 15:23:34.291161059 +03

Figür 28: Admin Panel Ana Sayfası - Turuncu olanlar saldırı altında olan cihazları ifade ediyor. [13]

```

hsrv@hsrv-e14:~/Desktop/deauth_anadolu/DeauthPanel$ python3 manage.py runserver
Watching for file changes with StatReloader
Performing system checks...
System check identified no issues (0 silenced).
June 22, 2020 - 12:41:16
Django version 4.2, using settings 'adminpanel.settings'
Running development server at http://127.0.0.1:8000/
Quit the server with CONTROL-C.

<QuerySet [DeviceData: ff:ff:ff:ff:ff:ff, <DeviceData: f8:4a:bf:58:12:00>, <DeviceData: f8:4a:bf:58:12:00>, <DeviceData: ec:3:bb:01:00:8f, <DeviceData: 01:25:9e:ee:ee:ee>, <DeviceData: 58:96:1d:2a:c3:d4>, <DeviceData: ac:75:1d:7fed:15>, <DeviceData: 02:96:ef:fd:0b:7f>, <DeviceData: dc:46:28:4e:e6:57>, <DeviceData: 01:00:5e:4d:4d:4d>, <DeviceData: 67:bb:56:5a:ea:9d>, <DeviceData: ec:77:1d:17:df:b4>, <DeviceData: 4c:facc:71:cc:eb>, <DeviceData: 00:00:0c:9f:f1:05>, <DeviceData: 02:b9:28:4b:0e:10>, <DeviceData: e0:e0:1f:4a:14:de>, <DeviceData: e6:56:48:d2:d3:5e>, <DeviceData: 66:30:dd:3f:1f:16>, <DeviceData: 2:a:aa:18:a7:24>f3>, <DeviceData: b2:53:93:ef:77:12>, ...]>]
[22/Jun/2024 12:41:20] "GET / HTTP/1.1" 200 38551
<QuerySet [DeviceData: ff:ff:ff:ff:ff:ff, <DeviceData: f8:4a:bf:58:12:00>, <DeviceData: f8:4a:bf:58:12:00>, <DeviceData: ec:3:bb:01:00:8f, <DeviceData: 01:25:9e:ee:ee:ee>, <DeviceData: 58:96:1d:2a:c3:d4>, <DeviceData: ac:75:1d:7fed:15>, <DeviceData: 02:96:ef:fd:0b:7f>, <DeviceData: dc:46:28:4e:e6:57>, <DeviceData: 01:00:5e:4d:4d:4d>, <DeviceData: 67:bb:56:5a:ea:9d>, <DeviceData: ec:77:1d:17:df:b4>, <DeviceData: 4c:facc:71:cc:eb>, <DeviceData: 00:00:0c:9f:f1:05>, <DeviceData: 02:b9:28:4b:0e:10>, <DeviceData: e0:e0:1f:4a:14:de>, <DeviceData: e6:56:48:d2:d3:5e>, <DeviceData: 66:30:dd:3f:1f:16>, <DeviceData: 2:a:aa:18:a7:24>f3>, <DeviceData: b2:53:93:ef:77:12>, ...]>]
[22/Jun/2024 12:41:36] "GET / HTTP/1.1" 200 38487
<QuerySet [DeviceData: ff:ff:ff:ff:ff:ff, <DeviceData: f8:4a:bf:58:12:00>, <DeviceData: f8:4a:bf:58:12:00>, <DeviceData: ec:3:bb:01:00:8f, <DeviceData: 01:25:9e:ee:ee:ee>, <DeviceData: 58:96:1d:2a:c3:d4>, <DeviceData: ac:75:1d:7fed:15>, <DeviceData: 02:96:ef:fd:0b:7f>, <DeviceData: dc:46:28:4e:e6:57>, <DeviceData: 01:00:5e:4d:4d:4d>, <DeviceData: 67:bb:56:5a:ea:9d>, <DeviceData: ec:77:1d:17:df:b4>, <DeviceData: 4c:facc:71:cc:eb>, <DeviceData: 00:00:0c:9f:f1:05>, <DeviceData: 02:b9:28:4b:0e:10>, <DeviceData: e0:e0:1f:4a:14:de>, <DeviceData: e6:56:48:d2:d3:5e>, <DeviceData: 66:30:dd:3f:1f:16>, <DeviceData: 2:a:aa:18:a7:24>f3>, <DeviceData: b2:53:93:ef:77:12>, ...]>]
[22/Jun/2024 12:41:43] "GET / HTTP/1.1" 200 38589
<QuerySet [DeviceData: ff:ff:ff:ff:ff:ff, <DeviceData: f8:4a:bf:58:12:00>, <DeviceData: f8:4a:bf:58:12:00>, <DeviceData: ec:3:bb:01:00:8f, <DeviceData: 01:25:9e:ee:ee:ee>, <DeviceData: 58:96:1d:2a:c3:d4>, <DeviceData: ac:75:1d:7fed:15>, <DeviceData: 02:96:ef:fd:0b:7f>, <DeviceData: dc:46:28:4e:e6:57>, <DeviceData: 01:00:5e:4d:4d:4d>, <DeviceData: 67:bb:56:5a:ea:9d>, <DeviceData: ec:77:1d:17:df:b4>, <DeviceData: 4c:facc:71:cc:eb>, <DeviceData: 00:00:0c:9f:f1:05>, <DeviceData: 02:b9:28:4b:0e:10>, <DeviceData: e0:e0:1f:4a:14:de>, <DeviceData: e6:56:48:d2:d3:5e>, <DeviceData: 66:30:dd:3f:1f:16>, <DeviceData: 2:a:aa:18:a7:24>f3>, <DeviceData: b2:53:93:ef:77:12>, ...]>]
[22/Jun/2024 12:41:49] "GET / HTTP/1.1" 200 38488

```

Figür 29: Admin Paneli Back-end Logları [13]

```

hsrv@hsrv-e14:~/Desktop/deauth_anadolu/IDS$ sudo ./run.sh
[sudo] password for hsrw:

Found 4 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

      PID Name
      555 avahi-daemon
      560 NetworkManager
     605 wpa_supplicant
     615 avahi-daemon

      PHY   Interface       Driver       Chipset
phy0    wlp3s0           iwlwifi      Intel Corporation Wi-Fi 6 AX200 (rev 1a)
          (mac80211 monitor mode vif enabled for [phy0]wlp3s0 on [phy0]wlp3s0mon)
          (mac80211 station mode vif disabled for [phy0]wlp3s0)

IDS AWAKE!

Time: Dec 18, 2020 18:42:58.482600000 +03
    wlan.fc.type_subtype wlan.fc.type wlan.fc.protected time_difference num_of_deauth_frames
0                 8             0                  0        0.004271           5
Deauth Attack!
Output info sent to the admin panel server successfully!
---
MAC: ff:ff:ff:ff:ff:ff
dbms: [-34, -34, -34]
GeoLocation: (x: 152.3471083315625, y: 157.47551935226284)
---

Time: Dec 18, 2020 18:42:58.585010000 +03
    wlan.fc.type_subtype wlan.fc.type wlan.fc.protected time_difference num_of_deauth_frames
0                 8             0                  0        0.008542           6
Deauth Attack!
Output info sent to the admin panel server successfully!
---
MAC: ff:ff:ff:ff:ff:ff
dbms: [-34, -34, -34]
GeoLocation: (x: 152.3471083315625, y: 157.47551935226284)
---

Time: Dec 18, 2020 18:42:58.629796000 +03
    wlan.fc.type_subtype wlan.fc.type wlan.fc.protected time_difference num_of_deauth_frames
0                 32            2                  1        0.012813           7
Deauth Attack!
Output info sent to the admin panel server successfully!
---
MAC: ff:ff:ff:ff:ff:ff

```

Figür 30: IDS'in, Admin Panel ile HTTP protokolü üzerinden haberleşmesi ve tutulan ek loglar. [13]



Figür 31: IDS sistemini test etmek için kendi yazdığımız saldırının arayüzü. [13]

```
Hi jumpppy :>

--> Network Adapter Mode: monitor

Available access points to attack:
ESSID          BSSID           Channel      S
signal Level

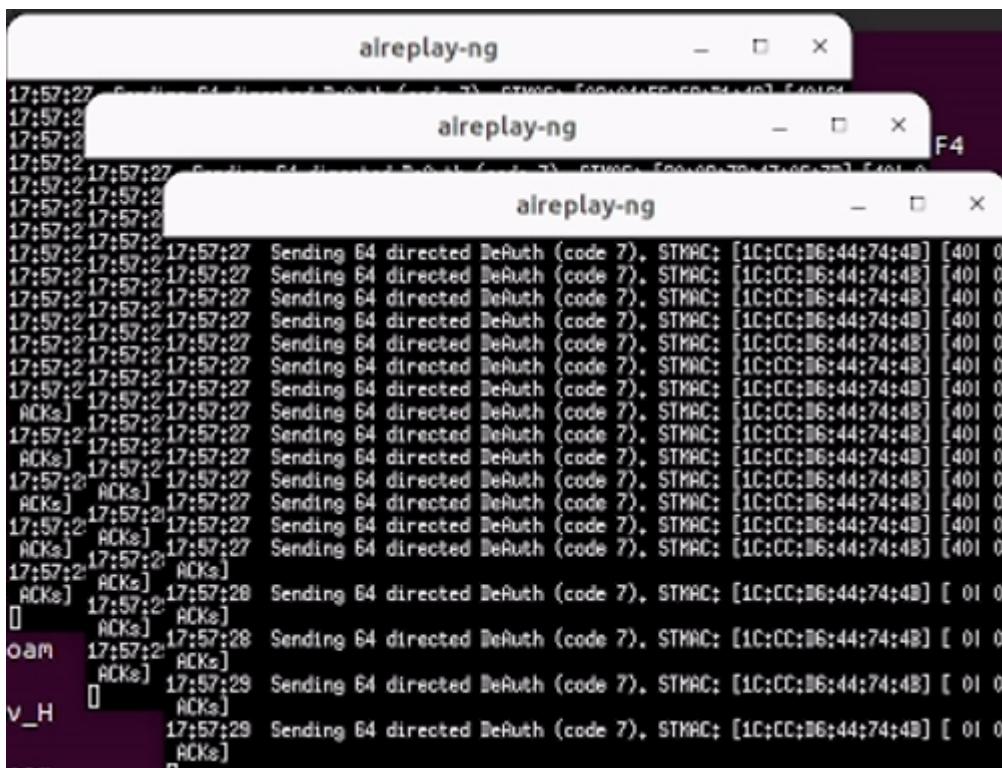
TEST WIFI      CE:83:9F:5A:77:F4          1
-40
kbunv_H        F8:4A:BF:58:0F:00          12
50
eduroam        F8:4A:BF:58:0F:02          12
50
kbunv_H        F8:4A:BF:58:0D:C0          11
57
eduroam        F8:4A:BF:58:0D:C2          11
58
kbunv_H        D4:B1:10:B1:FF:60          7
74
eduroam        D4:B1:10:B1:FF:62          7
75
kbunv_H        AC:4E:91:5F:03:00          9
75
eduroam        AC:4E:91:5F:03:02          9
75
kbunv_H        F8:4A:BF:58:10:40          6
76
eduroam        F8:4A:BF:58:10:42          6
77
eduroam        F8:4A:BF:58:0E:82          4
80
kbunv_H        F8:4A:BF:58:0E:80          4
81
Galaxy A318A16  86:F1:9E:B8:58:0D          6
-83
eduroam        AC:4E:91:5F:04:E2          10
84
kbunv_H        AC:4E:91:5F:04:E0          10
85
kbunv_H        F8:4A:BF:56:79:A0          8
85

Choose target BSSID (Default = all targets):CE:83:9F:5A:77:F4
```

Figür 32: Kendi yazdığımız Attacker aracımızda mevcut ağları listeleme ve hedef ağ(lar) seçimi. [13]

CH 1][Elapsed: 20 mins][2024-06-10 17:56][WPA handshake: CE:83:9F:5A:77:F4										
BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID	
BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes			
CE:83:9F:5A:77:F4	2A:08:72:47:A6:30	-29	1e-24	33	17132	EAPOL				
CE:83:9F:5A:77:F4	1C:CC:D6:44:74:4B	-32	1e- 1e	0	17859					
CE:83:9F:5A:77:F4	02:04:5C:C8:D1:48	-48	24e-24e	0	2173					

Figür 33: Hedef Access Point'e bağlı Client'ların listelenmesi. [13]



Figür 34: Hedef Client'lara paralel/eş zamanlı olarak saldırılması. [13]

BÖLÜM 5

SONUÇ ve GELECEK ARAŞTIRMA YÖNLERİ

Bu çalışmada, 802.11 Wi-Fi ağlarında De-authentication saldırısını tespit etmek için yenilikçi bir Makine Öğrenimi tabanlı Saldırı ve Saldırgan Tespit Sistemi (IDS) geliştirilmiştir. Önerilen IDS, De-authentication saldırularını yüksek tespit oranı ve düşük yanlış pozitif oranıyla belirleyerek, saldırı sonrası kimliği belirsiz saldırının coğrafi konumunu tespit etme yeteneğine sahiptir. Makine Öğrenimi tabanlı bu IDS'nin önemli bir avantajı, protokol değişikliklerine, şifreleme algoritmalarının kullanımına veya donanım yazılımı güncellemelerine ihtiyaç duymamasıdır. Ayrıca, bu sistem eski ve günümüz ağ sistemlerinde uygulanabilirliği ile dikkat çekmektedir.

Gelecekteki araştırma yönleri, saldırının coğrafi konumunu tespit etme gerekliliğini ortadan kaldırarak doğrudan kimliğinin belirlenmesi üzerine yoğunlaşabilir. Ayrıca, saldırının coğrafi konumunu daha hassas, daha az karmaşık ve maliyet açısından daha verimli bir şekilde belirleme yöntemleri üzerine çalışmalar da yapılabilir. Bu tür ilerlemeler, ağ güvenliğinde daha etkili ve kapsamlı çözümler geliştirilmesine katkı sağlayacaktır.

KAYNAKLAR

1. <https://www.wi-fi.org/beacon/philipp-ebbecke/protected-management-frames-enhance-wi-fi-network-security> (5 Aralık 2023)
2. <https://www.aircrack-ng.org/doku.php?id=aircrack-ng> (23 Aralık 2023)
3. <https://thecybersecurityman.com/2018/08/11/creating-an-evil-twin-or-fake-access-point-using-aircrack-ng-and-dnsmasq-part-2-the-attack/> (2 Ocak 2024)
4. Agarwal, M., Biswas, S., & Nandi, S. (2015, October). Detection of De-authentication DoS attacks in Wi-Fi Networks: A Machine Learning Approach. In 2015 IEEE International Conference on Systems, Man, and Cybernetics (pp. 1408-1413). IEEE.
5. <https://icsdweb.aegean.gr/awid/awid3> (6 Şubat 2024)
6. AWID 3 Veri Setinin readme.txt dosyası.
7. <https://www.quwireless.com/post/what-are-the-differences-between-omni-directional-and-unidirectional-antennas> (15 Nisan 2024)
8. <https://gisgeography.com/trilateration-triangulation-gps/> (20 Nisan 2024)
9. <https://www.101computing.net/cell-phone-trilateration-algorithm/> (10 Ocak 2024)
10. https://www.youtube.com/watch?v=vtnlgTj_A (15 Ocak 2024)
11. <https://www.meinbergglobal.com/english/info/ntp-packet.htm> (18 Haziran 2024)
12. <https://en.wikipedia.org/wiki/Light-second> (21 Haziran 2024)
13. <https://github.com/deauth-anadolu> (23 Haziran 2024)
14. Gebresilassie, S. K., Rafferty, J., Chen, L., Cui, Z., & Abu-Tair, M. (2023, Eylül 4). Transfer and CNN-Based De-Authentication (Disassociation) DoS Attack Detection in IoT Wi-Fi Networks. *Electronics*, 12(17), 3731.

ÖZGEÇMIŞ

Ahmet Husrev ÇEKER 2001 yılında İstanbul'da doğdu; ilk ve orta öğrenimini İstanbul'da tamamladı. 2019 yılında Karabük Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü'nde öğrenime başlamış olup 4. sınıfta öğrenimine hâlâ devam etmektedir. 2024 Ekim ayında diploma alması öngörlülmektedir.

ADRES BİLGİLERİ

Adres : İstanbul / Kartal

E-posta : ahmethusrev+bitirmeprojesi@protonmail.com