TOBB EKONOMİ VE TEKNOLOJİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

802.11AC ORTAMINDA MAKİNE ÖĞRENMESİ YAKLAŞIMLARI İLE DONANIM TABANLI SALDIRI TESPİT SİSTEMİ VE 802.11S ÖRGÜ AĞLARINA YÖNELİK SALDIRI GERÇEKLEMELERİ

YÜKSEK LİSANS TEZİ

Ozan YÜKSEL

Elektrik ve Elektronik Mühendisliği Anabilim Dalı

Tez Danışmanı: Prof. Dr. Murat ALANYALI

ARALIK 2021

TEZ BİLDİRİMİ

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, alıntı yapılan kaynaklara eksiksiz atıf yapıldığını, referansların tam olarak belirtildiğini ve ayrıca bu tezin TOBB ETÜ Fen Bilimleri Enstitüsü tez yazım kurallarına uygun olarak hazırlandığını bildiririm.

.

Ozan YÜKSEL

ÖZET

Yüksek Lisans Tezi
802.11AC ORTAMINDA MAKİNE ÖĞRENMESİ YAKLAŞIMLARI İLE DONANIM TABANLI SALDIRI TESPİT SİSTEMİ VE 802.11S ÖRGÜ AĞLARINA YÖNELİK SALDIRI GERÇEKLEMELERİ

Ozan YÜKSEL

TOBB Ekonomi ve Teknoloji Üniversitesi
Fen Bilimleri Enstitüsü
Elektrik ve Elektronik Mühendisliği Anabilim Dalı

Danışman: Prof. Dr. Murat Alanyalı
Tarih: Aralık 2021

Kablosuz teknolojiler günümüzde ulaştığı yüksek veri hızlarıyla beraber kullanım alanlarını günlük hayattan endüstriyel ve askeri uygulamalara kadar genişletmiştir. Kablosuz teknolojilerin kullanımın artmasıyla beraber konumlandırıldıkları ağlarda siber saldırılara maruz kalma riskleri ve bu risklerin potansiyel etkisi gün geçtikçe artmaktadır. Potansiyel saldırı senaryolarına ve ilgili korunma yaklaşımlarına ışık tutmak amacıyla tez çalışmasının ilk bölümünde 802.11 Temel Servis Seti mimarisinde Makine Öğrenmesi yaklaşımları ile donanım üzerinde uçtan uca oluşturulan modüler yapıda bir Kablosuz Saldırı Tespit Sistemi gerçeklenmektedir. İkinci bölümde ise 802.11s Kablosuz Örgü Ağlarında tanımlı Sahte Kimlik Doğrulama, Yol Saptırma ve Karadelik saldırıları özelinde oluşturulmuş yazılım mimarisi kullanılarak saldırı gerçeklemeleri yapılmaktadır.

Anahtar Kelimeler: 802.11, 802.11s, 802.11ac, HWMP, Kablosuz ağ güvenliği, Kablosuz ağ saldırıları, Örgüsel ağlar, Kampüs ağları, Kablosuz saldırı tespit sistemi, Makine öğrenmesi, Derin öğrenme

ABSTRACT

Master of Science

MACHINE LEARNING APPROACHES ON HARDWARE BASED INTRUSION DETECTION SYSTEM AND IMPLEMENTATIONS OF 802.11S ATTACKS ON AN 802.11AC BASED WIRELESS TESTBED ENVIRONMENT

Ozan YUKSEL

TOBB University of Economics and Technology
Institute of Natural and Applied Sciences
Department of Electrical and Electronics Engineering

Supervisor: Prof. Dr. Murat ALANYALI
Date: December 2021

Application areas of wireless LAN technologies follow a rapid expansion trend due to the ever increasing bandwidth they offer at the physical layer. This trend inevitably entails higher costs due to potential cyber security vulnerabilities. In the first part of this thesis, end-to-end and modular Wireless Intrusion Detection System are implemented with the machine learning approaches on hardware in 802.11 Basic Service Set architecture. In the second part, Fake Mesh Authentication, Path Diversion and Blackhole attacks which are defined in 802.11s Wireless Mesh Networks are implemented using software architecture specifically created for these attacks.

Keywords: 802.11, 802.11s, 802.11ac, HWMP, Wireless network security, Wireless attacks, Wireless mesh networks, Campus networks, Wireless intrusion detection system, Machine learning, Deep learning

TEŞEKKÜR

Yüksek Lisans süresince ders aldığım tüm TOBB Ekonomi ve Teknoloji Üniversitesi öğretim üyelerine paylaştıkları kıymetli bilgiler için şükranlarımı sunuyorum.

Ayrıca çalıştığım kurum olan ASELSAN A.Ş.'deki tüm çalışma arkadaşlarım ve yöneticilerime bu süreçteki destekleri için minnettarım.

Danışmanım Sn. Prof. Dr. Murat ALANYALI'ya Yüksek Lisans sürecim boyunca bana kattıklarından ötürü çok teşekkür ediyorum. Bana karşı her zaman olumlu ve hoşgörülü tutumunun yanı sıra, uzmanlığı, engin tecrübesi ve eşsiz rehberliği bu çalışmayı muktedir kılan en önemli nedenlerdir.

Son olarak sevgili ailem; Annem, Babam ve Abim. Bu zamana kadar kendime ne katabildiysem hepsi sizlerin sayesinde mümkün oldu. Giriştiğim her macerada sonsuz fedakarlıklarınızla yanımdaydınız ve tez çalışmalarım sırasında da bana olan desteğiniz paha biçilemezdi. Siz olmasaydınız, başaramazdım. İyi ki varsınız.

İÇİNDEKİLER

ŞEKİL LİSTESİ

Sayfa

ÇİZELGE LİSTESİ

Sayfa

KISALTMALAR

AES : Advanced Encryption Standard
A-MPDU **:** Aggregate MAC Protocol Data Unit
A-MSDU **:** Aggregate MAC Service Data Unit
AP **:** Access Point
AWID **:** Aegean Wi-Fi Intrusion Dataset
CCMP **:** Counter Mode Cipher Block Chainig Message Authetication Code Protocol
CPU **:** Central Processing Unit
CTS **:** Clear to Send
DOS **:** Denial of Service
EAP **:** Extensible Authentication Protocol
EAPOL **:** Extensible Authentication Protocol over LAN
EDCA : Enhanced Distributed Channel Access
Gbit/s **:** Gigabit bölü saniye
GHz **:** Giga Hertz
GPU **:** Grafical Processing Unit
HWMP **:** Hybrid Wireless Mesh Protocol
IP **:** Internet Protocol
IEEE **:** Institute of Electrical and Electronics Engineers
MAC **:** Media Access Control
Mbit/s **:** Megabit bölü saniye
MCCA : MCF Coordinated Channel Access
MHz **:** Mega Hertz
MIMO **:** Multiple Input Multiple Output
MP **:** Mesh Point
MU-MIMO : Multi User Multiple Input Multiple Output
OFDM **:** Orthagonal Frequency Division Muliplexing
OSI **:** Open System Interconnection
QAM **:** Quadrature Amplitude Modulation
RADIUS **:** Remote Authentication Dial-In User Service
RTS **:** Request to Send
Wi-Fi **:** Wireless Fidelity
RF **:** Radio Frequency
SSH : Secure Shell
SSID : Service Set Identifier
SU-MIMO **:** Single User Multiple Input Multiple Output
TKIP **:** Temporal Key Integrity Protocol
USB **:** Universal Serial Bus
WEP **:** Wired Equivalent Privacy
WPA **:** Wi-Fi Protected Access
WPA2 **:** Wi-Fi Protected Access-2
WPA3 **:** Wi-Fi Protected Access-3

1. GİRİŞ

Wi-Fi teknolojileri kullanıcılara günlük hayatta, endüstriyel ve askeri uygulamalarda güvenilir ve istikrarlı deneyim sunmaktadır. Wi-Fi teknolojileri kullanıcılara sunduğu bu deneyimin yanında, 3 Trilyon dolar market hacmiyle [1] beraber 13 milyar cihaza yayılan etki alanıyla dünya internet trafiğinin yarısından fazlasını taşımaktadır [2].

802.11ac gibi yayınlanan yeni Wi-Fi standartlarıyla beraber, Wi-Fi fiziksel katman bant genişlikleri 7 Gbit/s veri hızlarının ötesine geçmeye başlamıştır [3]. Kablosuz teknolojilerdeki önemli veri hızı artışlarıyla beraber, kablosuz ağ kullanımı Erişim Noktaları (Access Points) ve ona bağlı istasyonların (Stations) oluşturduğu Temel Servis Seti (Basic Service Set) ve Erişim Noktalarının IEEE 802.11s, Kablosuz Örgü Ağı, standardı ile uyumlu olarak oluşturduğu Örgü Temel Servis Seti (Mesh Basic Service Set) mimarilerini içeren dağıtık ağlarla beraber daha da genişlemekte, bunun yanında kompleks ve zorlu ağ topolojilerinin de kullanımı gün geçtikçe yaygınlaşmaya devam etmektedir. Ayrıca IEEE 802.11s standardı, dinamik olarak kendi kendini organize eden, kendi kendini yapılandıran ve insan müdahalesi olmaksızın ağ bağlantısını otomatik olarak kurabilen ve sürdürebilen, yönlendirme/anahtarlama yaparak çoklu atlama (multihop) özellikleriyle Kablosuz Örgü Ağları (Wireless Mesh Network) için esnek ve ölçeklenebilir bir mimarinin katman 2 özelliklerini içermektedir. Bu özellikler düşük maliyet, kolay ağ bakımı, gürbüzlük ve güvenilir hizmet kapsamı gibi önemli avantajlar sunmaktadır; böylelikle kablosuz teknolojilerin bağlantı katmanı yeteneklerine önemli ölçüde katkı sağlamaktadır [4].

Kablosuz teknolojilerle paralel olarak yeteneklerini arttıran ağ teknolojileri, neredeyse dünyadaki tüm ağ noktalarının birbirleriyle iletişim kurabileceği kompakt bir ağ modeline sahiptir. Bu kompakt ağ modeli, siber saldırıların neden olacağı potansiyel hasarı gün geçtikçe daha yıkıcı ve tolere etmesi zor hale getirmektedir. Kablosuz ağların dünya internet trafiğin önemli bir kısmını taşıdığı düşünülünce, Kablosuz Ağlarda siber güvenliğin önemi iyice artmaktadır. Temel servis setinin ve 802.11s Kablosuz Örgü Ağlarının önemli düzeyde avantajları olsa da, özellikle radyo iletişiminin çoklu yayın yapısını manipüle eden siber saldırılara da eğilimlidirler. Bu

tür saldırıların neden olacağı potansiyel hasarın, Kablosuz ağ teknolojilerinin yaygınlaşmasıyla önemli ölçüde artmasını beklemek mantıklıdır. Literatürde 802.11 saldırıları ve saldırı tespit sistemleriyle alakalı kapsamlı çalışmalar bulunmaktadır [5] [6] [7]. Bu çalışmaların teorik altyapısının yanı sıra, eğitim ve test amaçlı çok sayıda açık kaynak kodlu araç ve yazılımla desteklenen çalışmalar da bulunmaktadır [8]. Ancak yapılan çalışmaların derlenmesi sonucunda Temel Servis Seti mimarisinde uçtan uca Kablosuz Ağ Tespit Sisteminin, 802.11s ile uyumlu Kablosuz Örgü Ağlarında ise atak uygulamalarının gelişime açık alanlar olduğu görülmüştür. Bu nedenle tezin amacı, literatürde bahsedilen gelişme açık alanlara katkıda bulunmaktır.

Anlatılan bilgiler ışığında tez çalışması iki ana bölüme ayrılmıştır. İlk bölümde Temel Servis Seti ağ mimarisinde çalışan bir Kablosuz Saldırı Tespit Sistemi gerçeklenmektedir. Açık veri seti üzerinde popüler makine öğrenmesi metotlarından Decision Tree Classifier, Naive Bayes, Logistic Regression, Random Forest ve Sinir Ağlarıyla (Neural Networks) elde edilen modellerin jenerik bir donanım üzerinde konumlandırılmasıyla tasarlanan gömülü mimaride, modüler yapıda bir Kablosuz Saldırı Tespit Sistemi oluşturulmuştur. Efektif ve uygulaması görece daha kolay Ağ Bağlantısını Kesme (Deauthentication) saldırısı ile denenen sistemin uçtan uca çözüm yapısı ve sonuçları gösterilmektedir.

Tezin ikinci bölümü ise 802.11s Kablosuz Örgü Ağlarına yönelik atak gerçeklemelerini konu almaktadır. 802.11s ağlarına ve 802.11s varsayılan yönlendirme protokolü olan HWMP'ye (Hybrid Wireless Mesh Protocol) dair temel bilgiler ışığında benzer çalışmalara dair araştırmalar yapılmıştır. Sonrasında 802.11s Kablosuz Örgü Ağlarında Örgü Değiş-Tokuş Yönetimi (Mesh Peering Management) sürecinin ve HWMP temel prensipleri kullanılarak Sahte Kimlik Doğrulama (Fake Mesh Authentication), Yol Saptırma (Path Diversion) ve Karadelik (Blackhole) saldırıları özelinde geliştirilmiş saldırı yazılım mimarisi ile gerçeklenmiş, sonuçlar gösterilmiştir.

Tezin sonuç bölümü, her iki bölümde anlatılanların ışığında ana gözlemler ve son açıklamalar ile sona ermektedir. Bunlara ek olarak tezin temel oluşturduğu gelecekte yapılması planlanan çalışmalar için de bilgilere yer verilmiştir.

2. MAKİNE ÖĞRENMESİ YAKLAŞIMLARI İLE 802.11 KABLOSUZ SALDIRI TESPİTİ

Bu bölüm tezin ilk kısmını oluşturan 802.11ac uyumlu Temel Servis Seti kablosuz ağ mimarisinde makine öğrenmesi metotları kullanılarak oluşturulan modellerin, donanım üzerinde gerçeklenerek Ağ Bağlantısını Kesme saldırısının tespit sistemi hakkındaki çalışmaları içermektedir. İlgili bölümü sırasıyla Arkaplan, Benzer Çalışmaların İncelenmesi, Saldırı Tespit Sistemi, Deney Düzeneği ve Saldırı Gerçeklemeleri ve Sonuçları bölümleri takip etmektedir.

2.1 ARKAPLAN

Bu kısımda, tezin ilk aşamasında yapılan çalışmaların arkasındaki konseptlere ve bu konseptlerin altındaki kırılımlara ilişkin öne çıkan tanımlamalar yer almaktadır. Bu konseptlerin ilkini, tezdeki kablosuz gerçekleme ortamını oluşturan ana protokol olan ve yardımcı kablosuz teknolojilerin yaygınlaşmasını selef standartlara göre sunduğu önemli ölçüdeki veri hızlarıyla sağlayan IEEE 802.11ac'dir [9]. Anlatım sonrasında ise 802.11 Temel Servis Seti, Güvenliği ve Saldırılarıyla devam etmektedir.

2.1.1 IEEE 802.11ac

IEEE tarafından geliştirilen 802.11 WLAN (Kablosuz Yerel Alan Ağı) standardı, çoğunlukla 2,4 ve 5 GHz lisanssız frekans bantlarında yerel alan ağında kablosuz iletişim için kullanılmaktadır. IEEE 802.11ac, 5 GHz bandı için teorik olarak 7 Gbit/s fiziksel katman veri hızlarını aşabilen, gelişmekte olan çok yüksek verimli bir Kablosuz Yerel Alan Ağı standardıdır [3]. Elde edilen veri hızlarının arkasında, Fiziksel Katman ve Veri Katmanı Özellikleri başlıkları altında 802.11ac standardının temelini oluşturan özellikler anlatılmıştır.

Fiziksel Katman Özellikleri

802.11ac'nin OSI (Open System Interconnection) modelinde [10] bulunan ilk katman olan fiziksel katmandaki temel özellikleri aşağıda sıralanmıştır.

RF Kanal Bant Genişliği

802.11ac standardındaki önemli gelişmelerden biri, daha geniş bir RF kanal bant genişliği kullanmaktır. Daha geniş kanallar, genişlikleriyle orantılı olarak daha yüksek veri hızları sağlayabilmektedir. 802.11ac'nin öncülü olan 802.11n teknolojisinde 40 MHz olarak kullanılan kanal genişlikleri, 80 MHz ve 160 MHz'e genişletilmiştir. 80 MHz kanallar iki bitişik 40 MHz kanal, 160 MHz kanallar ise iki 80 MHz kanalın birleşimi olarak tanımlanmaktadır [11].

Uzaysal Yayılım

Uzaysal yayılım, bağımsız akışları aynı anda tek veya çoklu alıcılara iletmek için kullanılan Çoklu Giriş Çoklu Çıkış (Multiple Input Multiple Output - MIMO) protokolünün temelini oluşturmaktadır. Bu ilke sayesinde 2x2, 3x3, 4x4 gibi uzamsal akışların miktarı sırasıyla katlanabilmektedir. 802.11n standardında tanımlanan dört uzaysal yayılım, 802.11ac standardında sekiz uzaysal yayılıma ulaşmaktadır [3] [11]. Bugün 802.11ac destekli donanımlar 4x4'e kadar uzaysal yayılımı destekleyebilecek seviyeye erişmiştir. Erişim Noktaları ve terminal konfigürasyonları, çip, ekipman maliyetleri, fiziksel boyut ve güç kısıtlamaları nedeniyle farklılaşmaktadır. Erişim noktaları anten sayılarını arttırarak büyümekte, terminaller ise daha az sayıda antenin arkasında birden fazla uzaysal yayılım ve hüzmeleme özellikleri uygulayarak daha yetenekli hale gelmektedir. Bu farklılık, yüksek kapasiteli bir erişim noktasının birden çok, daha düşük verimli kullanıcıya aynı anda iletişim kurabileceği Çok Kullanıcılı MIMO için fırsatlar yaratmaktadır.

Çok Kullanıcılı MIMO (MU-MIMO)

802.11n standardıyla uyumlu bir radyo modülü, aynı anda birden fazla uzaysal yayılımı iletebilmekte ancak yalnızca tek bir adrese veya yayına yönlendirebilmektedir. Bireysel olarak adreslenen çerçeveler için bu durum, tek

seferde yalnızca tek bir cihazın (veya kullanıcının) veri aldığı anlamına gelmektedir. Buna Tek Kullanıcılı MIMO (Single User-MIMO) denmektedir. 802.11ac standardının yayınlanmasıyla birlikte, çok kullanıcılı MIMO (Multi User-MIMO) adı verilen yeni bir teknoloji tanımlanmıştır. Bu yeni özellik, bir erişim noktasının aynı anda birden fazla hedef kullanıcıya farklı akışlar iletmesine olanak tanımakta ve Erişim Noktasının anten kaynaklarını farklı istemcilere aynı anda ve aynı frekans spektrumu üzerinden birden fazla çerçeve iletmek için kullanabilmektedir [11].

Modülasyon ve Kodlama

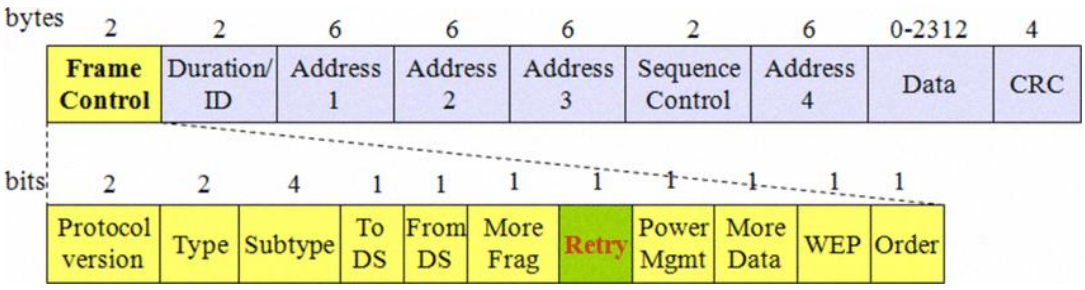
802.11ac standardında yapılan son değişikliklerle beraber, sinyal işleme kabiliyetini artırmayı amaçlayan daha verimli yarı iletken radyo tasarımındaki yeni teknolojiler modülasyon ve kodlama tekniklerinin sınırları genişletmiştir. 64 QAM (Quadrature Amplitude Modulation) tekniğinden 256 QAM'a sıçrayarak, Modülasyon ve Kodlama şemasında 8 ve 9'uncu seviyelerle karşılık gelen 3/4 ve 5/6 kod oranları eklenmiştir. 20 MHz kanalında akış, önceki en yüksek 802.11n veri hızı olan 65 Mbit/s'den sırasıyla 78 Mbit/s ve 86.7 Mbit/s'e çıkmış, bu sayede sırasıyla %20 ve %33'lük bir iyileştirme sağlamıştır [11].

Veri Bağlantı Katmanı Özellikleri

802.11ac'nin OSI katmanında [10] bulunan ikinci katman olan veri bağlantı katmandaki geliştirmeler aşağıda sıralanmıştır.

802.11ac Çerçeve Formatı

802.11ac çerçeve formatı Şekil 2.1'de gösterilmiştir.



Şekil 2.1: 802.11ac Çerçeve Yapısı

Şekilde görüldüğü gibi 802.11ac çerçeve yapısındaki ToDS ve FromDs alanları yardımıyla adres alanlarının işlevleri belirlenirken, Kablosuz Yerel Alan Ağındaki istemciler ile Erişim Noktaları arasında bağlantı ve veri aktarımı için dört adresli çerçeve mekanizması kurulmaktadır.

Çerçeve Yığınlanması

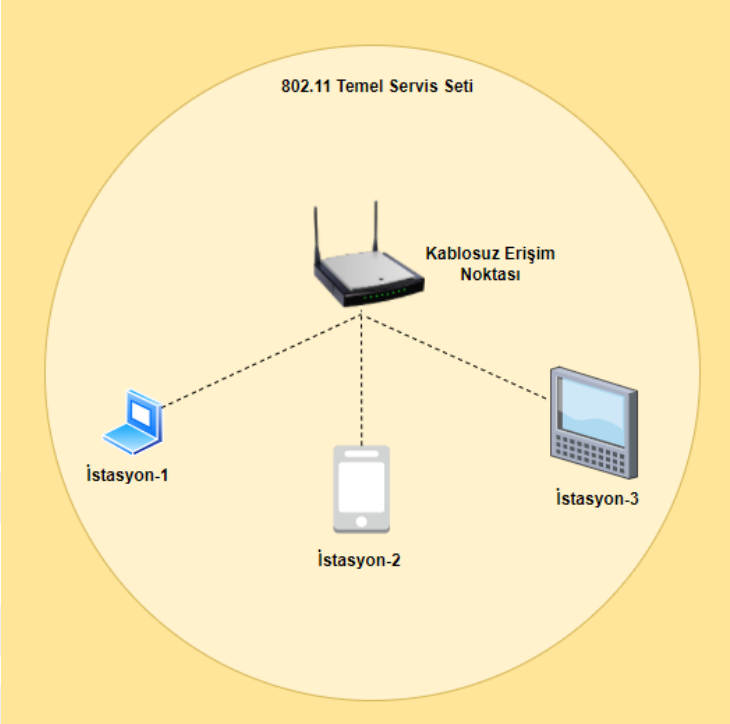
Çerçeve yığınlaması, kablosuz teknolojilerde birden çok çerçevenin bir iletim döngüsü sırasında çoklanarak gönderilmesini prensibine bağlı veri hızı arttırıcı bir mekanizmadır. A-MSDU (Aggregate MAC Service Data Unit) ve A-MPDU (Aggregate MAC Protocol Data Unit) olmak üzere ikiye ayrılmaktadır. 802.11ac standardıyla beraber A-MPDU mekanizması kullanılmaya başlamıştır. A-MPDU toplama kavramı, çoklu MPDU alt çerçevelerini tek bir önde gelen fiziksel katman başlığıyla birleştirme temellidir. A-MSDU yığınlamasına göre önemli bir farkı, A-MPDU'nun katman 2 başlık kapsüllenmemesinin ardından işlem görmesidir. Bu yöntem, A-MSDU'ya kıyasla daha yüksek katman 2 veri hızları sunmaktadır [12].

Dinamik Bantgenişliği Operasyonları

Kablosuz teknoloji gelişimiyle beraber terminaller ve Erişim Noktaları sayısı önemli ölçüde artmaktadır. Bu artış kablosuz ağ kullanımı da bir o kadar arttırmaktadır. Birden fazla kullanıcının aynı kanal ve bant genişliklerinde iletim ve dinleme zamanlarında birbirlerine en az şekilde girişim yapabilmeleri amacıyla, gelişmiş Request to Sent (RTS), Clear To Sent (CTS) mekanizması bulunmaktadır. Tüm Wi-Fi alıcı-vericileri akıllı bir şekilde bu çerçeve tiplerini ilgili ağa göndererek ve işleyerek doğru iletim zamanını öğrenip çerçeve çarpışmasını en aza indirecek şekilde iletimine devam etmeyi hedeflemektedir [12].

2.1.2 802.11 Temel Servis Seti

Kablosuz ağlarda bir Yerel Alan Ağı kapsamında, Erişim Noktası ve ona bağlı istasyonların oluşturduğu ağ mimarilerini tanımlamaktadır. Temel Servis Seti mimarisinin kapsama alanı içerisinde, terminaller/istasyonlar ile Erişim Noktaları arasında iletişim sağlanabilirken, Erişim Noktası terminaller arası yönlendirme sağlayarak terminaller arası bağlantıyı da mümkün kılabilmektedir. İstasyonlar, erişim noktalarının yayınladığı SSID’lere (Service Set Identifier), kablosuz şifreleme metoduna göre, ağ şifre işlemleri sonrası bağlantı kurabilmektedir.



Şekil 2.2: 802.11 Temel Servis Seti Ağ Topolojisi Örneği

2.1.3 802.11 Temel Servis Seti Erişim Güvenliği

Kablosuz teknolojilerin tarihsel gelişimi sürecinde, kablosuz ağ güvenliği gereği şifreleme protokolleri geliştirilmiştir; bunlar WEP (Wired Equivalent Privacy, WPA (Wi-Fi Protected Access), WPA2 (Wi-Fi Protected Access-2)'dir. 2009 yılından itibaren kablosuz ağ güvenliğinde WPA-2 standardı 802.11ac standardının yayınlandığı sıradaki en güvenilir standart olarak Temel Servis Seti mimarisinde yer almaya başlamıştır. Böylelikle 802.11ac uyumlu kablosuz ağlar WPA-2 ile korunmaktadır. WEP ve WPA'ya yönelik detaylı bilgiler çalışma [13]'den edinilebilmektedir. 802.11ac standardı WPA2 şifreleme protokolü ile korunması nedeniyle detaylarına yer verilmiştir.

WPA-2'nin temeli IEEE 802.1x [14] standardına dayanmaktadır. WPA-2 Personal ve WPA-2 Enterprise olarak ikiye ayrılmaktadır. WPA-2 Personal, Temel Servis Seti içerisinde bulunan istasyonların, bir ağ şifresi vasıtası ile ağa giriş yapmasını

sağlamaktadır. Şifreleme yöntemi için AES (Advanced Encryption Standard) ve CCMP (Counter Mode Cipher Block Chainig Message Authetication Code Protocol) algoritmalarını desteklemektedir. WPA-2 Enterprise'da ise kimlik doğrulaması için bir RADIUS (Remote Authentication Dial-In User Service) sunucusu ve EAP (Extensible Authentication Protocol) protokolü kullanılmaktadır. Kullanıcılar, kullanıcı adı ve parola dahil olmak üzere kimlik doğrulama bilgileri sağlamakta ve kimlik doğrulama sunucusu tarafından doğrulanmaktadır.

2.1.4 802.11 Temel Servis Setine Yönelik Saldırılar

802.11 Temel Servis Seti için tanımlanmış çok sayıda saldırı bulunmaktadır. Bu saldırıların öne çıkanlarından olan fiziksel katman ve veri iletim katmanında ayrı ayrı tanımlı DoS (Denial of Service) servis dışı bırakma saldırılarına ek olarak, sadece veri iletim katmanı özelinde tanımlı Key Retreiving, Key Stream Retreiving, Availability ve Man-in-the-Middle saldırılarıdır. Bu saldırılar, tasnif edilip alt kırılımlara ayrıldığında 30'dan fazla saldırı tipi olduğu görülmektedir. Bu tez çalışmasının ana çerçevesinin 802.11 Temel Servis Setine yönelik tüm saldırıları kapsamaması nedeniyle, bu saldırılara dair önemli ölçüdeki detaylara [7] ve [15] çalışmalarından erişilebilmektedir.

Bütün bu sınıflandırmaların içerisinde verimliliği ve kolay uygulanabilirliği bakımında en popüler ve etkili olarak kabul edilen saldırı, "flooding" kategorisi altında bulunan Ağ Bağlantısını Kesme (deauthentication) saldırısıdır [5]. Flooding saldırıları, saldırı yapılacak ağa karşı çok yüksek sayılarda trafik uygulayarak ağı servis dışı bırakma temelli saldırı kategorisidir. Ağ Bağlantısını Kesme, saldırganın öncelikle saldırı yapmak istediği ağ bileşenlerinin bilgilerini elde etmesi (Erişim Noktası ve bağlı istasyon MAC adresleri) ve bu bilgileri kullanarak hedef Erişim Noktasına, ağdaki istasyonları taklit etmek suratiyle sahte "deauthetication çerçeveleri" göndermesini ve Erişim Noktasının bu çerçeveleri işleyip, taklit edilen istasyonları ağdan düşürmesini amaçlayan saldırıdır.

2.2 BENZER ÇALIŞMALARIN İNCELENMESİ

Literatürde 802.11 kablosuz teknolojilere yönelik oluşturulmuş Saldırı Tespit Sistemlerine dair çok sayıda çalışma bulunmaktadır. Bu çalışmaların önemli bir kısmı incelenmiş, öne çıkan araştırmalar tezin ilk kısmı için hazırlanan yol haritasının temelini oluşturmuştur.

Göze çarpan önemli çalışmaların başında Kolias ve diğerlerinin yaptığı çalışma gelmektedir [15]. Çalışmada 802.11 ağlarına karşı literatürde tanımlı çok sayıda saldırıyı konu almıştır. Bu saldırıları analiz etmeden önce 802.11 mimarisindeki çerçeve tiplerinden ve çerçeve yapısından bahsetmiştir. Kablosuz ağ koruma metotlarından olan WEP, WPA, WPA2 özelindeki saldırı tiplerini açıklamıştır. Key Retrieving, Key Stream Retrieving, Availability ve Man-in-the-Middle başlıkları tanımladığı saldırıların tümünü 802.11n deney ortamında gerçeklemiştir. Gerçeklediği tüm saldırıların imza analizini çıkarmış ve sonuçlarını göstermiştir. Literatüre olan diğer önemli katkısı ise, saldırı kategorilerine uygun olarak gerçeklediği tüm saldırıları bir veri seti halinde açık olarak sunması olmuştur. AWID (Aegean Wi-Fi Intrusion Dataset) adı verilen bu veri seti, kablosuz saldırı tespit için kullanılacak veri setleri içerisinde en popüler olanıdır.

Kolias ve diğerlerinin çalışmasının açtığı yol ile beraber, saldırı tespit sistemi oluşturma amacını takip eden çok sayıda çalışma literatüre sunulmuştur. Çalışma [6] ve [16], AWID veri seti üzerinde yoğunlaştığı Derin Öğrenme uygulamalarıyla kablosuz ağlar üzerinde anomali tespitine dair modeller geliştirmiştir. Derin öğrenmenin çok sayıda temel prensibini kullanarak başarım kriterleri sunmuştur.

Bu çalışmalar sonucunda Saldırı Tespit Sistemlerindeki yanlış alarm üretme oranlarının yüksek olması, ilgili çalışmaların en önemli zorluklarından biri olarak görülmüştür. Yüksek yanlış alarm oranlarını düşürmek için çalışma [17]'de ve çalışma [18]'de farklı modeller öne sürülerek, eğitilen veri seti üzerinde geliştirilmiş optimizasyon parametreleri ve algoritmalar kullanılmasıyla başarım kriterleri arttırılmıştır.

Makine öğrenmesi algoritmalarına ek olarak, derin öğrenme yöntemlerinde de katkı veren geliştirmeler yapılmış çalışmalar mevcuttur. Çalışma [19] ve [20] veri seti içerisindeki farklı özellikleri eğiterek ve farklı mekanizmalar kullanarak derin öğrenme metotlarına katkı sağlayan modeller yaratabilmiş ve başarım oranları iyileştirilmiştir.

Bu çalışmaların analizi sonrasında görülmüştür ki; kablosuz ağlarda saldırı tespit sistemlerine dair uygulamalar oldukça yaygındır. Bu uygulamaların temelini de sayısı oldukça fazla olan makine öğrenmesi ve derin öğrenme metotları oluşturmaktadır. Tüm çalışmaların sonucunda, ilk olarak literatürde 802.11ac temelli kablosuz ağlarda saldırı gerçeklemelerinin 802.11n'deki kadar yaygın olmadığı kanaatine varılmıştır. Sonrasında ise makine öğrenmesi ve derin öğrenme metotlarıyla oluşturulan modellerin bir donanım platformu üzerinde koşacak şekilde gerçeklenip, gerçek bir deney ortamında oluşturulmuş saldırı tipleriyle test edilip, uçtan uca bir Kablosuz Saldırı Tespit Sisteminin sunulması konusunda gelişime açık olduğu görülmüştür.

Bu nedenle bu tezde, 802.11 ağlarında oldukça popüler saldırı tipi olan ağdan düşürme saldırısının 802.11ac tabanlı kablosuz ağlarda gerçeklenip, açık veri seti üzerinden oluşturulacak makine öğrenmesi ve derin öğrenme modellerinin bir donanım üzerine aktarılıp, uçtan uca bir gömülü mimarisi gerçeklenmesi hedeflenmiştir.

2.3 KABLOSUZ SALDIRI TESPİT SİSTEM MİMARİSİ

Bu bölümde 802.11ac test ortamında, kablosuz ağlara yönelik saldırı tespiti yapabilecek bir çözüm mimarisi oluşturulmuştur.

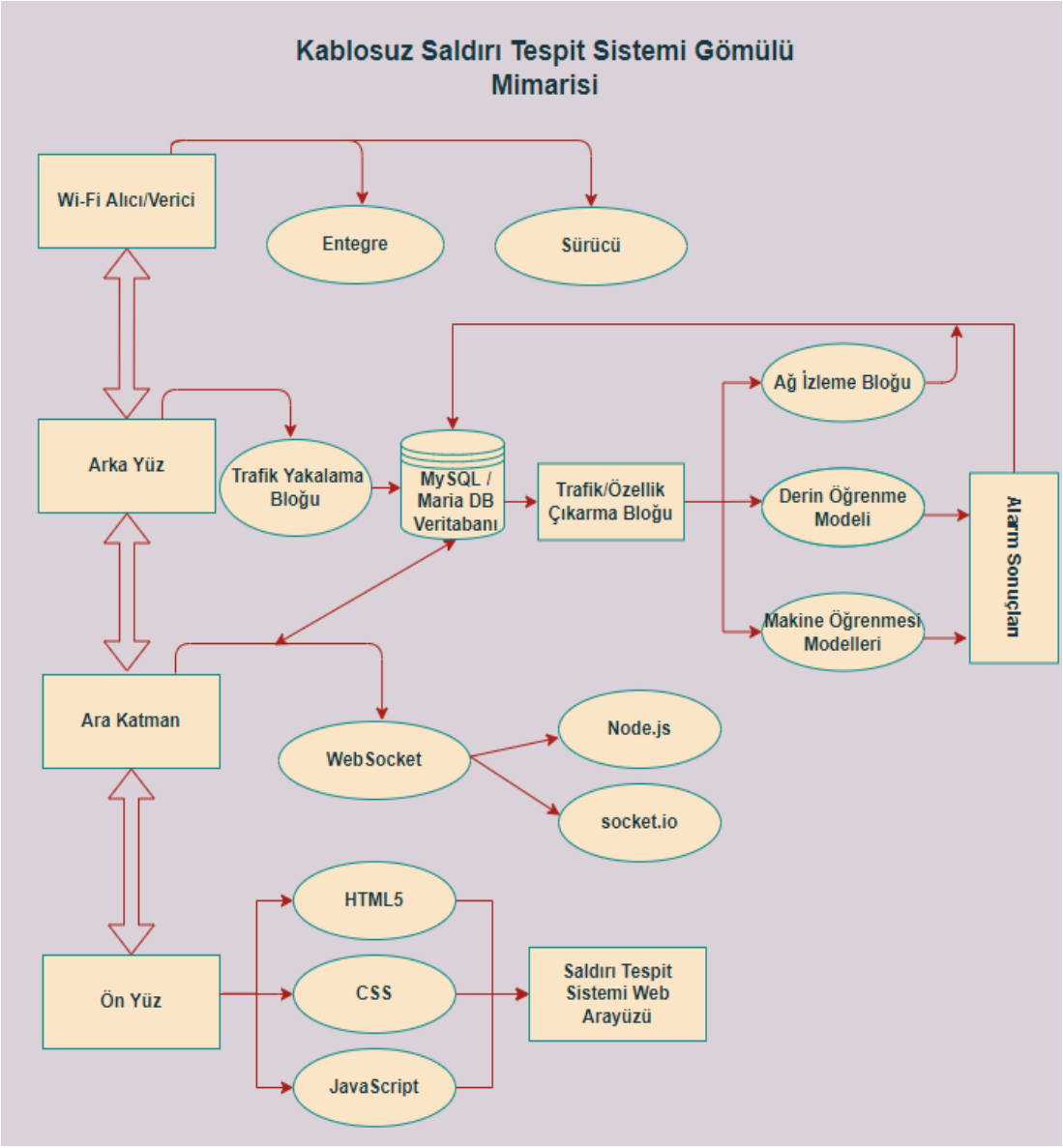
2.3.1 Kablosuz Saldırı Tespit Sistemi Bileşenleri

Bu bölümde tasarlanan Kablosuz Saldırı Tespit Sistemini oluşturan bileşenlerin detayları modüler olarak anlatılmaktadır.

Başlangıçta, 802.11ac kablosuz test ortamında Erişim Noktası ile kendisine bağlı terminallerin/istasyonların oluşturduğu Temel Servis Seti mimarisinde tanımlı saldırı gerçeklemeleri temel alınarak uçtan uca saldırı tespit çözüm mimarisi oluşturulması hedeflenmiştir.

Hedef kapsamında, saldırı önleme mekanizmaları için Makine Öğrenmesi algoritmaları ve içine aldığı alt küme olan Derin Öğrenme yöntemleri sonucu oluşturulan Sinir Ağları modelleri kullanılmıştır. Oluşturulan modellerin, saldırı tespit sisteminin üzerinde koşacağı donanıma aktarılıp ve gömülü sistem mimarisi içerisine konumlandırılmıştır.

Bu bilgiler ışığında, üzerinde çalışılan Kablosuz Saldırı Tespit Sistemi dört temel bileşenden oluşmaktadır. Bu bileşenler; Wi-Fi Alıcı/Verici, Arka Yüz (Backend), Ara Katman (Middleware) ve Ön Yüz (Frontend) olarak isimlendirilmektedir. Bahsedilen dört temel bileşenin birbirleriyle uyumlu şekilde bir bütün olarak çalışacağı platform için, piyasada rafta hazır ürün olarak bulunabilen jenerik donanım üzerinde gömülü bir sistem mimarisi oluşturulmuştur. Bu gömülü mimarinin amacı, yapı içerisinde bulunan tüm bileşenlerin birbiriyle uyumlu ve verimli bir şekilde entegre halde çalışmasıdır. Şekil 2.3'te Kablosuz Saldırı Tespit Sisteminin temelini oluşturan Gömülü Sistem Mimarisi gösterilmiştir.



Şekil 2.3: Bu Çalışmada Gerçeklenen Saldırı Tespit Sisteminin Temelini Oluşturan Gömülü Sistem Mimarisi

Saldırı tespit sistemin ilk bloğunu, Wi-Fi alıcı-vericisi oluşturmaktadır. Çalışma kapsamında 802.11ac kablosuz ortamının kullanılması hedeflendiği için, kablosuz alıcı verici bloğunun temelindeki donanım, 802.11ac ile uyumlu ve uygun sürücü yazılımı ile sürülebilecek şekilde konumlandırılmıştır.

Wi-Fi alıcı-vericisinin temel görevi çalışma kapsamında üzerinde analiz yapılacak çerçeveleri olabildiğince hatasız ve eksiksiz yakalayabilmesidir. Üzerinde analiz ve çalışma yapılacak çerçeveler, ağda kendi ağ arayüz kartına (network interface card) adreslenmeyeceği için ilgili çerçevelerin doğru yönetilebilmesi için operasyon frekans

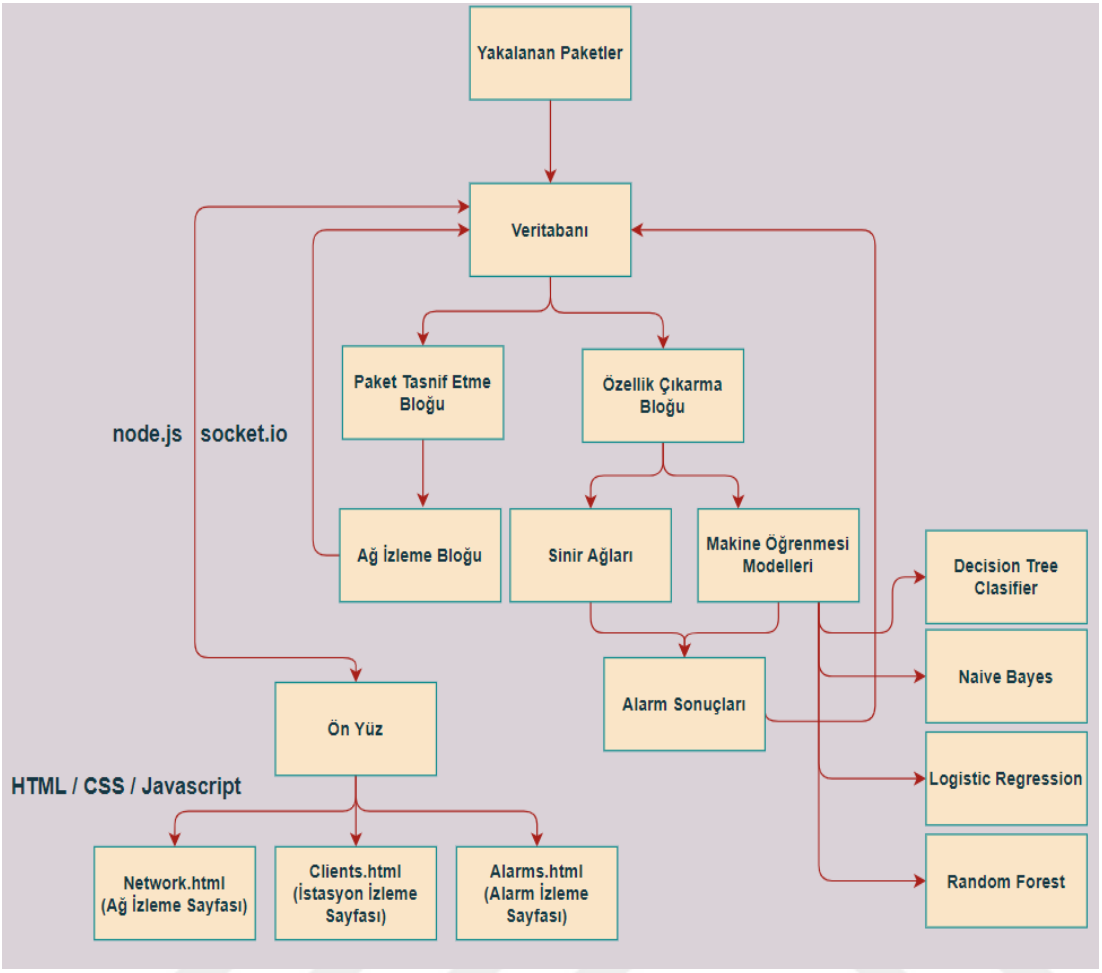
bandında monitor modda[1] çalışmaktadır. Böylelikle ortamdaki tüm kablosuz trafiğin izlenmesi amaçlanmaktadır.

Bir diğer kısım sistemin Arka Yüzünü içermektedir. Arka yüz bloğu, saldırı tespiti yapan makine öğrenmesi / sinir ağları modellerini, paketleri işleyebilecek, yorumlayabilecek, makine öğrenmesi tespit modellerine girdi sağlayabilecek tasnif işlemlerini yapabilecek paket işleme blokları ve paketleri operasyonunun merkezinde bulunacak veri tabanını içermektedir. Ayrıca kullanıcıya sunulacak arayüz için ağın monitör edilmesini sağlayan yapının uygulaması için ise ayrı bir blok bulunmaktadır.

Sistemin ön yüzünde ise, kullanıcılara sunulacak ağ monitör uygulaması ve tespit sisteminin izlenebileceği/yönetilebileceği bir arayüz gerçeklenmiştir. Ara katman sayesinde ise arka yüz ve ön yüz arasında bilgi alışverişi soket programlama mimarisinin sağladığı paralel ve çift yönlü aktarım yapısı olacak şekilde kurgulanmıştır. Bu yapının kullanılması, katmanlar arası veri aktarım hızını akabinde de sistemin cevap süresini hızlandırması amaçlanarak tasarlanmıştır.

Arka yüz, ön yüz ve ara katmanı içeren gömülü sistem mimarisinin detayları Şekil 2.4'te gösterilmiştir.

[1] Monitör mod, bir kablosuz ağ arayüz kartının bulunduğu ağdaki tüm trafiği ilgili ağa dahil olmadan izleyebilmeye olanak sağlayan moddur.



Şekil 2.4: Bu Çalışmada Gerçeklenen Saldırı Tespit Sisteminin Arka Yüz – Ara Katman ve Ön Yüzünü İçeren Bloklar

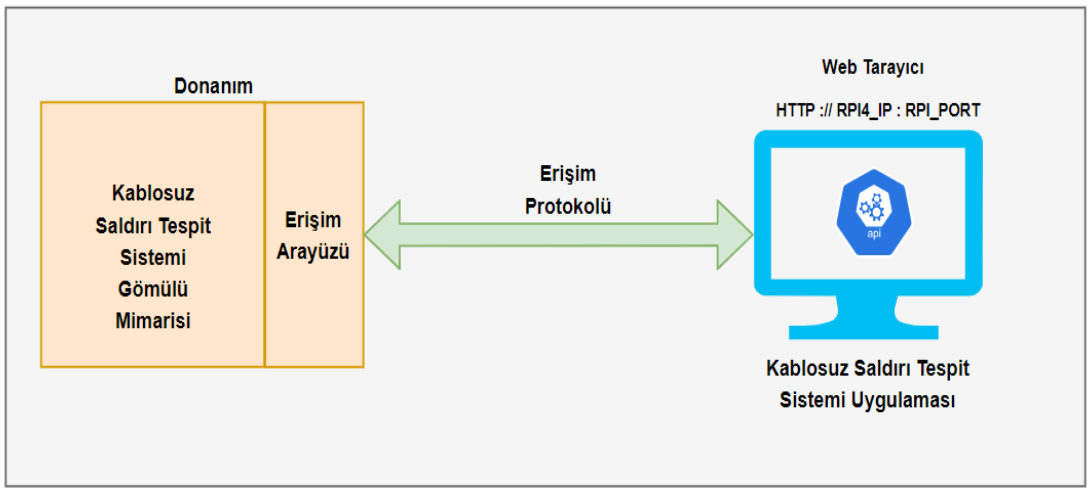
Wi-Fi alıcı/vericisi sayesinde yakalanan ağ trafiği, ilk olarak veri tabanına yazılmaktadır. Veri tabanına yazılan veriler, Paket Tasnif Etme bloğu vasıtasıyla, yakalanan trafiğin belirli alanları analiz edilerek ağ izleme arayüzü için bilgi kaynağı sağlanmakta ve veri tabanına tekrardan işlenmektedir.

Özellik çıkarma bloğu ise, saldırı tespiti için kullanılan Sinir Ağları ve Makine Öğrenmesi modellerine uygun fonksiyon girdisi sağlamak için tasarlanmıştır. Tüm modeller, sağlanan girdilerin ışığında bir sonuç üretmekte, üretilen sonuçlar veri tabanında tutulmaktadır.

Arka yüzde bulunan alt blokların veri tabanı ile etkileşimi oldukça, Ara Katman ilgili etkileşimlerin oluşturduğu güncel bilgiler, kullanıcı arayüzüne taşımaktadır.

Ön yüze taşınan bilgiler, oluşturulmuş WEB sayfa yapısı iskeletleri ve veri işleme motorlarıyla görsel bir arayüz olarak sunulmaktadır.

Tüm bu gerçeklemelerin ardından, uçtan uca Kablosuz Saldırı Tespit Sistemi gömülü mimarisi oluşturulmuştur. Kablosuz Saldırı Tespit Sisteminin servisi, sistem uygulamasının üzerinde koştuğu donanıma ağ üzerinden SSH [2] ya da Seri haberleşme arayüzü gibi erişim protokolleri vasıtasıyla erişilerek çalıştırılabilecek şekilde tasarlanmıştır.



Şekil 2.5: Bu Çalışmada Gerçeklenen Saldırı Tespit Sistemine Dış Ortamdan Bağlanılacak Topoloji

2.4 GERÇEKLEME DÜZENEĞİ

Bu kısım, tezin ilk aşamasını için yapılacak çalışmaların deneysel temelini oluşturan bileşenleri anlatmaktadır.

Wi-Fi Erişim Noktası

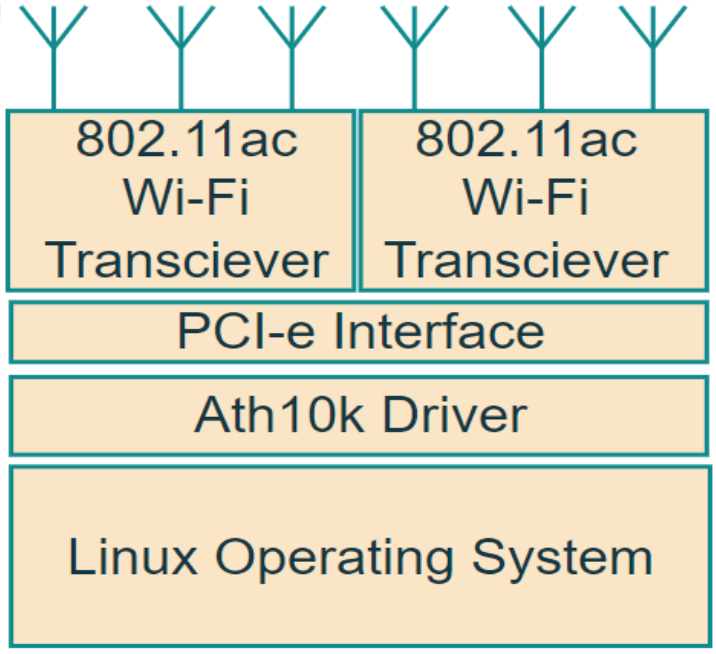
Tez çalışmaları içerisindeki tüm kablosuz operasyonları gerçekleştirecek Wi-Fi Erişim Noktası, bazı spesifik işlevleri gerçekleştirebilecek şekilde özel olarak tasarlanmış bir

[2] SSH (Secure Shell) uzak bir ağ cihazına bağlantı cihazına güvenli bağlantı yapmayı sağlayan protokoldür.

donanım bütünüdür. Bu kapsamda kullanılacak Wi-Fi Erişim Noktasının sahip olduğu temel özellikler aşağıda sıralanmıştır.

- Atheros QCA9880 işlemci tabanlı radyo modülü,
- 802.11b/g/n/ac standartlarına uyum,
- 5GHz bandında 1300Mbit/s fiziksel veri hızları,
- 3x3 MIMO ve OFDM Teknolojisi desteği,
- WPA-2 desteği
- 802.11s desteği

Wi-Fi Erişim Noktası olarak ayarlanan radyo modülü PCI-e arayüzü ile ana karta bağlanmaktadır ve tüm kablosuz aktiviteler Ath10k Linux Wi-Fi sürücüsü [21] kullanılarak Linux İşletim Sistemi tarafından kontrol edilmektedir. Ayrıca hata ayıklama (debug) arayüzünden ilgili işletim sistemine bağlanılabilmektedir. Wi-Fi Erişim Noktasının içinde bulunduğu donanım bütününün temel gömülü mimarisi Şekil 2.6'da gösterilmiştir.



Şekil 2.6 : Gerçekleme Düzeneğinde Kullanılan Wi-Fi Erişim Noktasının İçinde Bulunduğu Donanım Mimarisi

USB Wi-Fi Adaptörü

Çalışmada 802.11'e ait paketleri yönetmek kapsamıyla, paket dinleme ve ilgili ağa enjekte etmek için piyasada ticari bir ürün olarak yer alan ALFA marka AWUS036ACH model USB Wi-Fi Adaptör ürünü kullanılmıştır. Bu USB Wi-Fi Adaptörünün seçilmesinin nedeni, paket enjekte etme ve paket izleme konusunda oldukça yetenekli olması ve bu adaptöre yönelik çok sayıda açık kaynak sürücülerinin İnternet ortamında bulunmasının görece daha kolay olmasıdır. Ayrıca bu donanım, kablosuz test ortamının çalışma spektrumu olan 802.11ac standardını desteklemekte ve USB portu üzerinden bilgisayara bağlanmaktadır. Böylelikle bağlı olduğu bilgisayar üzerinde bir kablosuz arayüz oluşturmakta ve yönetilebilmektedir. Çalışma yapılacak kablosuz ağdan elde edilecek ya da enjekte edilecek tüm paketler USB Wi-Fi Adaptörü kullanılarak yapılacaktır.

Saldırgan Bilgisayarı

Saldırgan olarak tanımlanan bilgisayar, ağı manipüle etmek için saldırı komut dosyalarını içeren cihazdır. USB Wi-Fi Adaptör ile bağlantısı yapılarak donanımı yönetebilmekte ve saldırı betiklerini (script) USB Wi-Fi Adaptör üzerinden ilgili ağa enjekte edebilmektedir. Kali Linux [22], paket enjekte etme ve paket monitörleme için önerilen işletim sistemlerinden biridir. Bu nedenle, Saldırgan bilgisayarın 20.04 sürümlü Kali Linux (Kernel 5.10.0) işletim sistemi üzerinde çalışması tercih edilmiştir. Bu işletim sistemi, kablosuz adaptörlerin monitör modda yapılandırılıp, kullanım kolaylığı sağlarken, USB Wi-Fi adaptörünün donanım kısıtlamalarını ortadan kaldıran çeşitli açık kaynaklı sürücülerle uyumluluğu ile öne çıkmaktadır.

Raspberry Pi 4

Raspberry Pi 4, rafta hazır ürün olarak bulunan Single Board Computer tanımına giren bir donanımdır. İçerisine işletim sistemi kurulabilmektedir. Bu tezdeki gerçeklemede, sahip olduğu 802.11ac desteği ve CPU kapasitesinin paralel çalışması gereken uygulamalarla uyumlu olması sebebi ile seçilmiştir. Üzerindeki Wi-Fi entegresi sayesinde saldırı tespit sistemi özelindeki paket yakalama işlemleri bu donanım ile gerçekleştirilecek, oluşturulan gömülü mimari bir bütün halinde Raspberry Pi 4 üzerinde çalışacaktır.

Kablosuz Terminaller

Kablosuz terminaller deney ortamını oluşturan bir diğer bileşenlerdir. 802.11ac uyumlu telefon, tablet ve uygulamaya özel geliştirilen olarak geliştirilen cihazla beraber üç farklı terminal tipi deney düzeneğinde konumlandırılmıştır. Tez kapsamında yapılan saldırılara dair ağ trafiği ve bu bileşenlerin oluşturduğu topoloji üzerinden elde edilmektedir. Terminallerin kablosuz ağ arayüz kartı modülleri standarda uygun olarak tasarlandığı için, tespit veya saldırı sistemlerinde farklı sonuçlar vermemektedirler.

2.5 GERÇEKLEMELER VE ELDE EDİLEN SONUÇLAR

Bu bölüm Kablosuz Saldırı Tespit Sisteminin oluşturulması için gerçeklenen tüm aşamaları anlatmaktadır.

2.5.1 Tehdit Modelleme

Tehdit modelleme (Threat Modelling), bir sistemin güvenliğini tehdit edecek riskleri, ilgili risklerin kapsamını, potansiyelini ve bu risklerden korunma metotlarını belirlemek için uygulanan süreçtir [23]. Bu sürecin temel amacı, sistemdeki güvenlik risklerine dair kapsamlı bilgi edinmek ve bu bilgiler ışığında karar mekanizması işletebilmektedir. Aşağıda, Tehdit Modellemesi süreci kapsamında tez çalışmasının bu bölümü için genel bir açıklama yapılmıştır.

Bu bölümde 802.11 Temel Servis Seti mimarisinde bulunan Erişim Noktalarına, Kablosuz Saldırı Tespit Sistemi için girdi oluşturan ve detayları Bölüm 2.5.2'de anlatılan Ağ Bağlantısını Kesme saldırısı uygulanmaktadır. Başarılı saldırı sonrasında, ağdan bağlantısı kesilen terminallerin Erişim Noktasına tekrar kayıtlanması esnasında el sıkışma çerçevelerinin yakalanarak WPA2 ile korunan kablosuz ağın ağ şifresini elde etmek amaçlanmaktadır.

Başarılı saldırı sonucunda, saldırgan ağ şifresini elde ettiği için kendisini terminal olarak yapılandırarak ya da başka bir terminal kullanarak Erişim Noktasına kayıtlanabilmektedir. Bu durum tez çalışmasının bu bölümünü kapsayan, Erişim Noktası ve ona bağlı istasyonlar özelinde kurulan ağ topolojilerinde, saldırganın sadece ilgili yerel alan ağında bulunan Erişim Noktası ve bağlı terminalleri ile iletişim kurmasını ve veri iletimi yapmasını sağlayabilmektedir. Fakat Erişim Noktası, kablolu veya kablosuz arayüzleri vasıtasıyla diğer herhangi bir ağ ile doğru yapılandırma sonucu iletişim halinde ise (diğer yerel alan veya geniş alan ağları), saldırgan ağda bulunan diğer istasyonların erişebildiği her ağ noktasına erişebilmekte ve saldırı yüzeyini büyüterek tehdit potansiyelini arttırabilmektedir.

802.11 Temel Servis Setine yönelik Ağ Bağlantısını Kesme saldırıları için korunma yöntemleri, "yönetim" tipli çerçevelerin şifrelenmesi prensibine bağlı güvenlik standardı olan 802.11w'nün [24] ağda aktif edilmesi veya şu an en güncel şifreleme metodu olan WPA-3 (Wi-Fi Protected Access-3) [25] şifreleme metodunu destekleyen Erişim Noktaları ve terminaller ile ağ bileşenlerinin güncellenmesidir. Fakat günümüzde WPA-3 korumalı ağlarda da "Denial of Service" saldırılarına yönelik çalışmalar literatürde yer bulmaya başlamıştır [26].

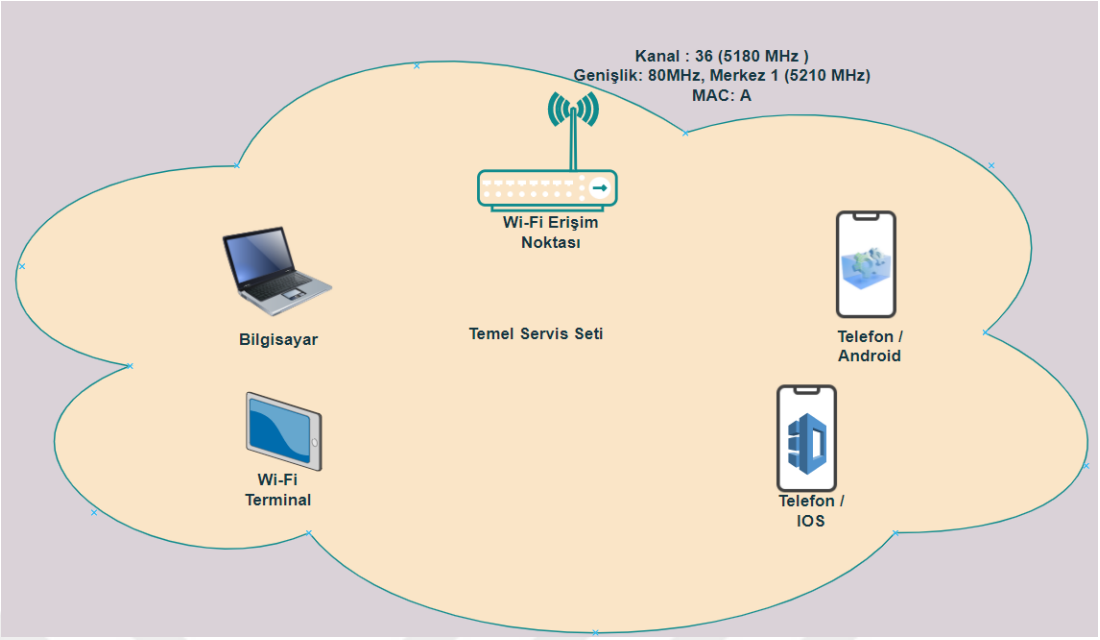
Ayrıca ağda Erişim Noktası ile entegre bir Kimlik Doğrulama Sunucusu (Authentication Server) konumlandırarak ağa erişim sağlayacak herhangi bir terminali yetkilendirilebilmek için kimlik bilgisi ve parola gibi bilgilerinin kullanıldığı bir güvenlik mekanizması kullanmak, 802.11 Temel Servis Seti saldırıları önlemek için kullanılan bir diğer yöntemdir [7].

2.5.2 Ağ Bağlantısını Kesme Saldırısı ve WPA2 Şifre Kırılması İşlemi

Bu bölüm ilk olarak Temel Servis Set'inde bulunan erişim noktasına bağlı terminallere Ağ Bağlantısını Kesme saldırısı yapılmasını anlatmaktadır. Temel Servis Seti mimarisine yönelik saldırılar için açık kaynak kodlu aircrack [27] saldırı yazılım aracından faydalanılmıştır ve bu saldırıları yapabilmek için Wi-Fi Erişim Noktası, Saldırgan Bilgisayar, USB Wi-Fi adaptör ve kablosuz terminaller kullanılmıştır.

Temel olarak, başarılı Ağ Bağlantısını Kesme saldırısı sonrası ağdan düşürülmesi istenen terminaller, saldırı bittiğinde Erişim Noktasına tekrardan bağlanma aşamasına geçtiklerinde, el sıkışma aşamasında yakalanan EAPOL (Extensible Authetication Protocol over LAN) çerçeveleri sayesinde ile WPA2 şifresinin kırılması hedeflenmektedir.

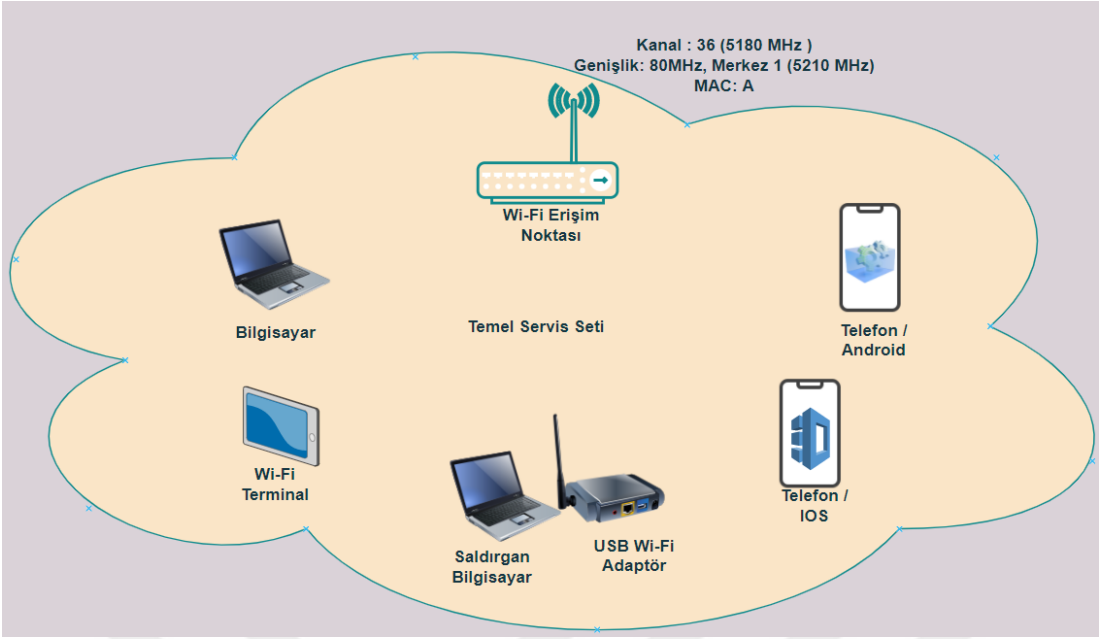
Deney ortamında öncelikli olarak 802.11 Temel Servis Set'i mimarisi oluşturmak için Şekil 2.7'de gösterilen topoloji kurulmuştur.



Şekil 2.7: Deney Ortamında Kurulan Temel Servis Seti Topolojisi

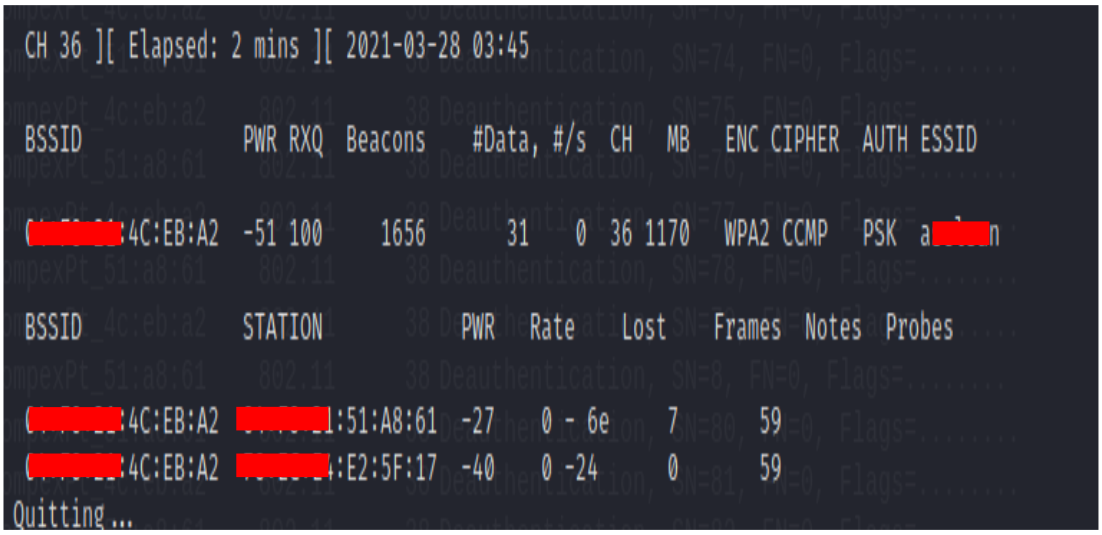
Wi-Fi Erişim Noktası 36. Kanala (Merkez Frekans 5180 MHz, Kanal Genişliği 80 MHz) ayarlanmıştır ve bir MAC adresine sahiptir. SSID ve şifre yapılandırmaları terminallere işlenmiş ve Temel Servis Seti mimarisi oluşturulmuştur. Wi-Fi Erişim noktası WPA-2 ile korunmaktadır ve her bir cihazın Erişim Noktası ve diğer terminallerle WPA-2 şifreleme metoduna göre bağlantı sağladığı görülmüştür.

Saldırı, saldırgan cihazın Şekil 2.8'deki gibi Temel Servis Seti'nin etki alanı içerisindeki herhangi bir noktadan ağa girmesiyle başlamaktadır. Saldırgan bilgisayar aracılığıyla, USB Wi-Fi adaptör monitör modda çalıştırılır ve ağı dinlemek üzere konumlanır.



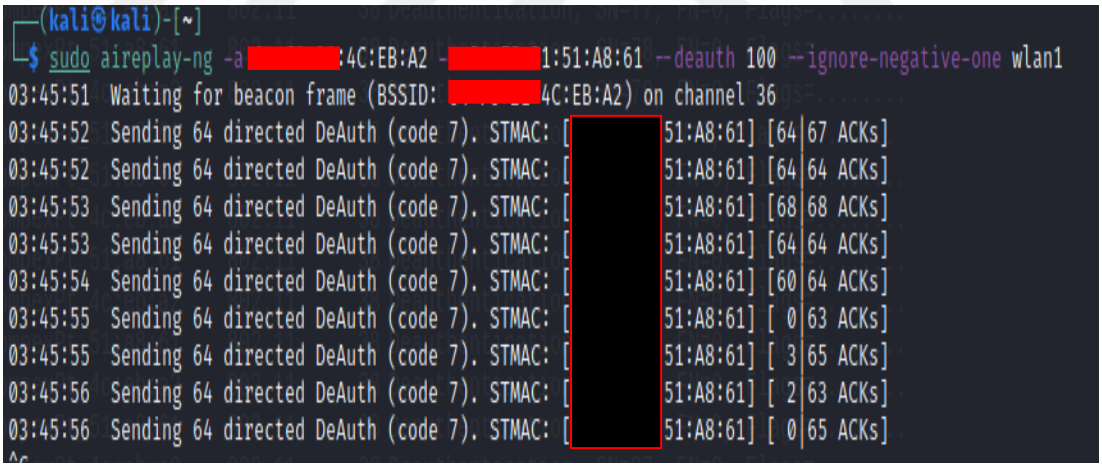
Şekil 2.8: Deney Ortamında Kurulan Temel Servis Seti Topolojisine Saldırgan Bilgisayarın Konumlanması

Kablosuz arayüz olarak USB Wi-Fi Adaptörün kullanıldığı Saldırgan bilgisayar üzerinden çalıştırılan "airmon-ng" aracı ile 802.11ac'nin kapsadığı 5 GHz frekans bandında kanallar arası ağ aktivitesi taranmaya başlanır ve aktivitenin olduğu frekans bandı tespit edilir. USB Wi-Fi adaptör aktivitenin tespit edildiğini frekans bandına uyumlanır (tune) ve ilgili frekansta bulunan Erişim Noktası ve Erişim Noktasına bağlı terminallere dair bilgileri elde eder. Bu bilgilerden önemli olanları, cihaz MAC adresleri ve kablosuz şifreleme yöntemidir.



Şekil 2.9 : Airmon-ng Aracı Kullanılarak Temel Servis Seti Ağ Taraması Sonucu Ağ Bilgilerinin Elde Edilmesi

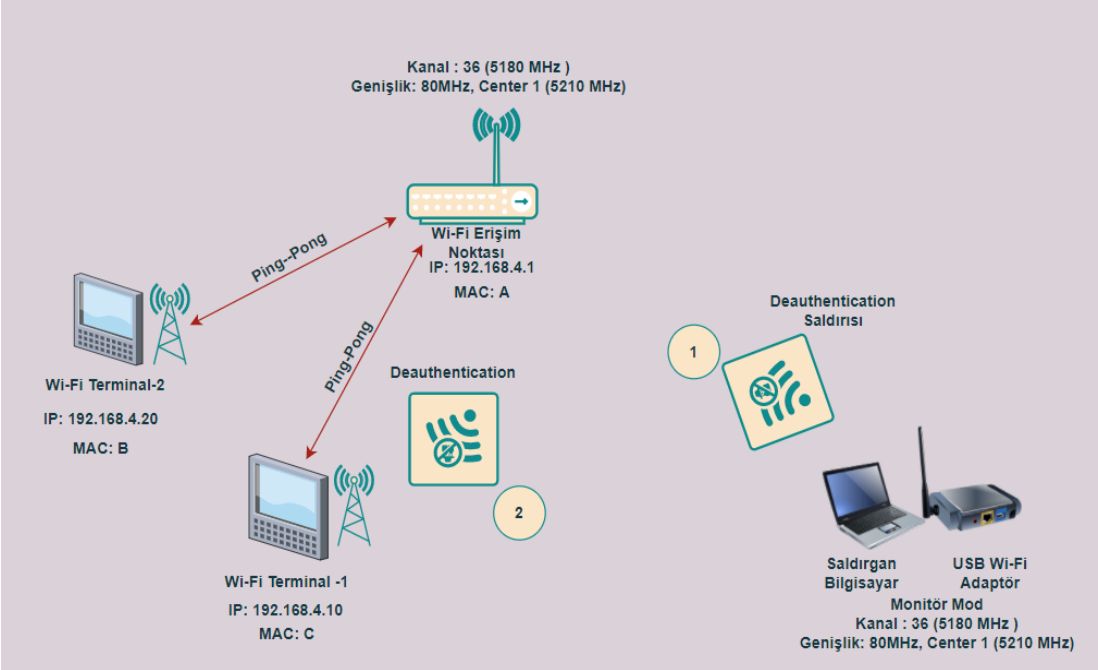
Erişim noktaları ve bağlı terminallerin MAC adreslerinin ve şifreleme yönteminin tespitinin ardında WPA-2 korumalı ağlar için kullanılan "aireplay-ng" aracı yardımıyla Ağ Bağlantısını Kesme saldırısı başlatılır.



Şekil 2.10: Aireplay-ng Aracı Kullanılarak Yapılan Ağ Bağlantısını Kesme Saldırısı Uygulama Çıktısı

Saldırının doğru yapılıp yapılamadığının onayı için kurulmuş olan örnek bir topoloji Şekil 2.11'de gösterilmiştir. Şekilde de görüldüğü üzere kablosuz terminaller, kablosuz cihazlar ile aynı alt ağda olacak şekilde IP adresleri yapılandırılmıştır. Sonrasında ise terminaller, bağlı oldukları Erişim Noktaları ile devamlı olarak

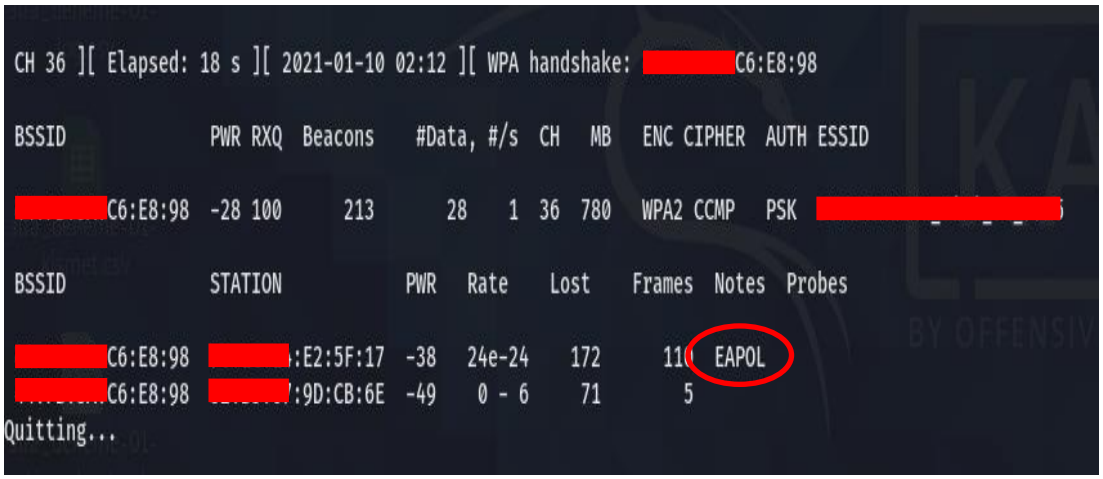
haberleştirilmektedir. Deney düzeneğindeki haberleşme Ping haberleşmesi ile sağlanmaktadır.



Şekil 2.11: Temel Servis Seti Topolojisinde Ağ Bağlantısını Kesme Saldırısının Yapılması

Wi-Fi Terminal-1'in MAC adresi taklit edilerek ve Wi-Fi Erişim Noktası-1'in MAC adresine yönelik yapılan Ağ Bağlantısını Kesme saldırısı sonrası, Wi-Fi Terminal-1'in Wi-Fi Erişim Noktası ile iletişiminin kesildiği görülmüştür. Ayrıca saldırıların Wi-Fi Terminal-2 ile Wi-Fi Erişim Noktasını arasındaki trafiği etkilemediği gözlemlenmiştir. Bu sonuç doğrudan Wi-Fi Erişim Noktasının Temel Servis Setinde anahtarlamaya dair olası bir servis dışı kalma durumundan ziyade, Wi-Fi Terminal-1'e yapılan Ağ Bağlantısını Kesme çerçevelerini işlediğini göstermektedir.

Saldırı sonlandırıldığında, Wi-Fi Terminal-1 tekrardan Wi-Fi Erişim Noktasına bağlanmaya çalışmaktadır (terminallerde otomatik bağlan seçeneği aktif). Bu sonucun ardından bağlanma sırasındaki el sıkışma anında EAPOL (Extensible Authetication Protocol over LAN) çerçevesinin yakalanması amaçlanmaktadır.



Şekil 2.12: Airmon-ng Aracı Kullanılarak EAPOL Çerçeve Yakalama Adımı

Şekil 2.12'de görüldüğü üzere, Ağ Bağlantısını Kesme saldırısıyla ağdan düşen istasyonun, saldırı bitirildikten sonra tekrardan Erişim Noktasına bağlanması sırasında, Erişim noktası ile arasındaki el sıkışma sekansında, 802.11 çerçevesinin bilgi bulunan kısmında (payload) şifre içeren EAPOL çerçevesi yakalanmıştır. Yakalanan çerçeveye ait kayıt dışarıya aktarılmıştır. Uzantısı .cap olan kayda, aircrack-ng tool'u yardımıyla, hazırlanan bir şifre sözlüğü yardımıyla, çevrimdışı olarak kaba kuvvet (brute force) saldırısı yapılmıştır.

Çevrimdışı yapılan bu saldırının sonuç vermesi için, hedef şifre sözlükte içerisinde yer almalıdır. Şekil 2.13'te hedef ağın şifresi, kullanılan örnek sözlüğe eklenmiştir. Çevrimdışı kaba kuvvet saldırısının ardından, hedeflenen ağ şifresi elde edilebilmiştir.

Şekil 2.13: Aircrack-ng Aracı Kullanılarak Kaba Kuvvet Saldırısı İle Ağ Şifresinin Elde Edilmesi

Saldırıların çevrimdışı yapılmasından ötürü, EAPOL çerçeve yakalandıktan sonra ağ şifresi değişmediği sürece günümüz teknolojilerinin sağladığı gelişmiş şifre sözlükleri ve işlem gücü yüksek şifre kırma motorları düşünüldüğünde şifre kırılmasının olanağının yüksek olduğu görülmektedir [28].

2.5.3 Açık Veri Seti Üzerinde Makine Öğrenmesi Model Çalışmaları

Bu kısımda, tasniflenmiş çok sayıda saldırı kayıtlarına yer veren açık veri seti üzerinde Makine Öğrenmesi modelleri oluşturulmuştur.

Veri seti seçimi için, Kablosuz Saldırı Tespit Sistemleri arasında en kapsamlı açık veri setlerinden biri olan AWID (Aegean Wi-Fi Intrusion Dataset) veri seti tercih edilmiştir. [15]. Veri seti içerisindeki "AWID-CLS-R-Trn" isimli alt veri seti üzerinde çalışmalar yapılmıştır [29]. Veri setinde bulunan saldırılar "flooding", "impersonation", "injection", "normal" sınıflarına ayrılmış kayıtları içermektedir. Test veri seti için ise "AWID-CLS-R-Tst" isimli alt veri seti kullanılmıştır ve isimlendirme notasyonu aşağıda gösterilmiştir.

CLS: Bir paketin hangi atak sınıfına ait olduğuna dair bilgiler içerdiği için gösterilen etikettir.
R: Veri setinin orijinal haline göre azaltılmış bir versiyonu olduğunu belirten etikettir.
TRN: Train (eğitim) veri seti olduğu anlamına gelmektedir.
TST: Test veri seti olduğu anlamına gelmektedir

Her bir kayıt .txt uzantılı dosya olarak tasnif edilmiştir ve 155 adet sütuna sahiptir. İlk 154 sütun ilgili kaydın özelliğini, son sütun ise bu kaydın hangi saldırı sınıfına ait olduğunu göstermektedir. Kayıtların sütun yapısı [30]'de gösterilmiştir.

Veri setini eğitebilmek adına, işlem gücü yüksek bilgisayarların kullanılması süreleri kısaltacağı için bu işlemleri gerçekleştirmek üzere "Google Colab" ortamı kullanılmıştır [31]. Google Colab, Web tarayıcı üzerinden Makine Öğrenmesi ve Derin Öğrenme algoritmaları çalıştırabilecek çok sayıda Python [32] kütüphanesi ile beraber kullanılabilen bir geliştirme ortamıdır. Bu veri seti, Google'ın yüksek işlem yapabilme yeteneğinde olan güçlü GPU'lara sahip sunucuları sayesinde istenen işlemler kişisel bilgisayarla göre çok daha kısa sürelerde gerçekleştirebilmektedir.

Çalışma ortamı ayarlandıktan sonra ilgili veri seti üzerinde eğitim yapma esasına dayalı olarak Makine Öğrenmesi ve Derin öğrenme işlemlerinin temel prensipleri uygulanmıştır. Temel prensipler gözetilirken, modellerin başarım kriterlerinin yüksek olması bu tez kapsamında asıl etki yaratması beklenen önemli bir parametre olarak tasarım yapılmamıştır. Literatürde daha önceden oluşturulmuş çok sayıda modelin tez çalışmaları kapsamında kullanılan modellerden daha etkili sonuç verdiği bilinmektedir. Bu nedenle tez kapsamında ilk olarak hedef, herhangi bir modelin uçtan uca çalışan gömülü mimari içerisinde tutarlı ve verimli sonuç sunabileceği bir yapı oluşturmaktır. Bu nedenle öncelikle tutarlı olarak çalışabilen bir modelin elde edilmesi çalışmalar yapılmıştır.

Veriler eğitilmeden önce; Veri Temizleme işlemine sokulmuştur. Bu işlemlerin kapsamı aşağıda sırasıyla anlatılmıştır.

- Veri seti içerisindeki değeri olmayan ve "?" işareti ile gösterilen tüm kayıtlar "NaN" olacak şekilde değiştirilmiştir.

- Veriseti içerisinde tüm değerleri “NaN” olan sütunlar çıkarılmıştır.
- Değerlerinin %60’ından fazlası “NaN” olan sütunlar çıkarılmıştır.
- Tüm değerleri aynı olan sütunlar (değerleri arasında varyans olmayan) eğitim aşamasında anlamlı bir katkı sunmayacakları için çıkarılmıştır.
- Modelin matematiksel işlemleri için uyumsuzluk yaratacağı olan veri yapıları (özellikle MAC Adresleri ve String’ler), adres alanları gözetilerek tam sayı format çevrilmiştir.
- “MinMax Scaling” normalizasyonu yapılmıştır.

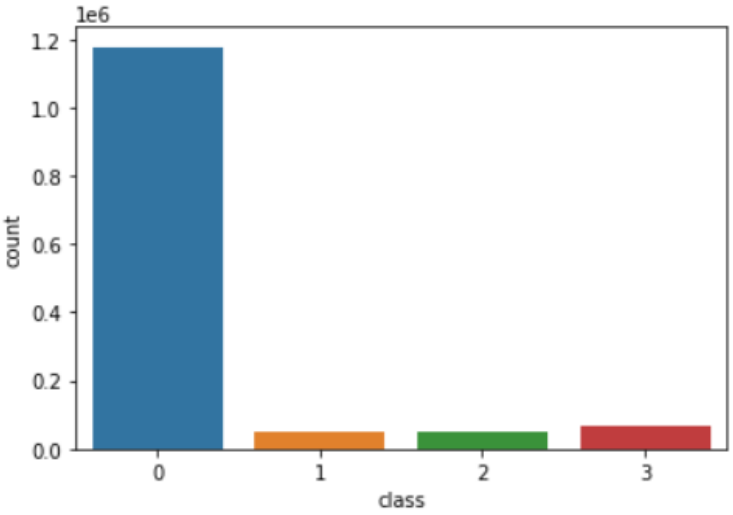
Böylelikle ilk işlemlerde değerlendirilecek özellik sayısı 154’ten 37’e düşürülmüştür. Bu özellikler aşağıda çizelge halinde gösterilmiştir.

Çizelge 2.1: İlk Veri Temizleme İşlemi Sonrası Kalan Özellikler Çizelgesi (37 özellik)

frame.time_delta	radiotap.channel.type.cck	wlan.ra
frame.time_delta_displayed	radiotap.channel.type.ofdm	wlan.da
frame.len	radiotap.dbm_antsignal	wlan.ta
frame.cap_len	wlan.fc.type_subtype	wlan.sa
radiotap.length	wlan.fc.type	wlan.bssid
radiotap.present.tsft	wlan.fc.subtype	wlan.frag
radiotap.present.flags	wlan.fc.ds	wlan.seq
radiotap.present.channel	wlan.fc.frag	wlan.wep.iv
radiotap.present.dbm_antsignal	wlan.fc.retry	wlan.wep.key
radiotap.present.antenna	wlan.fc.pwrmgt	wlan.wep.icv
radiotap.present.rxflags	wlan.fc.moredata	data.len
radiotap.datarate	wlan.fc.protected	
radiotap.channel.freq	wlan.duration	

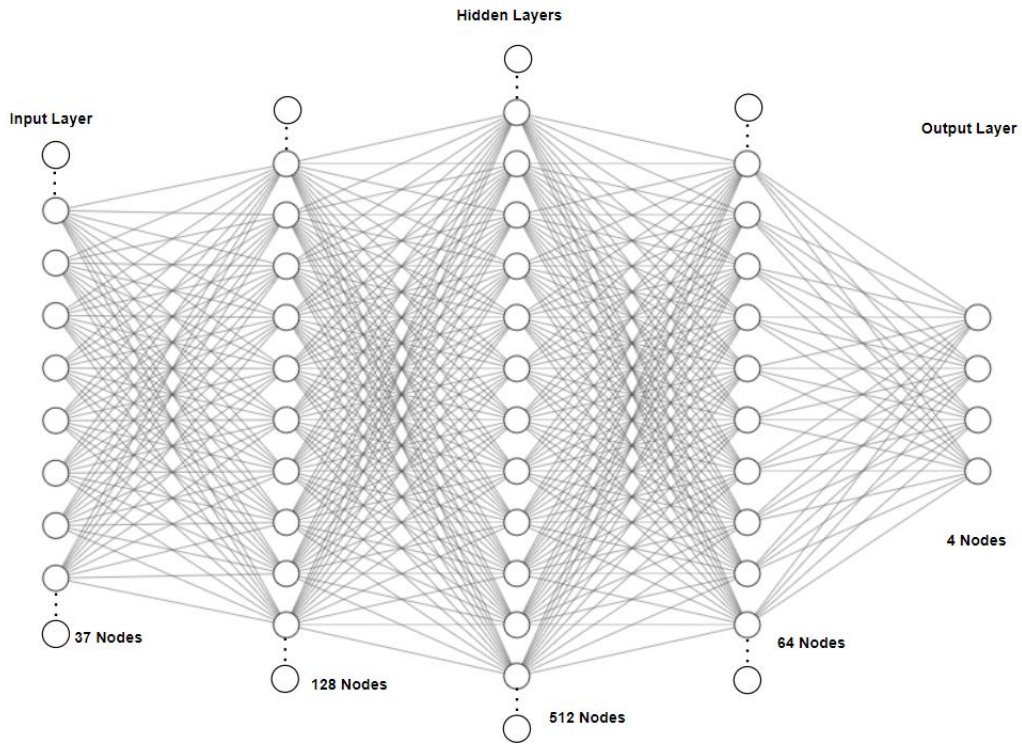
İlk aşamadaki büyük ölçüde temizleme sonucunda veri setinin içerdiği normal ve saldırı sınıflarına dair dağılım grafiği Şekil 2.14’te gösterilmiştir. Google Colab Ortamında saldırı sınıflarına tam sayı (integer) değeri ataması yapılabildiği için

sayılara karşılık gelen saldırı sınıfları şu şekilde gösterilmiştir; 0: Normal, 1: Flooding, 2: Impersonation, 3: Injection)



Şekil 2.14: Kayıtların Sınıflarına Göre Dağılım Oranları (0: Normal, 1: Flooding, 2: Impersonation, 3: Injection)

Veri temizleme işlemi sonrasında, veri seti üzerinde Eğitim (Training), Doğrulama (Validation) ve Test süreçleri işletilmiştir. Bu işlemler yapılırken, farklı projelerden örnek yaklaşımlar kullanılmıştır [33, 34, 35, 36]. Analiz edilen veri setinin bahsedilen aşamaların sonucunda öncelikli olarak 3 “hidden” ve giriş-çıkış katmanlarına sahip Sinir Ağları modeli oluşturulmuştur. Katmanlara ve düğüm noktalarına ilişkin bilgiler Şekil 2.15’te gösterilmiştir.

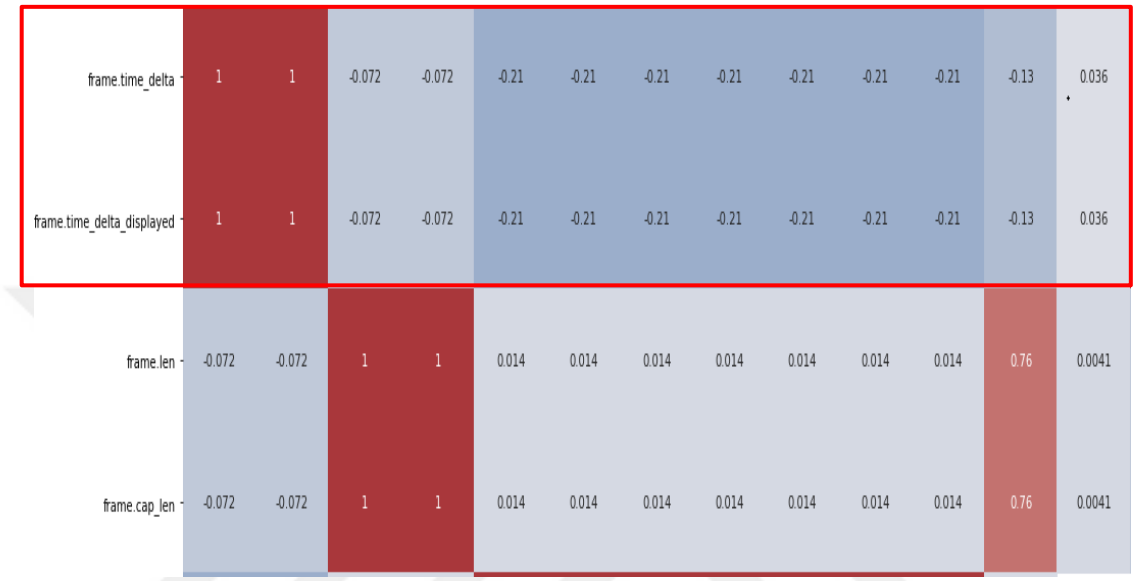


Şekil 2.15: Bu Çalışmada Kullanılan Sinir Ağları Modelinin Gösterimi (37 Özellik Giriş - 4 Sonuç Çıkış)

Üstte temsili olarak verilen Sinir Ağları modeline girdi olarak verilen test veri setinin başarım sonuçları dikkate alındığında kayıtların sadece "flooding" saldırısı varken "flooding" olarak işaretlendiği başarı kıstasındaki oranı %75 olarak elde edilmiştir. Sonuçları alınan veri seti öncelikle yapılan işlemlerin doğruluğunu onaylayabilmek adına kontrollü deney yapılabilmesi için, eğitim veri seti içerisinde bulunan verilen %20'lik son kısmının test olarak verilmesiyle elde edilmiştir.

Ağ Bağlantısını Kesme yani "flooding" kategorisindeki saldırıların tespit başarım oranını arttırmak için model üzerinde geliştirmelere devam edilmiştir. 155'ten 37 düşürülen özellik kümesi üzerinde yapılan çalışmalar sonucu özellik kümesi 16'ya indirilmiştir. Özelliklerin sadeleştirme işlemleri için öncelikle popüler bir uygulama olan "heat-map" matrisi oluşturulup çıktısı incelenmiştir. Bu matris veri setinde özelliklerin birbirleriyle olan korelasyonlarını ortaya koyarken, korelasyonları aynı ya da birbirlerine çok benzer olan özelliklere ait satırların veri setine olan etkisini aynı olacağı için, ilgili özellikler eksiltilmiştir.

Örnek olarak Şekil 2.16'da görüldüğü üzere, "frame.time_delta" ile "frame.time_delta_displayed" özelliklerinin veri setine olan etkilerinin aynı olduğu görülebilmektedir. Böylelikle bu iki özellik aslında tek bir özellik olarak değerlendirmeye alınabilmektedir.



Şekil 2.16: Heatmap Matrisinin Örnek İki Özellik İçin Korelasyon Sonuç Çıktısı

Sadeleştirmeyle beraber kalan özellikler Çizelge 2.2'de gösterilmiştir.

Çizelge 2.2: İyileştirilmiş Modele Ait Özellik Listesi (16 Özellik)

frame.time_delta	radiotap.dbm_antsignal	wlan.fc.protected
frame.len	wlan.fc.type	wlan.duration
radiotap.length	wlan.fc.subtype	wlan.da
radiotap.datarate	wlan.fc.ds	data.len
radiotap.channel.type.cck	wlan.fc.retry	
radiotap.channel.type.ofdm	wlan.fc.pwrmgt	

Bu alanda benzer uygulamalar içeren çalışmalar sonucu oluşturulan [37, 5] ve aşağıdaki şekilde verilen özelliklerin atak tipleri özelinde etkisi çizelgesi referans

alındığında, 16 özelliğe düşürülen modelin kapsadığıyla, referans uygulamalarda sunulan özelliklerin benzerlik gösterdiği görülmüştür. Bu nedenle modelin eğitim aşamasında tutarlı kıstaslar altında yorumlandığı değerlendirmiştir.

Class Name	Feature	Value	Impact
Flooding	wlan.fc.type (6)	High	Negative Low
	frame.len (0)	Low	Positive Low
	radiotap.dbm_antsignal (5)	High	Positive High
	radiotap.datarate (2)	Low	Positive Low
	wlan.da (16)	High	Positive Low
Impersonation	wlan.seq (18)	High	Negative High
	wlan.fc.subtype (7)	Low/High	Positive High
	radiotap.dbm_antsignal (5)	high	Positive High
	frame.len (0)	Low	Positive High
	wlan.fc.pwrmgt (11)	High	Positive Low
Injection	wlan.duration (14)	High	Positive High
	wlan.fc.protected (13)	High	Positive High
	wlan.fc.subtype (7)	Low	Positive High
	wlan.fc.ds (8)	Low/High	Positive High
	frame.len (0)	Low	Negative High
Normal	frame.len (0)	Low	Positive High
	wlan.fc.subtype (7)	Low/High	Positive High
	wlan.duration (14)	High	Positive Low
	radiotap.datarate (2)	High	Positive Low
	wlan.fc.type (6)	High	Positive Low

Şekil 2.17: Özelliklerin Saldırı Tiplerine Olan Etkisi [37]

Veri setinin son hali için tekrardan sinir ağları oluşturulup başarım sonuçları analiz edilmiştir. Veri seti üzerine Makine Öğrenmesi çatısı altında bulunan popüler algoritmalardan Decision Tree Classifier, Naive Bayes, Logistic Regression ve Random Forest [38] uygulanmıştır. Tüm algoritmaların flooding sınıfa ait, 16 özelliğe düşürülmüş veri seti üzerinde gerçek test veri seti girdi olarak verildiğinde alınan başarım kriterleri aşağıdaki çizelgede gösterilmiştir. Başarım, yine kayıtların sadece "flooding" saldırısı varken, "flooding" olarak işaretlenen kayıtlara göre kıstas oluşturularak hesaplanmıştır.

Çizelge 2.3: Uygulanan Metotların Başarım Sonuçları

Algoritma	Sinir Ağları	Decision Tree Classifier	Naive Bayes	Logistic Regression	Random Forest
Flooding Başarı Sonucu	0.83	0.9203	0.8916	0.4439	0.7139

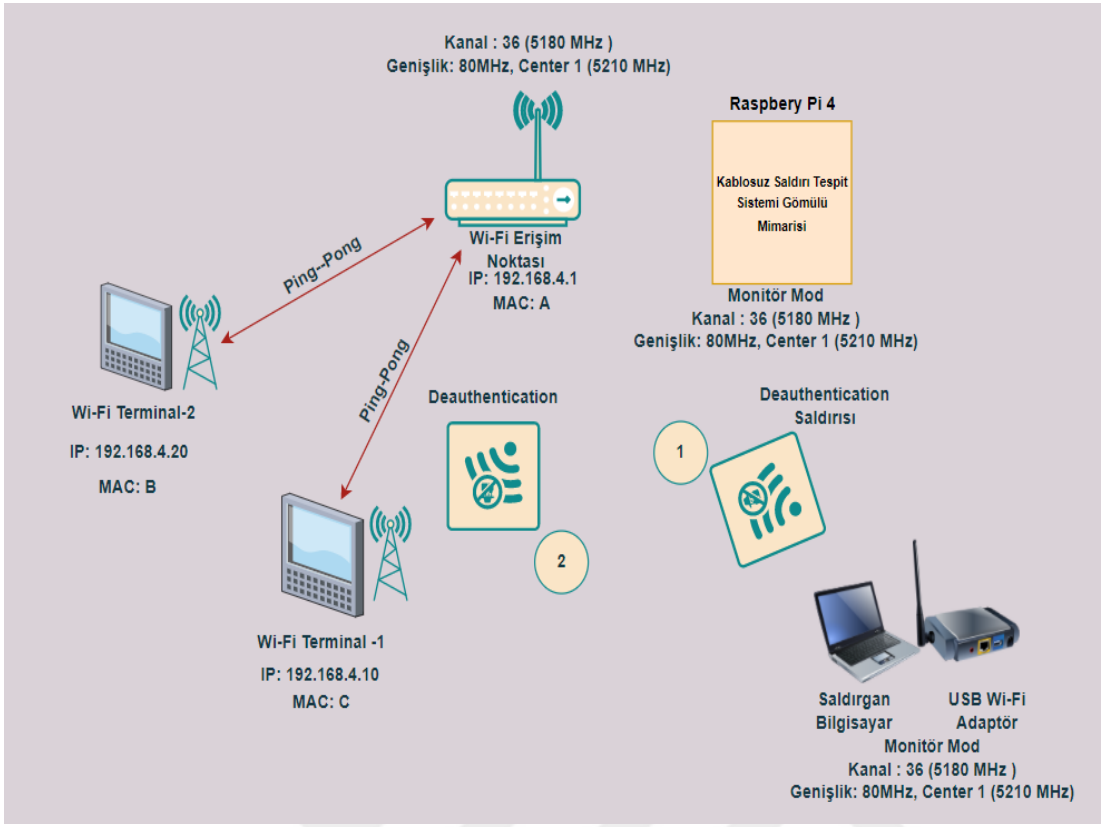
2.5.4 Modellerin Donanıma Aktarılması ve Kullanıcı Arayüzü

Bu bölümde, oluşturulan Makine Öğrenmesi modellerinin arka yüzde konumlandırılması ve kullanıcı arayüzünün gerçeklenmesini anlatmaktadır.

Google Colab ortamında elde edilen Makine Öğrenmesi ve Derin Öğrenme modelleri arka yüzde konumlandırılmıştır. Arka yüzde konumlandırılan modellere gerçek veriler uygun şekilde girdi olarak verilirken, uçtan uca çözüm üzerinden sonuçlar incelenmiştir.

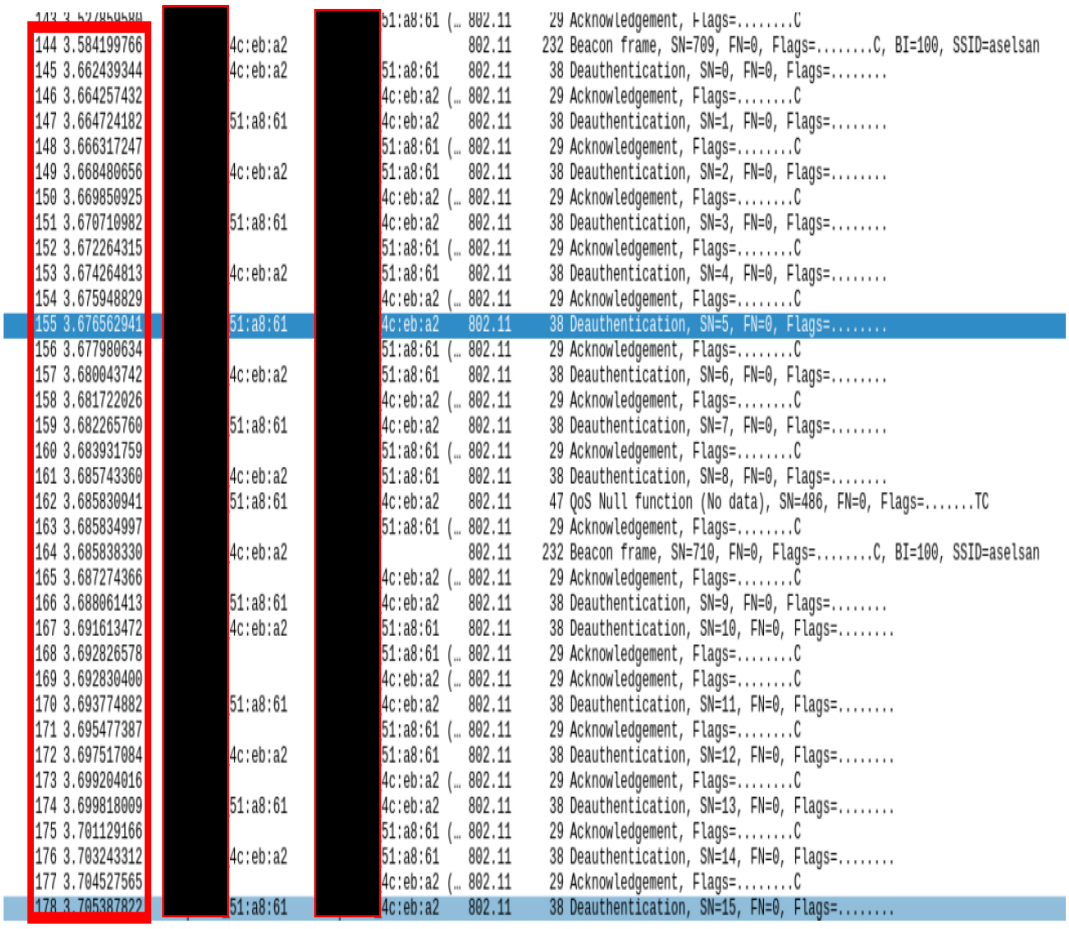
Google Colab ortamında GPU tabanlı fiziksel kaynaklar üzerinde hazırlanan modellerin, Raspberry PI 4 üzerinde CPU tabanlı bir ortama aktarılması için Pickle [39] aracı kullanılmıştır. Modellerin çalıştırabilmesi, doğru paket ve değişken formatlarının hazırlanabilmesi için Google Colab Ortamındaki Python kütüphane versiyonları ile Raspberry Pi 4 üzerinde kurulu Python kütüphane versiyonları uyumlu hale getirilmiştir.

Modellerin aktarılması ve doğruluğunun onaylanmasıyla beraber, ilgili modeller Bölüm 2.3.1'de anlatılan Kablosuz Saldırı Tespit Sistem mimarisine konumlandırılmıştır. Ardından gerçek bir senaryo üzerinden denemeye tabi tutulmuştur. Bölüm 2.5.2'de anlatıldığı gibi Ağ Bağlantısını Kesme saldırısı Şekil 2.11'deki topoloji düzeneğine ek olarak Kablosuz Saldırı Tespit Sisteminin üzerinde çalıştığı Raspberry Pi 4 donanımı eklenerek yeni bir topoloji kurulmuş, uçtan uca çözüm mimarisi test edilmiştir.



Şekil 2.18: Bu Çalışmada Oluşturulmuş Donanım Tabanlı Kablosuz Saldırı Tespit Sisteminin Ağ Bağlantısını Kesme Saldırısı Topolojisine Eklenmesi

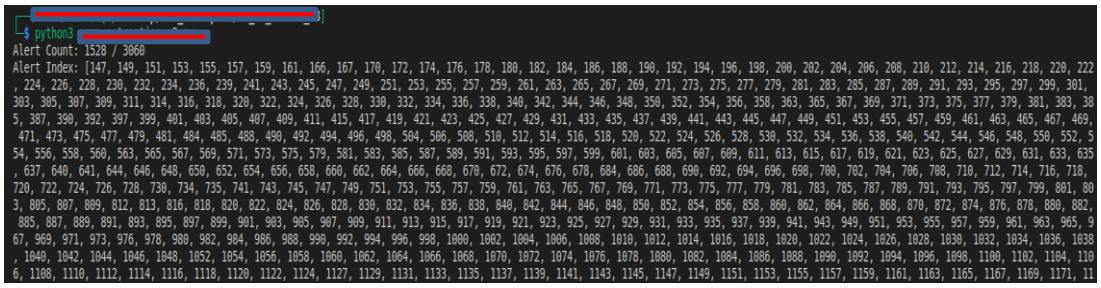
Ayrıca saldırılar Şekil 2.19'da görüldüğü üzere kayıt altına alınmıştır.



Şekil 2.19: Ağ Bağlantısını Kesme Saldırısı İçeren .pcap Dosyasının Belirli Bir Kısmı

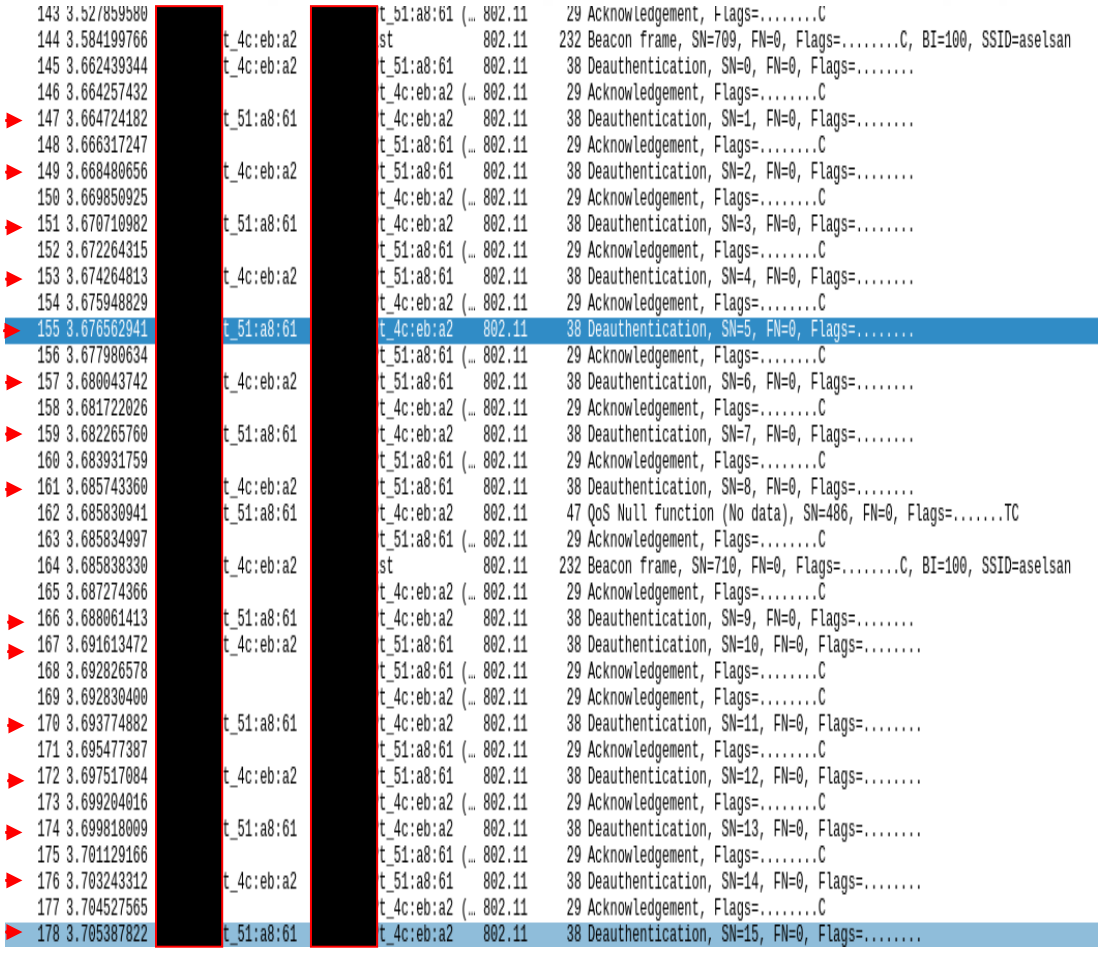
Paralel olarak analiz edilen sonuçlar için, başarım kriteri Makine Öğrenmesi uygulamalarında en yüksek olan Decision Tree algoritması ve ek olarak Sinir Ağları modeli kullanılmıştır. Blokların atak olarak alarm ürettikleri indeksler belirlenmiştir.

Saldırı sırasında, Saldırı Tespit Sistemi mimarisi içerisinde çalışan Decision Tree Classifier modelinin ürettiği alarm indeks çıktıları Şekil 2.20'de gösterilmiştir. Çıktıların .pcap dosyasında karşılık geldiği çerçeveler de Şekil 2.21'deki gibi işaretlenmiştir.



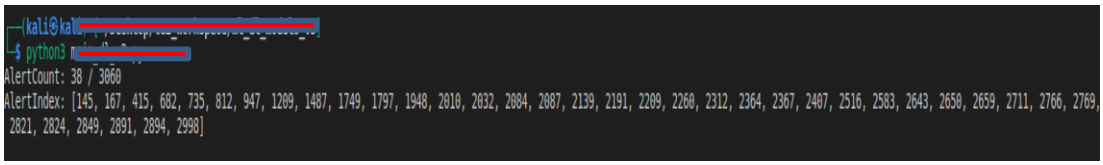
Şekil 2.20: Decision Tree Classifier Modeli Alarm İndeks Çıktıları

Test ortamındaki elde edilen kayıtlar dikkate alındığında, Decision Tree Classifier modeli ile, Ağ Bağlantısı Kesme saldırı indeksli paket sayısının yakalanma oranı %98 olarak sağlanmıştır.

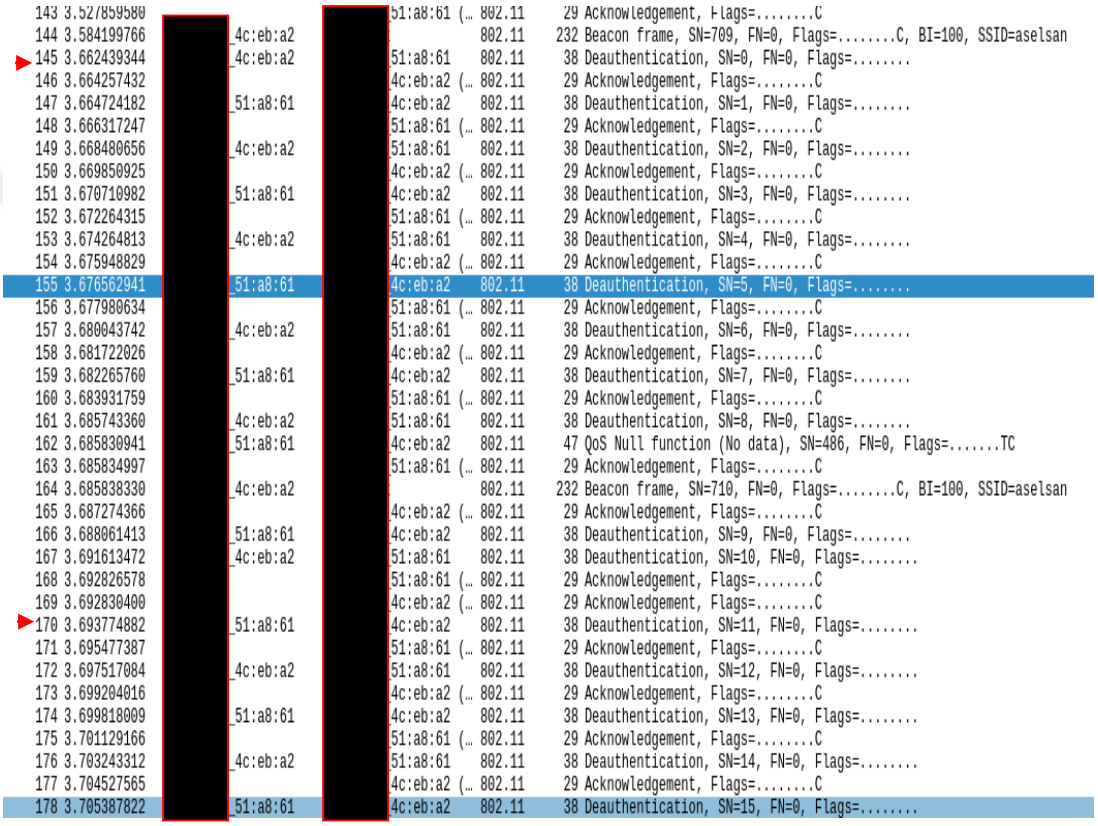


Şekil 2.21: Decision Tree Classifier Modelinin Ürettiği Alarm İndeks Çıktılarına Karşılık Gelen Çerçeveler

Aynı saldırı sırasında, Saldırı Tespit Sistemi mimarisi içerisinde çalışan Sinir Ağları modelinin ürettiği alarm indeks çıktıları Şekil 2.22'de gösterilmiştir. Çıktıların .pcap dosyasında karşılık geldiği çerçeveler de Şekil 2.23'teki gibi işaretlenmiştir.



Şekil 2.22: Sinir Ağları Modelinin Ürettiği Alarm İndeks Çıktıları



Şekil 2.23: Sinir Ağları Modelinin Ürettiği Alarm İndeks Çıktılarına Karşılık Gelen Çerçeveler

Test ortamındaki elde edilen kayıtlar dikkate alındığında, Sinir Ağları modeli ile, Ağ Bağlantısı Kesme saldırı indeksli paket sayısının yakalanma oranı %43 olarak sağlanmıştır.

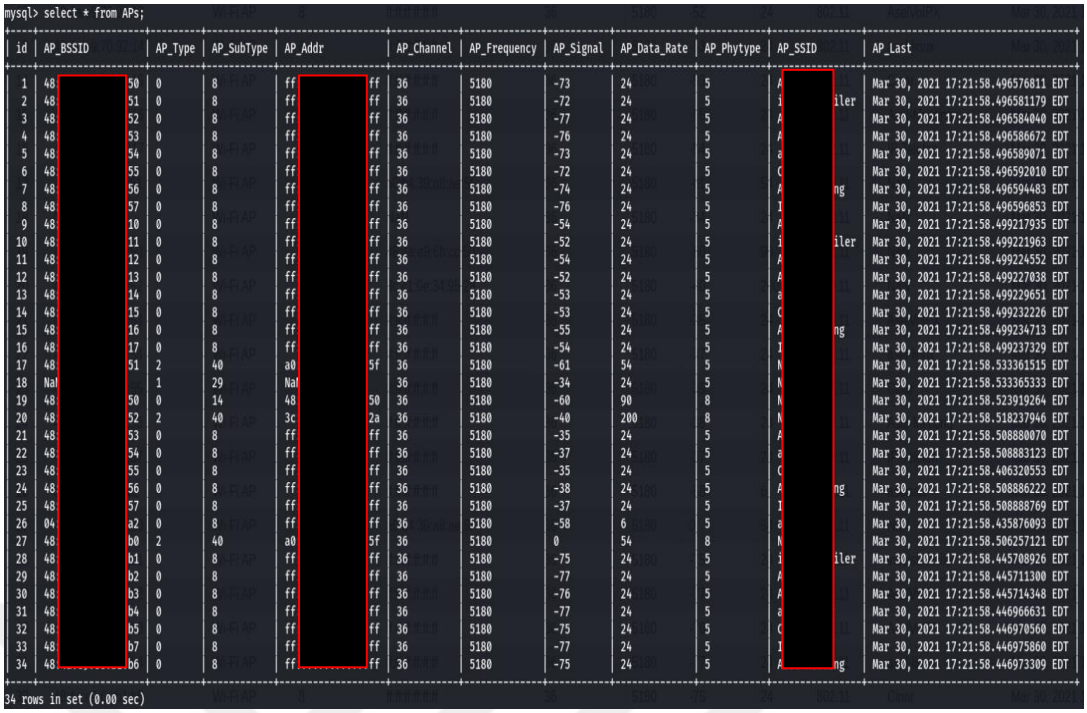
Çıktılar incelendiğinde modellerin belli başarım oranlarında Ağ Bağlantısını Kesme çerçevelerini yakalayıp, alarm olarak ürettiğini görülmektedir. Fakat bu tahminler, üzerinde çok sayıda optimizasyon yapılması gerektiren kaba tahminler olmakla beraber geliştirmeye açık durumdadırlar. Sonuç olarak, üzerinde detayları

çalışılabilecek ya da benzer teknikler ile oluşturulabilecek modeller, ana sistemin arka yüzüne başarıyla aktarılabilmiştir. Algoritmalar ya da yaklaşımlar değiştirilerek arka yüzde bulunacak herhangi bir modele yapılacak güncellemeler, sistemin alarm üretme mekanizmasını değiştirebilmektedir. Sistem mimarisinin jenerik tasarımı ile, herhangi bir model eklenmesi veya güncellenmesi, sistemin işleyişini bozmamaktadır.

Bir sonraki aşama ise; saldırı sonrası paketlerin arka yüzde analiz edilerek, ara katman vasıtasıyla ön yüzde gösterilmesidir. Blok şemada da anlatıldığı üzere, yakalanan paketler arka yüzde bulunan paket yakalama ve tasnif bloklarını içeren alt servisler aracılığıyla işleme alınmaktadır. Okuma servisi; paketlerin "Bssid, Type, Subtype, Dest_Addr, Channel, Frequency, Signal Power, Data Rate, Phy, SSID, Last_seen" [40] alanlarına bakarak veri işleme yapmaktadır. Okuma servisinde, Python sarıcısı(wrapper) olan ve Wireshark [41] disektörleri kullanılarak Python paket ayrıştırmasına izin veren Pyshark [42] kütüphanesi kullanılmıştır. Ağ durum bilgisini sunabilmek adına, bu alanların yeterli olduğu ön görülmüş olmakla beraber, gelecek çalışmalardaki ihtiyaçlara binaen değiştirilebilecek şekilde gerçeklenmiştir.

Okunan paketler, öncelikle "MySQL" veri tabanına yazılmaktadır. Veri tabanına yazılan bilgiler iki farklı kontrolden geçirilmektedir. İlk kontrol kapsamında herhangi erişim noktasına dair bir bilgi arka yüze ilk defa gelmişse, ilgili Erişim Noktasına bir "ID" atanmaktadır ve bu ID adı altında bilgiler veri tabanında tutulmaktadır. Daha önce ID atanmış erişim noktalarına ilişkin bilgiler gelmeye devam ettikçe, veri tabanında ilgili ID'ye dair alanlar güncellenmektedir.

36. Kanal üzerinde örnek bir ortam dinlemesi yapan Raspberry Pi 4'ün elde ettiği bilgilere göre MySQL veri tabanını şekillendirmesine dair örnek bir çıktı Şekil 2.24'te gösterilmiştir.



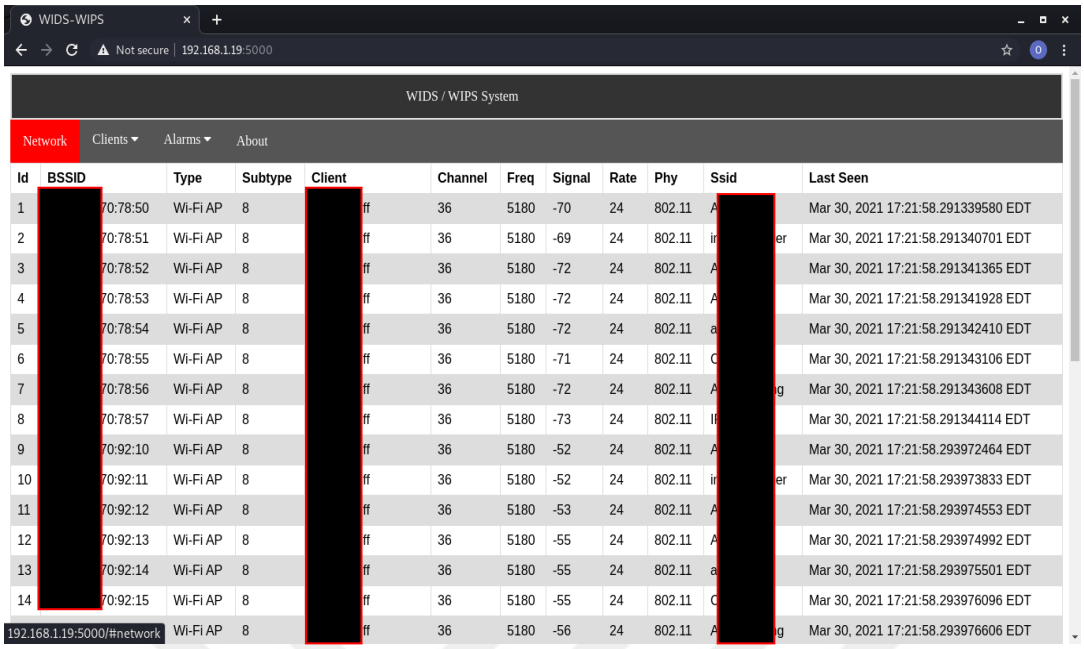
```
mysql> select * from APs;
+----+-------------------+---------+------------+-------------------+------------+--------------+-------------+---------------+-----------+---------+-------------------------------+
| id | AP_BSSID          | AP_Type | AP_SubType | AP_Addr           | AP_Channel | AP_Frequency | AP_Signal   | AP_Data_Rate  | AP_Phytype| AP_SSID | AP_Last                       |
+----+-------------------+---------+------------+-------------------+------------+--------------+-------------+---------------+-----------+---------+-------------------------------+
|  1 | 48[redacted]50    |       0 |          8 | ff[redacted]ff    |         36 |         5180 |         -73 |            24 |         5 | A[redacted]   | Mar 30, 2021 17:21:58.496576811 EDT |
|  2 | 48[redacted]51    |       0 |          8 | ff[redacted]ff    |         36 |         5180 |         -72 |            24 |         5 | i[redacted]iler | Mar 30, 2021 17:21:58.496581179 EDT |
|  3 | 48[redacted]52    |       0 |          8 | ff[redacted]ff    |         36 |         5180 |         -77 |            24 |         5 | A[redacted]   | Mar 30, 2021 17:21:58.496584040 EDT |
|  4 | 48[redacted]53    |       0 |          8 | ff[redacted]ff    |         36 |         5180 |         -76 |            24 |         5 | A[redacted]   | Mar 30, 2021 17:21:58.496586672 EDT |
|  5 | 48[redacted]54    |       0 |          8 | ff[redacted]ff    |         36 |         5180 |         -73 |            24 |         5 | a[redacted]   | Mar 30, 2021 17:21:58.496589071 EDT |
|  6 | 48[redacted]55    |       0 |          8 | ff[redacted]ff    |         36 |         5180 |         -72 |            24 |         5 | C[redacted]   | Mar 30, 2021 17:21:58.496592010 EDT |
|  7 | 48[redacted]56    |       0 |          8 | ff[redacted]ff    |         36 |         5180 |         -74 |            24 |         5 | A[redacted]ng | Mar 30, 2021 17:21:58.496594483 EDT |
|  8 | 48[redacted]57    |       0 |          8 | ff[redacted]ff    |         36 |         5180 |         -76 |            24 |         5 | I[redacted]   | Mar 30, 2021 17:21:58.496596853 EDT |
|  9 | 48[redacted]10    |       0 |          8 | ff[redacted]ff    |         36 |         5180 |         -54 |            24 |         5 | A[redacted]   | Mar 30, 2021 17:21:58.499217935 EDT |
| 10 | 48[redacted]11    |       0 |          8 | ff[redacted]ff    |         36 |         5180 |         -52 |            24 |         5 | i[redacted]iler | Mar 30, 2021 17:21:58.499221963 EDT |
| 11 | 48[redacted]12    |       0 |          8 | ff[redacted]ff    |         36 |         5180 |         -54 |            24 |         5 | A[redacted]   | Mar 30, 2021 17:21:58.499224552 EDT |
| 12 | 48[redacted]13    |       0 |          8 | ff[redacted]ff    |         36 |         5180 |         -52 |            24 |         5 | A[redacted]   | Mar 30, 2021 17:21:58.499227038 EDT |
| 13 | 48[redacted]14    |       0 |          8 | ff[redacted]ff    |         36 |         5180 |         -53 |            24 |         5 | a[redacted]   | Mar 30, 2021 17:21:58.499229651 EDT |
| 14 | 48[redacted]15    |       0 |          8 | ff[redacted]ff    |         36 |         5180 |         -53 |            24 |         5 | C[redacted]   | Mar 30, 2021 17:21:58.499232226 EDT |
| 15 | 48[redacted]16    |       0 |          8 | ff[redacted]ff    |         36 |         5180 |         -55 |            24 |         5 | A[redacted]ng | Mar 30, 2021 17:21:58.499234713 EDT |
| 16 | 48[redacted]17    |       0 |          8 | ff[redacted]ff    |         36 |         5180 |         -54 |            24 |         5 | I[redacted]   | Mar 30, 2021 17:21:58.499237329 EDT |
| 17 | 48[redacted]51    |       2 |         40 | a0[redacted]5f    |         36 |         5180 |         -61 |            54 |         5 | M[redacted]   | Mar 30, 2021 17:21:58.533361515 EDT |
| 18 | Nal[redacted]     |       1 |         29 | Nal[redacted]     |         36 |         5180 |         -34 |            24 |         5 | M[redacted]   | Mar 30, 2021 17:21:58.533365333 EDT |
| 19 | 48[redacted]50    |       0 |         14 | 48[redacted]50    |         36 |         5180 |         -60 |            90 |         8 | M[redacted]   | Mar 30, 2021 17:21:58.523919264 EDT |
| 20 | 48[redacted]52    |       2 |         40 | 3c[redacted]2a    |         36 |         5180 |         -40 |           200 |         8 | M[redacted]   | Mar 30, 2021 17:21:58.518237946 EDT |
| 21 | 48[redacted]53    |       0 |          8 | ff[redacted]ff    |         36 |         5180 |         -35 |            24 |         5 | A[redacted]   | Mar 30, 2021 17:21:58.508880070 EDT |
| 22 | 48[redacted]54    |       0 |          8 | ff[redacted]ff    |         36 |         5180 |         -37 |            24 |         5 | a[redacted]   | Mar 30, 2021 17:21:58.508883123 EDT |
| 23 | 48[redacted]55    |       0 |          8 | ff[redacted]ff    |         36 |         5180 |         -35 |            24 |         5 | C[redacted]   | Mar 30, 2021 17:21:58.406320553 EDT |
| 24 | 48[redacted]56    |       0 |          8 | ff[redacted]ff    |         36 |         5180 |         -38 |            24 |         5 | A[redacted]ng | Mar 30, 2021 17:21:58.508886222 EDT |
| 25 | 48[redacted]57    |       0 |          8 | ff[redacted]ff    |         36 |         5180 |         -37 |            24 |         5 | I[redacted]   | Mar 30, 2021 17:21:58.508888769 EDT |
| 26 | 04[redacted]a2    |       0 |          8 | ff[redacted]ff    |         36 |         5180 |         -58 |             6 |         5 | a[redacted]   | Mar 30, 2021 17:21:58.435876093 EDT |
| 27 | 48[redacted]b0    |       2 |         40 | a0[redacted]5f    |         36 |         5180 |           0 |            54 |         8 | M[redacted]   | Mar 30, 2021 17:21:58.506257121 EDT |
| 28 | 48[redacted]b1    |       0 |          8 | ff[redacted]ff    |         36 |         5180 |         -75 |            24 |         5 | i[redacted]iler | Mar 30, 2021 17:21:58.445708926 EDT |
| 29 | 48[redacted]b2    |       0 |          8 | ff[redacted]ff    |         36 |         5180 |         -77 |            24 |         5 | A[redacted]   | Mar 30, 2021 17:21:58.445711300 EDT |
| 30 | 48[redacted]b3    |       0 |          8 | ff[redacted]ff    |         36 |         5180 |         -76 |            24 |         5 | A[redacted]   | Mar 30, 2021 17:21:58.445714348 EDT |
| 31 | 48[redacted]b4    |       0 |          8 | ff[redacted]ff    |         36 |         5180 |         -77 |            24 |         5 | a[redacted]   | Mar 30, 2021 17:21:58.446966631 EDT |
| 32 | 48[redacted]b5    |       0 |          8 | ff[redacted]ff    |         36 |         5180 |         -75 |            24 |         5 | C[redacted]   | Mar 30, 2021 17:21:58.446970560 EDT |
| 33 | 48[redacted]b7    |       0 |          8 | ff[redacted]ff    |         36 |         5180 |         -77 |            24 |         5 | I[redacted]   | Mar 30, 2021 17:21:58.446975860 EDT |
| 34 | 48[redacted]b6    |       0 |          8 | ff[redacted]ff    |         36 |         5180 |         -75 |            24 |         5 | A[redacted]ng | Mar 30, 2021 17:21:58.446973309 EDT |
+----+-------------------+---------+------------+-------------------+------------+--------------+-------------+---------------+-----------+---------+-------------------------------+
34 rows in set (0.00 sec)
```

Şekil 2.24: Ağ İzleme Birimini Kapsayan MySQL Veri Tabanı Tablo Çıktısı

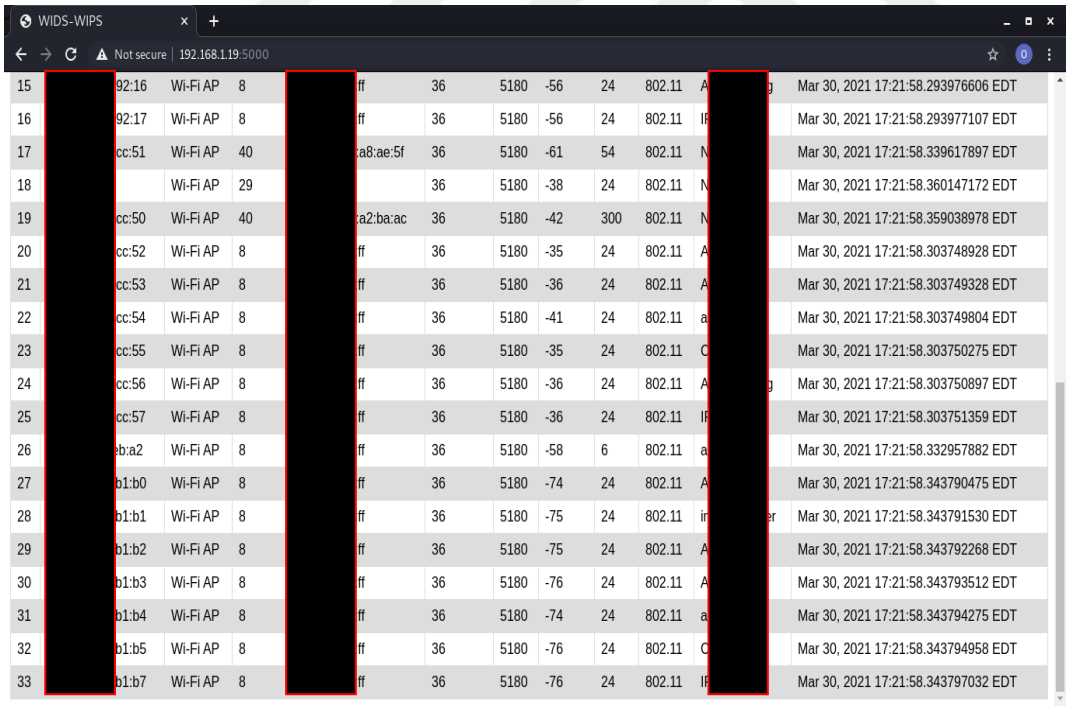
Mimari, ağda etkinlik oldukça aksiyon alacak şekilde “event-driven” [43] olarak gerçeklenmiştir. Veri tabanı, paketlere hiçbir filtre uygulanmadan gerçek zamanlı olarak uygulamalardan gelen tüm paketleri depolamak için kullanılabilmektedir. Yakalanan paketlerin okunması ve beraberinde veri tabanına bilgilerin eklenmesi ya da güncellenmesi sonunda, soket programlama esasına dayanan “socket.io” [44] ve “node.js” [45] yazılım iskeleti (framework) vasıtasıyla ilgili bilgiler ön yüze aktarılmaktadır. Bu nedenle ön yüzde Web Arayüzü üzerinden servis veren yapılar oluşturulmuştur. “Javascript” [46] yazılım iskeleti ile okunan veriler, “HTML” [47] yazılım iskeleti üzerine “CSS” [48] dili ile tasarlanmış sayfalar aracılığıyla gösterilmektedir. Ön yüzde Web arayüzü üzerinden sunulan bilgiler için 4 temel sayfa oluşturulmuştur.

Network (Ağ İzleme) Sayfası

Ağ İzleme Sayfası, Ağda bulunan tüm Erişim Noktalarının, üstte anlatılan alanlarına ilişkin bilgilerinin gerçek zamanlı sunulması ve güncellenmesiyle, ilgili sayfada ağa eklenen ya da bilgileri güncellenen her cihaz için gerçek zamanlı ve dinamik bir şekilde yenilenmektedir. Örnek bir deney düzeneğinden elde edilen ve Ağ İzleme sekmesi altında bilgilerin verildiği ekran görüntüleri Şekil 2.25 ve Şekil 2.26’da gösterilmiştir.



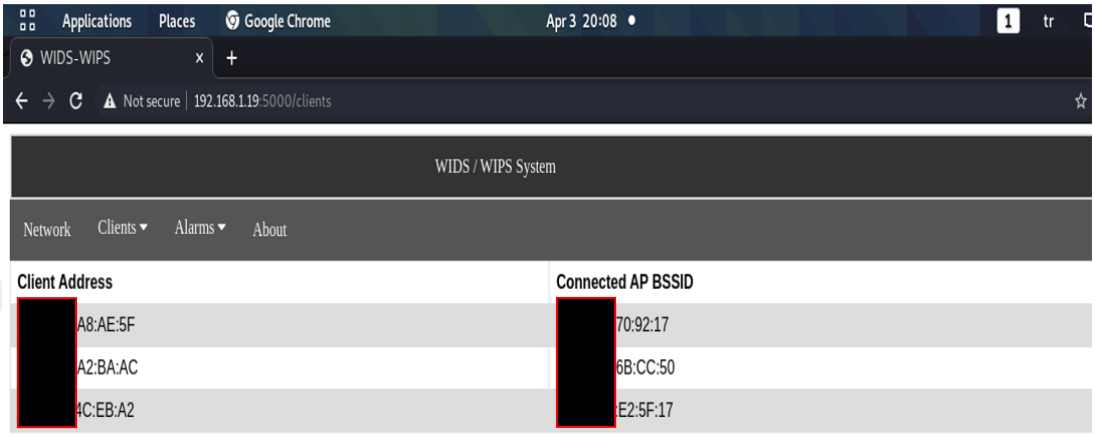
Şekil 2.25: Temel Servis Seti Mimarisinde Bulunan Ağ Cihazlarının Bilgilerini İçeren Sayfa (Network.html)



Şekil 2.26: Temel Servis Seti Mimarisinde Bulunan Ağ Cihazlarının Bilgilerini İçeren Sayfa-2 (Network.html)

Clients (İstasyonlar) Sekmesi

Yakalanan trafik içerisinde, erişim noktalarının hedeflediği istasyonlar ayrı bir tabloda tutulmaktadır. Tutulan tablo, clients (istasyonlar) sekmesinde sunulmaktadır. İlgili sayfa, ağa eklenen ya da bilgileri güncellenen her cihaz için gerçek zamanlı ve dinamik bir şekilde yenilenebilmektedir.

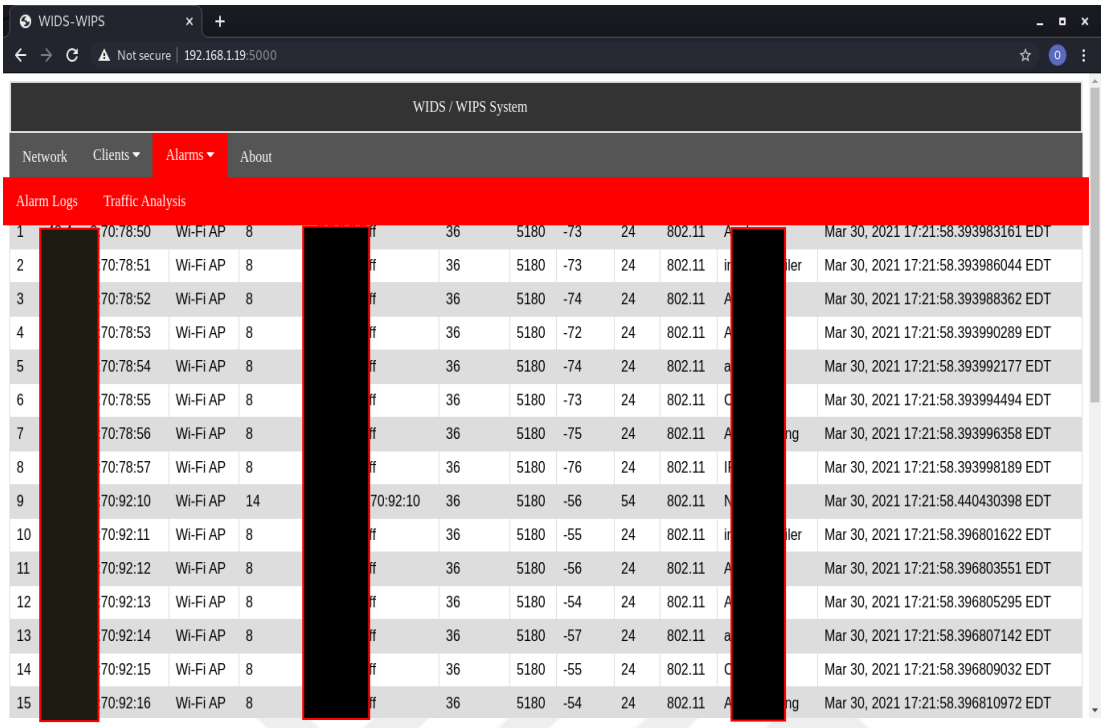


Şekil 2.27: Temel Servis Seti Mimarisinde Bulunan Erişim Noktaları ve Ona Bağlı Olan İstasyon Bilgileri Sayfası (clients.html)

Alarms (Alarmlar) Sekmesi

Alarmlar menüsü ve iki alt sekmeye ayrılmıştır. Bu sekmeler alarm kayıtları ve trafik analiz menüsü olarak tasarlanmıştır.

Alarm kayıtları; ağda bulunan herhangi bir cihaza saldırı geldiğinde güncellenmesi, trafik analiz sekmesi ise analiz edilen paketlere ilişkin metriklerin/istatistiklerin vs. sunulması planlanan sekmeler olarak düşünülmüştür. İlgili sayfa, ağa eklenen ya da bilgileri güncellenen her cihaz için gerçek zamanlı ve dinamik bir şekilde yenilenmektedir. Alarmlar sekmesi altında ağdaki bilgilerin verildiği ekran görüntüleri Şekil 2.28'de gösterilmiştir.



Şekil 2.28: Alarmlar Sayfası Alt Sekmeleri

Ağ Bağlantısını Kesme saldırısının tespit edilmesiyle beraber saldırının alarm olarak ön yüze çıktı oluşturduğu görülmüştür, ilgili durum Şekil 2.29'da gösterilmiştir.

Şekil 2.29: Temel Servis Seti Mimarisinde Uygulanan Ağdan Düşürme Saldırısına İlişkin Alarm Üretme Kaydının Alarmlar Sayfasında Gösterilmesi

3. 802.11AC TABANLI 802.11S ÖRGÜ AĞLARINA YÖNELİK SALDIRI GERÇEKLEMELERİ

Bu bölüm tezin ikinci aşamasını oluşturan 802.11s Kablosuz Örgü Ağlarına yönelik saldırı gerçeklemelerini içeren çalışmalara yer vermektedir.

3.1 ARKAPLAN

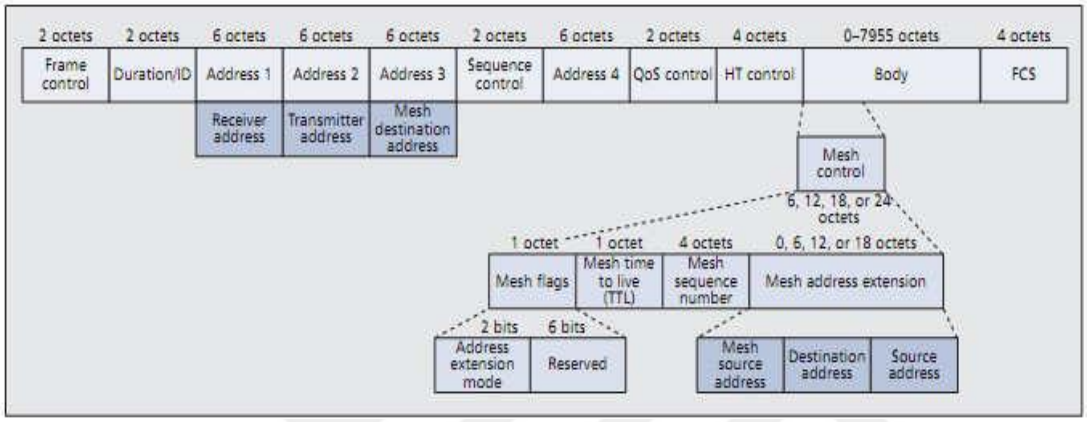
Bu bölüm, tezin ikinci kapsamında üzerinde çalışmalar yapılan kavramların arkaplanını ve kavramları oluşturan gerekli açıklamaları kapsamaktadır. Bunlar, IEEE 802.11ac teknolojisinin yardımcı protokolü IEEE 802.11s, 802.11s protokolü ile oluşturulan 802.11s tabanlı örgü ağları ve bu standardın varsayılan yönlendirme protokolü olan Hybrid Wireless Mesh Protokolü'dür.

3.1.1 IEEE 802.11s

IEEE 802.11ac başta olmak üzere fiziksel katmanda kablosuz teknolojilerin gelişmesiyle birlikte, diğer kablosuz standartların kullanımı da aynı oranda yaygınlaşmaya başlamıştır. Bu noktada, kablo bağlantılarının mümkün veya verimli olmadığı halka açık, kampüs, endüstriyel ve askeri vb. ağları kapsayacak şekilde kablosuz teknolojilerin kullanılması için 802.11 çalışma grubunu, kablosuz iletişim için bir mekanizma olarak IEEE 802.11s, Kablosuz Örgü Ağı (Wireless Mesh Networking), standardını tanımlamak üzere bir araya getirmiştir [49]. Bu standartla beraber Örgü Noktaları (Mesh Points) IEEE 802.11s ile beraber Örgü Temel Servis Seti (Mesh Basic Service Set) oluşturarak, kullanıcılara kablosuz ağlarda bir Dağıtık Yapı (Distribution System) sunabilmektedir [50]. Sahip olduğu esnek mimari, genişletilebilir yapı, kendi kendini onarabilir yetenek, gürbüzlük ve hızlı dağıtıma sahip olmasıyla öne çıkmaktadır. [4].

802.11s Çerçeve Formatı

Örgü noktaları arasında dağıtık yapının kurulmasını ardından, noktalar arası iletişim için çerçeveler gönderilmektedir. Bu çerçevelere 802.11s çerçeveleri adı verilmektedir. 802.11s'e dair çerçeve formatı aşağıdaki şekilde gösterilmiştir.



Şekil 3.1: 802.11s Çerçeve Yapısı

802.11s ve 802.11ac çerçeve tipleri arasında küçük farklılıklar vardır. Örgü ağlarına özel ek iki adres alanı daha içermesiyle beraber toplamda altı adresli çerçeve formatı kullanılmaktadır. 802.11ac çerçeve yapısında olduğu gibi FromDS ve ToDS bitleri kullanılarak dağıtık ağda katman 2 anahtarlamaya ve atlamaya (hopping) dair işlemler bu şekilde gerçekleştirilir [51].

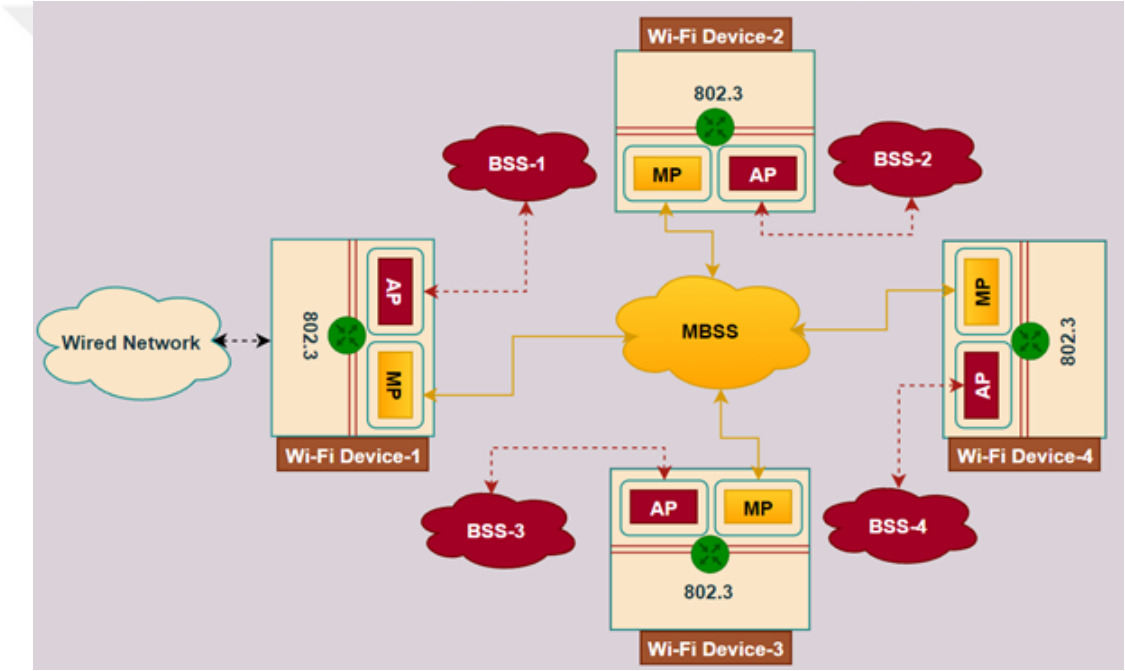
3.1.2 802.11s Tabanlı Kablosuz Örgü Ağları

802.11s Tabanlı Kablosuz Örgü Ağları, Örgü Noktaları arasında 802.11s protokolü kullanılarak oluşturulan herhangi bir Dağıtık Sisteme verilen addır. Temel olarak tüm ağa ait cihazların kablosuz bir ortam aracılığıyla birbirleriyle iletişim kurmasını sağlayan bir ağ topolojisi oluşturmak için tanımlanmaktadır. Ayrıca Örgü Noktalarının oluşturduğu ağda mümkün kılınan özellikler, işlevler ve çerçeve tipleri kümesini kapsamaktadır [52].

Örgü Temel Servis Seti'ni oluşturmak için öncelikle tüm örgü noktalarının birbirini keşfetmesi gerekmektedir. Keşif aşamasının yürütülmesi için en önemli özellik, tüm örgü noktalarının tanımlayıcısı olan "Mesh ID" dir. Bir Örgü Temel Servis Setine

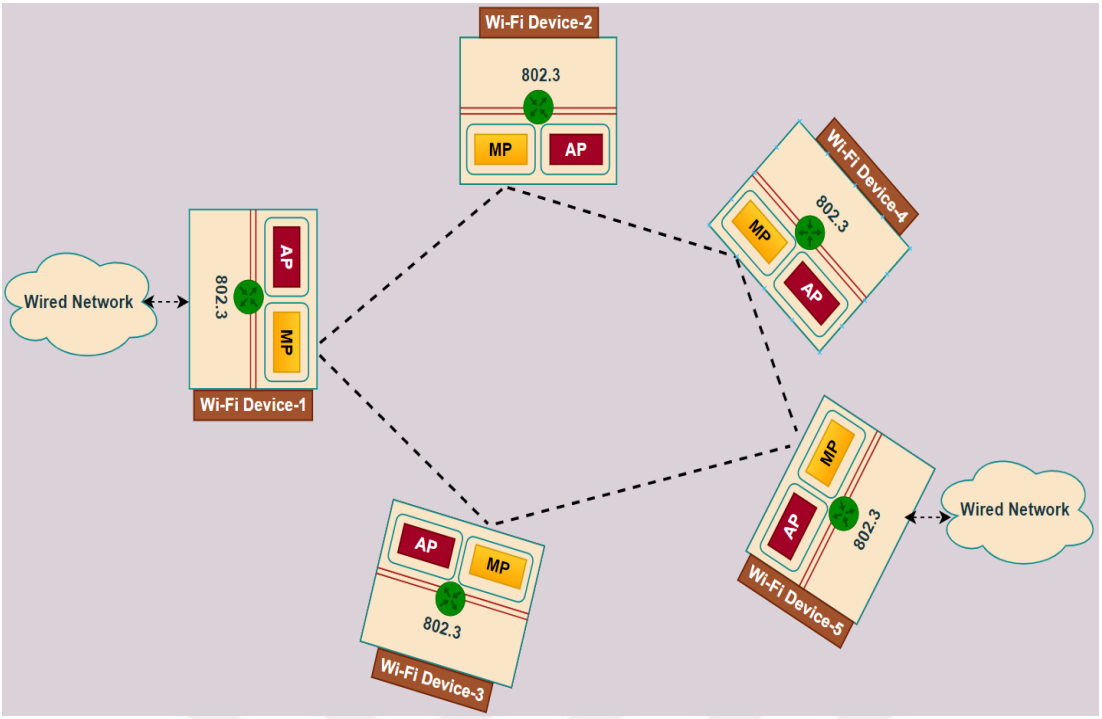
katılan ağ istasyonları, kendi kimliklerini kullanarak ağa bilgilerini gönderir ve “probe response”, “probe request” çerçevelerine yanıt verir. Keşif sürecinden sonra ise, Örgü Noktaları bir sonraki Örgü Değiş-Tokuş Yönetimine (Mesh Peering Management) aşamasına geçerler [51]. Örgü Değiş-Tokuş Yönetimi aşaması tamamlandıktan sonra, Örgü Noktalarını birbirlerine bağlı oldukları bir Örgü Temel Servis Setiyle beraber Dağıtık Yapı oluştururlar.

Kablosuz Dağıtık Ağ Mimarisinde 802.11s uyumlu Örgü Noktaları, kullanımlarına göre yönlendirici, ağ geçidi ve menzil genişletici hizmeti de sağlayabilirler. Aşağıdaki şekilde örnek olarak genel bir Örgü Temel Servis Set mimarisi gösterilmektedir.



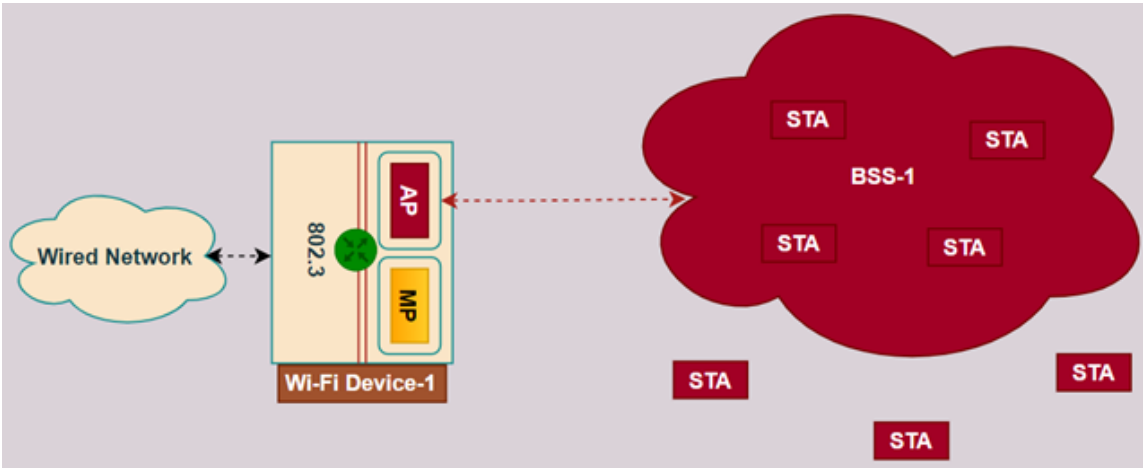
Şekil 3.2: Kablosuz Dağıtık Ağ Mimarisi Örnek Topolojisi

Dağıtık ağ kapsamında Şekil 3.3’te gösterilen topolojide, Örgü Noktaları Katman 2’de aralarında doğrudan bağlantı (directly connected) olmayan hatlar arası yönlendirme yapabilirken, kablolu ağlara geçiş için ağ geçidi hizmeti de verebilmektedir.



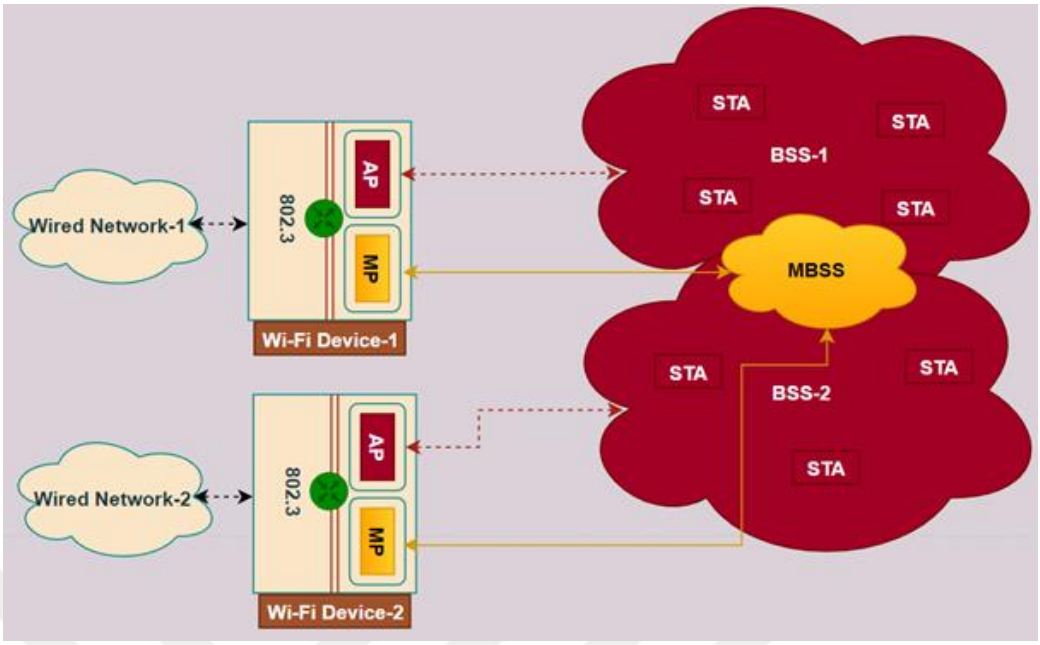
Şekil 3.3: Kablosuz Örgü Ağlarında Örgü Yapısı Kuran Örgü Noktalarına İlişkin Ağ Topolojisi Örneği

Örgü Noktaları, günlük hayattaki yaygın kullanımında olduğu gibi Temel Servis Setlerini birbirine bağlamanın bir başka türevi olarak da kullanılabilir. Aşağıdaki şekil, bir Temel Servis Seti kapsama alanında dışındaki istasyonları göstermektedir.



Şekil 3.4: Temel Servis Seti Kapsama Alanında Bulunan İstasyonlara İlişkin Ağ Topolojisi Örneği

Örgü noktaları kapsama alanı dışındaki uygun yerlere konumlandırılarak diğer ağa ait Temel Servis Seti içerisinde menzil genişletici olarak da hizmet verebilmektedir.



Şekil 3.5: Dağıtık Yapıda Kablosuz Örgü Ağları ile Temel Servis Setlerinin Birbirine Bağlanmasına İlişkin Ağ Topolojisi Örneği

3.1.3 Hybrid Wireless Mesh Protocol

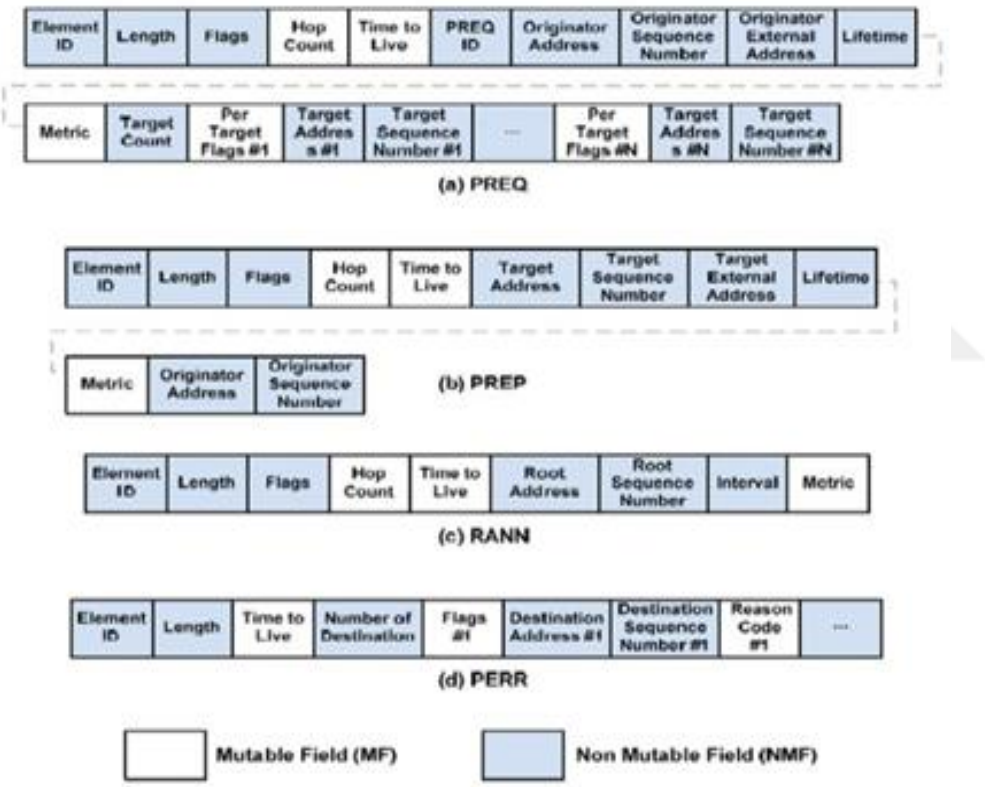
802.11s'de kullanılabilecek üreticilere özel ağ protokolleri bulunmasına rağmen, Hybrit Wireless Mesh Protokolü (HWMP / Hibrit Kablosuz Örgü Protokolü) 802.11s için varsayılan yönlendirme protokolü olarak desteklenmektedir [53]. HWMP, yönlendirme ve anahtarlama için hem proaktif hem de reaktif yol seçimi sağlamaktadır. Reaktif yol seçimi, Ad Hoc On-Demand'a (AODV) [54], proaktif ise Ağaç Tabanlı Yönlendirmeye [55] dayanır. Bir çerçeveyi bilinmeyen bir hedefe iletmesi gereken bir ağ istasyonu, bu hedefe giden en kısa yolu dinamik olarak keşfedebilir. Ağ istasyonları ayrıca dağıtık yapıdaki noktaları proaktif olarak keşfedebilir ve herhangi bir veri çerçevesi göndermeye gerek duymadan örgü ağının herhangi bir noktasına giden en kısa yolları belirleyebilmektedir [56].

HWMP Çerçeve Formatı

Yol İsteği (Path Request / PREQ), Yol Yanıtı (Path Replay / PREP), Yol Hatası (Path Error / PERR) ve Kök Duyurusu (Root Announcement / RANN) dahil olmak üzere dört tür HWMP çerçevesi vardır [57]. Bu çerçevelerin tanımları aşağıda gösterilmiştir.

PREQ: Hedef örgü noktalarından kaynak göndericiye bir yol oluşturmasını isteyen bir tek noktaya yayın(unicast) veya çoklu yayın(broadcast) paketidir.
PREP: Kaynak göndericiye bir yol oluşturan ve ters yolu onaylayan tek noktaya yayın paketidir.
PERR: Kaynak göndericinin artık belirli bir hedefi için yolu desteklemediğini bildiren bir çoklu yayın paketidir.
RANN: Örgü Noktalarına kök noktanın varlığını ve mesafesini bildiren bir yayın paketidir [58].

HWMP çerçeve format aşağıdaki şekilde gösterilmiştir.



Şekil 3.6: HWMP Çerçeve Tipleri ve Çerçeve Yapısı

Şekil 3.6'da görüldüğü üzere, HWMP çerçeve formatı içerisinde bulunan Metrik alanı, iki örgü noktası arasındaki hat kalitesini gösteren bileşendir. Bu alan, ağ içerisindeki iletişim kurulan Örgü Noktası tarafından güncellenebilmektedir.

HWMP Sekans Numarası (Sequence Number) alanı ise, ağda bulunan gönderici ve alıcı Örgü Noktasının, ilgili çerçevenin güncel olup olmadığı kararını vermek için bir göstergedir. Güncel olmayan sekans numaralarına ait çerçeveler Örgü Noktaları tarafından işleme tabii tutulmaz.

3.2 BENZER ÇALIŞMALARIN İNCELENMESİ

Literatürde 802.11s kablosuz ağlarına yönelik çok sayıda atak mekanizmasını içeren çalışmalar bulunmaktadır. Bu bölümde, 802.11 kablosuz ağlarına yönelik çalışmalara dair literatürdeki araştırmaların kapsamı ve derinliği incelenecektir.

Başlangıçta, bu tezin ikinci bölümünü belirleyecek olan 802.11s ağlarına yönelik araştırmalar analiz edilmiştir. Bu kapsamda üç ana çalışma tezin katkı yapabileceği alanlar için temel alınacak çalışmalar anlamında öne çıkmıştır.

İlk çalışma [57], Kablosuz Örgü Ağlarının dinamikliği ve kullanım potansiyelinin çok yüksek olduğundan bahsederken, bu gelişmelerin Kablosuz Örgü Ağlarına yönelik çok sayıda tehdide de yer verdiğini vurgulamaktadır. Kablosuz ağ işlemlerini yerine getirebilecek cihazların Örgü Yönlendiricisi ve Örgü İstasyonu olarak kullanılabildiğini belirten bu çalışma, kablolu ağlara bir ağ geçidi olarak hizmet verebilecek Wi-Fi cihazının, kablolu arayüzü üzerinden saldırılar planlanabildiğinden bahsetmiştir. Aynı çalışmada kablosuz arayüzleri üzerinden yapılabilecek saldırıların, Wi-Fi cihazların çoklu yayın yapma doğası gereği Güvenilirlik ve Bütünlük, Yetkilendirme ve Yönlendirme temelleri üzerinde saldırıların kurgulanabildiğinden de bahsetmiştir. Ayrıca, verilen konu başlıkları altında bu çalışma Kablosuz Örgü Ağlarında paket manipüle ederek en kısa yol hesaplamalarını istismar etmek, herhangi bir örgü noktasını taklit etmek, ağdaki trafiğin saldırgan tarafından kontrol edilerek farklı yerlere aktarmak veya kendi üzerinde sonlandırmak gibi saldırıların teorik olarak Kablosuz Örgü Ağları üzerinde gerçeklenebileceğini açıklamıştır.

İkinci çalışma ise [59], kablosuz örgü ağlarına dahil olmaya yetkisi olan bir kullanıcının, bulunduğu ağda yönlendirme ve ortam erişim parametrelerini manipüle ederek, ağı istismar etmeye yönelik bir çalışmadır. Yönlendirme protokollerinden HWMP, Ortam erişim parametrelerinde EDCA (Enhanced Distributed Channel

Access) ve MCCA (MCF Coordinated Channel Access) kavramları üzerinde odaklanılan bu çalışmada, yine bu kavramların açıklarına yönelik teorik arka planları verilerek nasıl istismar edileceğine dair bilgiler sunulmuştur.

Üçüncü çalışmada ise [58], Kablosuz Örgü ağlarına saldırı yapacak noktaların ağa erişimlerinin yetki veya yetkili olmayan durumlara göre sınıflandırarak analiz edilmiştir. Her iki durumda da 802.11s'in varsayılan yönlendirme protokolü olan HWMP'nin temel özelliklerini ele alarak, "Flooding", "Path Diversion", "Fake Path Metrik", "Wormhole ve Blackhole" ve "Impersonation" atakları anlatılmıştır. Bu çalışmada da atakların 802.11s ağlarında teorik olarak nasıl yapıldığından bahsedilmiştir. Sonrasında ise bu saldırı sistemlerine karşı özel bir yönlendirme protokolleri sunulmuştur.

Tezin ikinci kısmı için bu üç temel çalışma ele alındığında görülmüştür ki; 802.11s ağlarında, ağın temel bileşenleri kullanılarak çok sayıda saldırı yapılabilme imkanı mevcuttur. Fakat literatürde önerilen çalışmaların gerçek bir Wi-Fi Örgü Noktası ile 802.11s tabanlı kablosuz örgü ağını oluşturulup, bu ağa yönelik saldırıların pratik olarak gerçeklenmesinin literatürde geliştirilmeye açık bir alan olduğu görülmüştür. Bu nedenle tezin ikinci bölümünün amacı, 802.11s'e dair atakların test ortamı kurularak, saldırı gerçeklemelerinin yapılıp sonuçların elde edilmesi olacaktır.

3.3 802.11S KABLOSUZ ÖRGÜ AĞLARINA YÖNELİK SALDIRILAR

Bu kısım, 802.11s Kablosuz Örgü Ağlarına (Wireless Mesh Network) Yönelik saldırı tiplerine dair açıklamaları içermektedir.

802.11s Örgü Ağlarına öne çıkan üç tip saldırı şunlardır; Sahte Kimlik Doğrulama (Fake Mesh Authentication), Yol Saptırma (Path Diversion), Karadelik (Blackhole) saldırılarıdır.

Örgü Temel Servis Seti'ni oluşturmak için öncelikle tüm örgü noktalarının birbirini keşfetmesi gerekmektedir. Keşif aşamasının yürütülmesi için en önemli özellik, tüm örgü noktalarının tanımlayıcısı olan "Mesh ID" dir. Bir Örgü Temel Servis Setine katılan ağ istasyonları, kendi kimliklerini kullanarak ağa bilgilerini gönderir ve çoklu yayın çerçevelerine yanıt verir.

Sahte Kimlik Doğrulama Saldırısı, Kablosuz Örgü Ağlarında yetki kazanmaya yönelik herhangi bir ayrıcalığı olmayan ve ağa dahil olmayan bir saldırganın, örgü ağlarında kimlik doğrulama sürecinin temelinin oluşturan Örgü Değiş-Tokuş Yönetimi (Mesh Peering Management [51] sürecini hedef almasıyla beraber hedef örgü noktası ile yetkisiz bir şekilde kimlik doğrulamasını kapsayan saldırı tipidir. Öncelikle iki kablosuz ağ bileşenin (Wi-Fi radyo) birbirleriyle Örgü Ağı oluşturabilmesi için, Örgü Noktası olarak yapılandırılması gerekmektedir. Sonraki aşamada yapılandırıldıkları konfigürasyona özel olarak "Mesh ID" tanımlamalarının yapılması ve kablosuz ortamda bileşenlerin birbirlerini bu "ID" ile keşfetmesi gerekmektedir. Böylece Kimlik doğrulama aşamasını tanımlayacak Örgü Değiş-Tokuş Yönetim sürecine geçebilmektedirler [53].

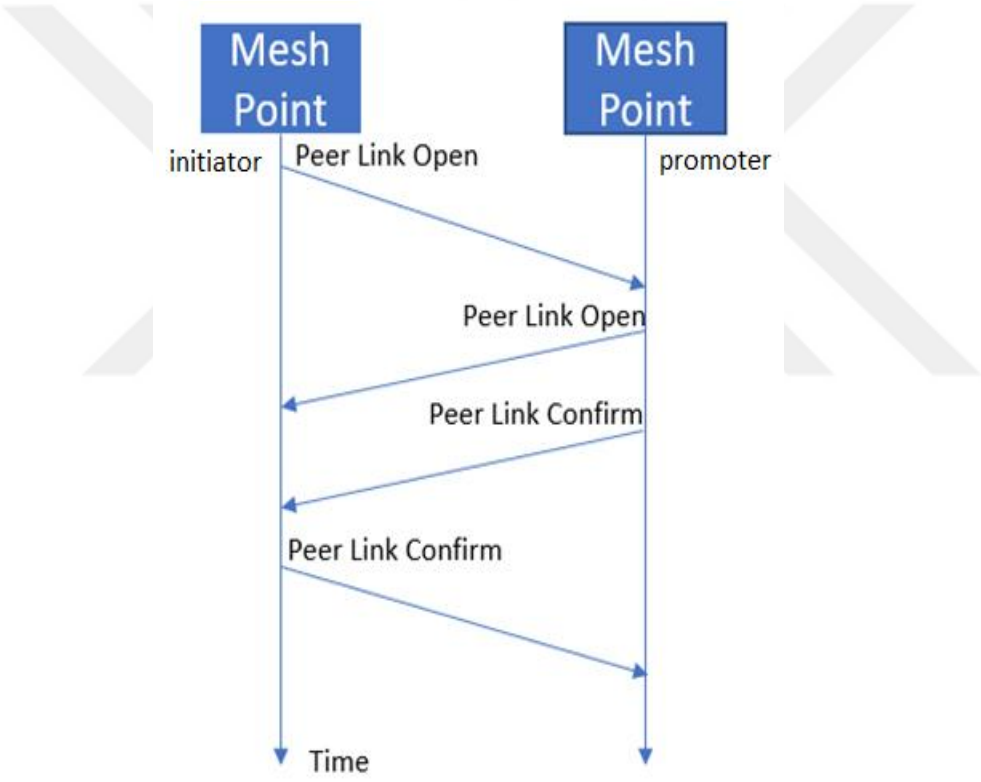
Örgü Değiş-Tokuş Yönetimi'de üç tip işlem kodu vardır. "Action" (eylem) çerçeve tipi altında bulunan işlem kodları aşağıda açıklanmıştır.

Örgü Değiş-Tokuş Açık (Mesh Peering Open): Keşfedilen Örgü Noktasına eşleme isteği sunmak için kullanılan, tek noktaya yayın çerçevesidir.

Örgü Değiş-Tokuş Onayı (Mesh Peering Confirm): Başlatıcı Örgü Noktasından eşleme isteğini kabul etmek için kullanılan tek noktaya yayın çerçevesidir.

Örgü Değiş-Tokuş Kapalı (Mesh Peering Close): Bir nedenden dolayı değiş-tokuşu sonlandırmak için kullanılan tek noktaya yayın çerçevesidir.

Başlatıcı (Initiator) ve destekleyici (promoter) iki örgü noktası arasında ideal bir senaryoda Örgü Değiş-Tokuş Yönetimi sürecinin akış şeması aşağıdaki şekilde gösterilmektedir.



Şekil 3.7: Örgü Değiş-Tokuş Yönetimi Sürecine Ait Akış Şeması

Şekil 3.7'de gösterilen akış şeması aşağıdaki gibi adım adım detaylandırılmıştır.

- Örgü Değiş-Tokuş Yönetimi süreci, herhangi bir Örgü Noktasının süreci tetiklemesiyle başlamaktadır.

- Süreci başlatan Örgü Noktası, "action" tipi ve "Mesh Peering Open" işlem kodlu olan çerçeveyi, destekleyici örgü noktasına gönderir. Çerçeve ayrıca IEEE 802.11 Kablosuz Yönetim başlığında "Kaynak MAC Adresi" (başlatıcının adresi), "Hedef MAC Adresi" (destekleyici Örgü Noktasının adresi) ve "Local Link ID" (başlatıcı Örgü Noktasının kimliği) bilgilerini içermektedir.

- Bir sonraki adımda destekleyici Örgü Noktası gelen çerçeveye aynı eylem tipi olan “Mesh Peering Open” ile yanıt verir. Bu çerçeve ayrıca "Kaynak MAC Adresi" (destekleyici Örgü Noktasının adresi), "Hedef MAC" (başlatıcı Örgü Noktasının adresi) ve "Local Link ID" (destekleyici Örgü Noktasının kimliği) bilgilerini içermektedir.

- Daha sonra, destekleyici Örgü Noktası, başlatıcı Örgü Noktasına “Mesh Peering Confirm” çerçevesi göndermekte ve kendi kimliğini bu çerçeveye bir "Local Link ID" ve başlatıcı Örgü Noktasının kimliğini "Peer Link ID" olarak koymaktadır.

- Son adımda, başlatıcı Örgü Noktasının ayrıca Örgü Değiş-Tokuş Yönetimi sekansını bitirmek için kendi kimliğini bir "Local Link ID" ve destekleyici Örgü Noktasının kimliğini "Peer Link ID" olarak koyarak destekleyici Örgü Noktasına “Mesh Peering Confirm” çerçevesi göndermektedir.

Bu aşamalarda bulunan “Local Link ID” ve “Peer Link ID” her kimlik doğrulama sürecinde rastgele oluşturmaktadır. Örgü Değiş-Tokuş Yönetimi sürecinin başarılı bir şekilde tamamlanmasıyla, iki Örgü Noktası birbirleri arasında kimlik doğrulayabilmektedir.

Bu bölümde tanımlanan Sahte Kimlik Doğrulama saldırısı ise, Örgü Değiş-Tokuş Yönetimi sürecini hedef alarak, süreci istismar eden etmeyi hedefleyen bir saldırı

tipidir. Saldırının temel prensibi, saldırganın Örgü Değiş-Tokuş Yönetimi sürecini, arkaplanına uygun olacak şekilde birebir taklit edilme esasına dayanmaktadır. Örgü noktası olarak tanımlanmadan ya da ekstra bir yetkiye sahip olmadan, istenen MAC adresi ile hedef Örgü Noktası, sahte bir şekilde kimlik doğrulamaktadır.

İkinci saldırı tipi olan Yol Saptırma, HWMP PREQ çerçevelerinin manipülasyonuna dayanmaktadır [59]. İki Örgü Noktası arasında herhangi bir veri trafiği geçtiğinde, ağda dinamik olarak yol tayini yapılabilmesi için, bu noktalar arası periyodik olarak HWMP çerçeveleri gönderilmektedir. Trafiği başlatan taraf ağa çoklu yayın çerçevesi tipinde sürekli olarak PREQ çerçeveleri gönderirken, ağda bu nokta ile iletişim kuran diğer Örgü Noktaları, gelen çoklu yayın çerçevelerine karşılık olarak metrik bilgilerini içeren PREP çerçeveleri gönderir. Metrik bilgisi, üzerinde trafik aktarılması için anlaşılan ilgili yol için hat kalitesini tanımlamaktadır [57]. Bu mesajlaşmanın ardından, her iki Örgü Noktası da, bu metrikleri içeren bilgileri yönlendirme tablolarında tutmakta ve bilgi yenilendikçe de güncellemektedir. Ayrıca herhangi bir HWMP çerçevesi gönderen Örgü Noktaları, bu çerçevelerin sekans numarası alanını da kullanarak, her bir çerçeve için artan sırada etiketleme işlemi yapmaktadır. Ağda aynı özellikteki çerçevelerden sekans numarası düşük olanlar, Örgü Noktalarınca işleme alınmamaktadır [53]. Hedef Örgü noktalarına Yol Saptırma saldırıları yapılarak, saldırı altındaki Örgü Noktasının yönlendirme tablosu, hedef Örgü Noktası için istenilen ölçüde farklılaştırılabilir. Böylelikle Örgü Noktasını ağdaki herhangi bir varış noktasını seçme süreci manipüle edilebilmektedir.

Tezin bu kısmı kapsamında konu alınan son saldırı ise Karadelik (Blackhole) saldırısıdır [58]. Karadelik saldırısı da Yol Saptırma saldırısında olduğu gibi HWMP PREQ paketlerinin manipüle edilmesi ilkesini esas almaktadır. Saldırının temel amacı, Hedef Örgü Noktasının yönlendirme tablosunun manipüle edilmesiyle beraber, ağ trafiğinin saldırganın üzerine alınması prensibine dayanmaktadır. Saldırgan ağa sahte PREP mesajlarıyla, en iyi metrik bilgisinin akabinde en kısa yolun kendisi üzerinden anahtarlanması gerektiğini ve ağdaki cihazların herhangi bir varış noktası için hep saldırganın adresini seçmesini hedefler. Saldırganın trafiği başarılı bir şekilde üzerine almasıyla beraber, ilgili trafiği hiçbir noktaya yönlendirmeyerek kendi üzerinde sonlandırır. Böylelikle ağ içerisinde birbirlerini hedefleyen cihazlar, saldırgan trafiği

üzerine alabildiği sürece birbirleriyle haberleşemezler ve saldırgan üzerinde bir karadelik oluşur.

3.4 GERÇEKLEME DÜZENEĞİ

Bu bölümde, tezin ikinci kapsamında yapılacak deneysel çalışmaların alt yapısını oluşturan tüm bileşenler sırasıyla anlatılmıştır. Ek olarak bu bileşenlerle oluşturulabilecek temel deney düzeneği gösterilmiştir.

Gerçekleme düzeneğinin bileşenlerinden olan USB Wi-Fi Adaptörü ve Saldırgan Bilgisayar Bölüm 2.4'te anlatılmıştır ve anlatılan özellikler kapsamında kullanılacaktır. Bunlara ek olarak aşağıda gerçekleme düzeneğini oluşturan diğer bileşenler gösterilmiştir.

Wi-Fi Örgü Noktası

Gerçekleme düzeneğinde kullanılan Wi-Fi Örgü Noktasının, Bölüm 2.4'te anlatılan Wi-Fi Erişim noktasından farklı olan tek özelliği, Wi-Fi Radyo modülünün bir Örgü Noktası olarak operasyon göstermesi için yapılandırılmış olmasıdır. Bu sayede, 802.11s Kablosuz Örgü Ağlarını oluşturarak gerçeklemelerde kullanılmıştır.

RF Zayıflatıcı

RF Zayıflatıcılar, sinyalin genlik seviyesini azaltmaya yarayan bileşenlerdir. Temel kullanım amacı, sistemleri işlenemeyecek kadar yüksek bir güç seviyesine sahip bir sinyale maruz bırakmaktan korumaktır. RF zayıflatıcılar değişken zayıflatma seviyelerine sahip olabilirler (10dB, 20dB zayıflatıcı vb.). Farklı zayıflatma seviyelerine sahip zayıflatıcılar kullanılarak Wi-Fi Radyolar arasındaki her RF bağlantısının kontrol edileceği ve ayarlanacağı kablosuz ağ topolojileri kurulabilmektedir. Bu şekilde, test ortamında istenilen yol ve metrik kombinasyonlarına sahip gerçek dünya topolojileri oluşturulabilmektedir.

RF Kablo

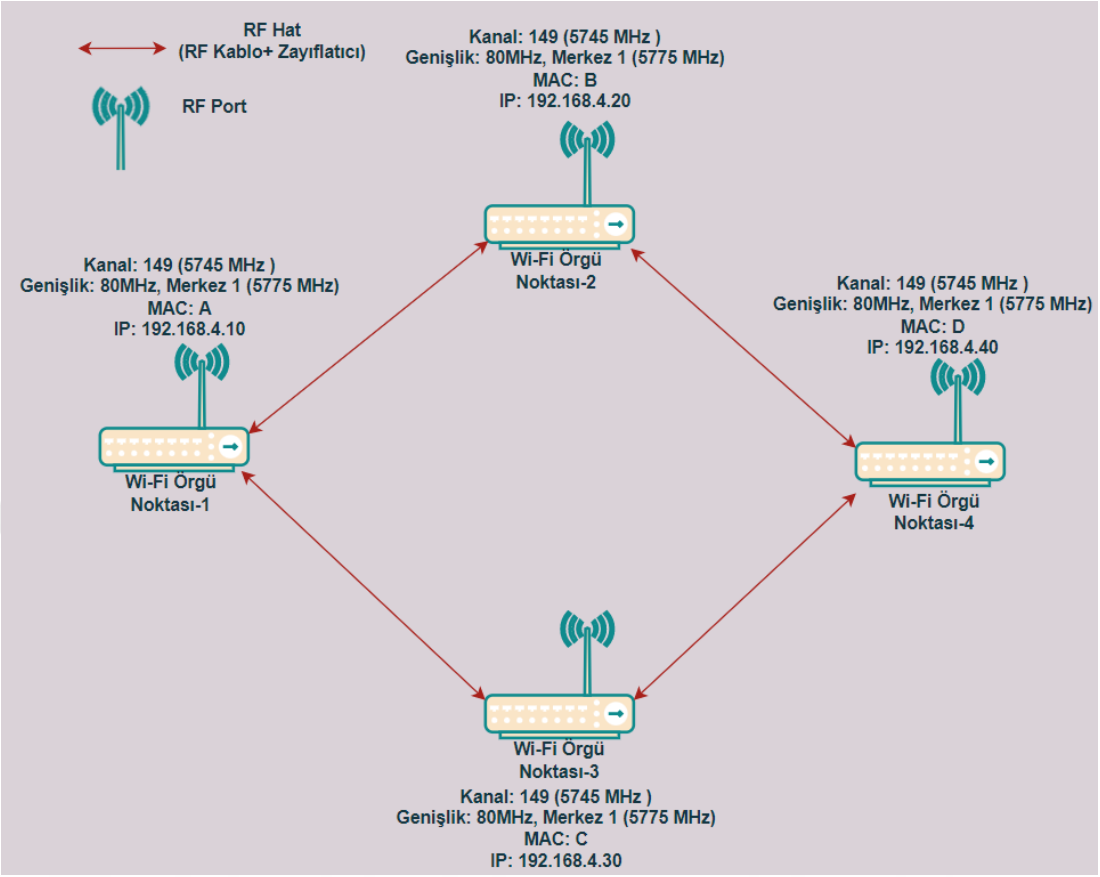
RF kabloları, radyo frekansı sinyalleri göndermek için kullanılan bir tür koaksiyel kablodur. Wi-Fi Cihazlarının RF portlarına takılabilir ve RF zayıflatıcılarla birleştirilebilir. Bu çalışmada, çeşitli RF bağlantılarına sahip Wi-Fi Örgü Noktalarını birbirine bağlamak için kullanılmışlardır.

Temel Deney Düzenekleri

Önceki bölümlerde açıklanan bileşenler yardımıyla 802.11ac tabanlı kablosuz deney ortamında çeşitli kablosuz ağ topolojileri oluşturulabilmektedir. Wi-Fi radyo modüllerinin Örgü Noktası olarak ayarlanabilir olmasıyla beraber, Wi-Fi Örgü Noktalarının birbirleriyle bağlantısını sağlanabilmektedir. 802.11s standardı ile uyumlu olan bağlantı ve ağda oluşan yapı Örgü Temel Servis Setini oluşturmaktadır.

Örgü Temel Servis Setindeki Wi-Fi Örgü Noktaları, çok sayıda yönlendirme ve atlama yeteneğine sahiptir. Önceki bölümde açıklanan HWMP protokolü ile yönlendirme ve atlama mekanizmalarının temelini sağlarlar. Yönlendirme kararlarını vermek için MAC adresleri kullanılmaktadır ve her cihazın birbirinden farklı fabrika varsayılan MAC adresi vardır. Ayrıca Wi-Fi donanımı üzerinde koşan işletim sistemi üzerinden cihazların her bir kablosuz arayüzüne IP ataması yapılabilmektedir. Radyo modüllerinin çalışacağı frekans ataması da işletim sistemi arayüzü üzerinden ayarlanabilmektedir.

Çalışmalar 802.11s ile oluşturulan Örgü Temel Servis Seti özelinde yapılacağı için hazırlanan örnek topolojiler bu yönde sınırlıdır. RF zayıflatıcılar ve RF kablolar sayesinde doğrudan ve dolaylı yolları içeren farklı topolojiler oluşturulabilmektedir. Günlük hayatımızda yer alan ticari ürünlerde gördüğü gibi, normal koşullar altında kablosuz cihazların, RF arayüzlerine anten bağlantısı yapılarak kullanılmaları beklenmektedir. Fakat test ortamında kablosuz bağlantıların sinyal gücünün hassas bir şekilde ayarlanması ve istenilen topolojilerin kolaylıkla hazırlanması için RF bileşenler kullanılmaktadır. Aksi takdirde bu topolojileri hazırlayabilmek ve kontrollü deneyler yapabilmek için cihazlar arasında kapsama alanlarını aşması adına çok fazla mesafe bırakılması gerekmekte, kontrollü deney yapabilme yeteneği de bir o kadar azalmaktadır. Şekil 3.8, deney ortamında çalışmaların önemli bir kısmında kullanılan kapsamlı bir Kablosuz Örgü Ağı topoloji örneğini göstermektedir.



Şekil 3.8: Deney Düzeneğinde Wi-Fi Örgü Noktalarıyla Oluşturulan Örnek Kablosuz Örgü Ağı Topolojisi

Wi-Fi Örgü Noktaları arasında, Wi-Fi Örgü Noktası-1 ile Örgü Noktası-4 arası doğrudan olmayan bir bağlantıyı içeren topoloji görülmektedir. Ek olarak bu noktalar, Wi-Fi Örgü Noktası-2 ve Wi-Fi Örgü Noktası-3 ile doğrudan bir bağlantı kurmaktadır. Wi-Fi Örgü Noktası-1 ile Wi-Fi Örgü Noktası-4 arasındaki hat üzerinde seçilecek yol, bu noktalar arasındaki bulunun diğer bileşenlerle aralarındaki hat kalitesine göre seçilmektedir.

3.5 SALDIRI GERÇEKLEMERİ VE ELDE EDİLEN SONUÇLAR

Bu bölüm, çalışmanın temelini oluşturan ve Bölüm 3.3'te anlatılan saldırıların gerçekleme aşamalarını anlatmakta ve gerçeklemelerin ardından elde edilen sonuçları göstermektedir.

Saldırıların uygulanmasının temelini, gerçeklemeler için özel olarak tasarlanan saldırı yazılımları oluşturmaktadır. Saldırı yazılımları Python [32] programlama dili kullanılarak oluşturulmuştur. Çerçeve yönetimi ve analizi işlemleri için Tshark [60], Python sarıcısı(wrapper) olan ve Wireshark disektörleri kullanılarak Python paket ayrıştırmasına izin veren Pyshark kütüphanesi kullanılmaktadır. Bir diğer önemli kütüphane ise, çerçeveleri oluşturmak ve hedef ağa enjekte etmek için kullanılan Scapy'dir [61]. USB Wi-Fi Adaptör'ün saldırı paketlerini ağa aktarabilmesi için doğru sürücü ile sürülmesi gerekmektedir. Piyasa kullanım amacı özel oluşturulmuş saldırı betikleri ile ağ saldırıları uygulamak olmayan USB Wi-Fi adaptör, paket enjekte etmek için tersine mühendislik yöntemleriyle oluşturulmuş sürücü ile yapılandırılmıştır [62].

Ek olarak, deney ortamındaki Wi-Fi Örgü Noktalarının operasyon frekansı 149. Kanal (Merkez Frekans: 5745, Kanal Genişliği: 80MHz) olarak yapılandırılarak kullanılmıştır. Ağda bulunan tüm örgü ağlarının IP yapılandırılması, aynı alt ağda olacak şekilde ayarlanmış ve ağdaki tüm "Mesh ID" bilgileri aynı olacak şekilde seçilmiştir.

3.5.1 Tehdit Modelleme

Aşağıda Bölüm 2.5.1'de tanımı verilen tehdit modelleme süreci kapsamında, tezin bu bölümü için genel bir açıklama yapılmıştır.

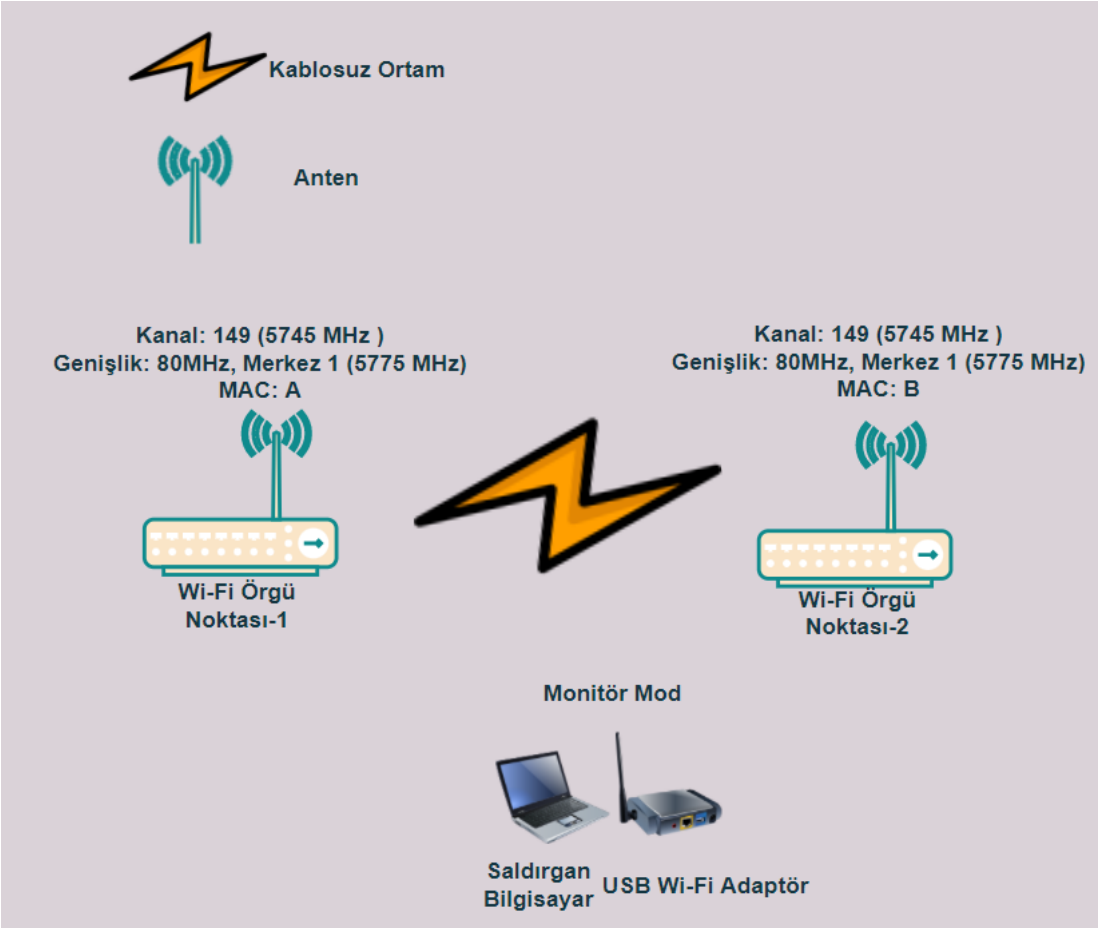
İlerleyen bölümlerde detayları anlatılan Sahte Kimlik Doğrulama, Yol Saptırma ve Karadelik saldırılarının gerçekleyebilmenin temeli Kablosuz Örgü Ağını oluşturan Örgü Noktalarının, Örgü Değiş-Tokuş Yönetimi ve varsayılan yönlendirme protokolü olan HWMP'nin temel prensiplerinin manipülasyonuyla mümkün olmaktadır.

Tez çalışmasının bu bölümünde Örgü Noktalarının oluşturduğu yerel alan ağ topolojisi üzerinde çalışmalar yapılmıştır. Başarılı saldırı sonucunda saldırgan, Örgü Noktalarıyla kimlik doğrulayabilmekte, ağ trafiğinin akışını değiştirebilmekte ve ağ trafiğini sonlandırabilmektedir. Bu çalışmada saldırgan sadece yerel alan ağında bulunan Örgü Noktalarına kayıtlanıp, veri iletimi yapabilmektedir. Fakat saldırgan, saldırı altındaki Örgü Noktalarının kablolu veya kablosuz arayüzleri vasıtasıyla doğru yapılandırma sonucunda iletişim halinde olabileceği diğer yerel ve geniş alanlar üzerinde yetkilendirilmiş diğer Örgü Noktalarının veya onlarla iletişim kuracak terminallerin erişebileceği her ağ noktasına erişebilip saldırı yüzeyini ve potansiyelini genişletebilmektedir.

Kablosuz Örgü Ağlarında, yukarıda anlatılan Örgü Değiş-Tokuş ve HWMP çerçevelerinin saldırgan tarafından yapılacak manipülasyonundan korunmak için Örgü Noktaları arasında "Kimliği Doğrulanmış Örgü Değiş-Tokuşu" (Authenticated Mesh Peering Exchange-AMPE) eşleşme modu kullanılabilmektedir. Bu güvenli değiş-tokuş modunun temelini, Örgü Noktaları arasında kullanılan SAE (Simultaneous Authentication of Equals) şifreleme yöntemi oluşturmaktadır [63]. Başarılı el sıkışmanın ardında değiş-tokuş ve HWMP çerçeveleri ağda şifreli şekilde yol almakta, çerçeve dinleme ve taklit etme süreçlerine karşı dayanıklı hale gelmektedir. Bir diğer korunma yöntemi ise Temel Servis Seti mimarisinde yapılan ile benzer olarak; ağa herhangi bir Örgü Noktası ile entegre bir şekilde çalışan Kimlik Doğrulama Sunucusu konumlandırarak, ağa erişim sağlayacak herhangi bir Örgü Noktasını yetkilendirilebilmek için kimlik bilgisi ve parola gibi bilgilerinin kullanıldığı bir güvenlik mekanizması kullanmaktır.

3.5.2 Sahte Kimlik Doğrulama Saldırısının Gerçeklenmesi

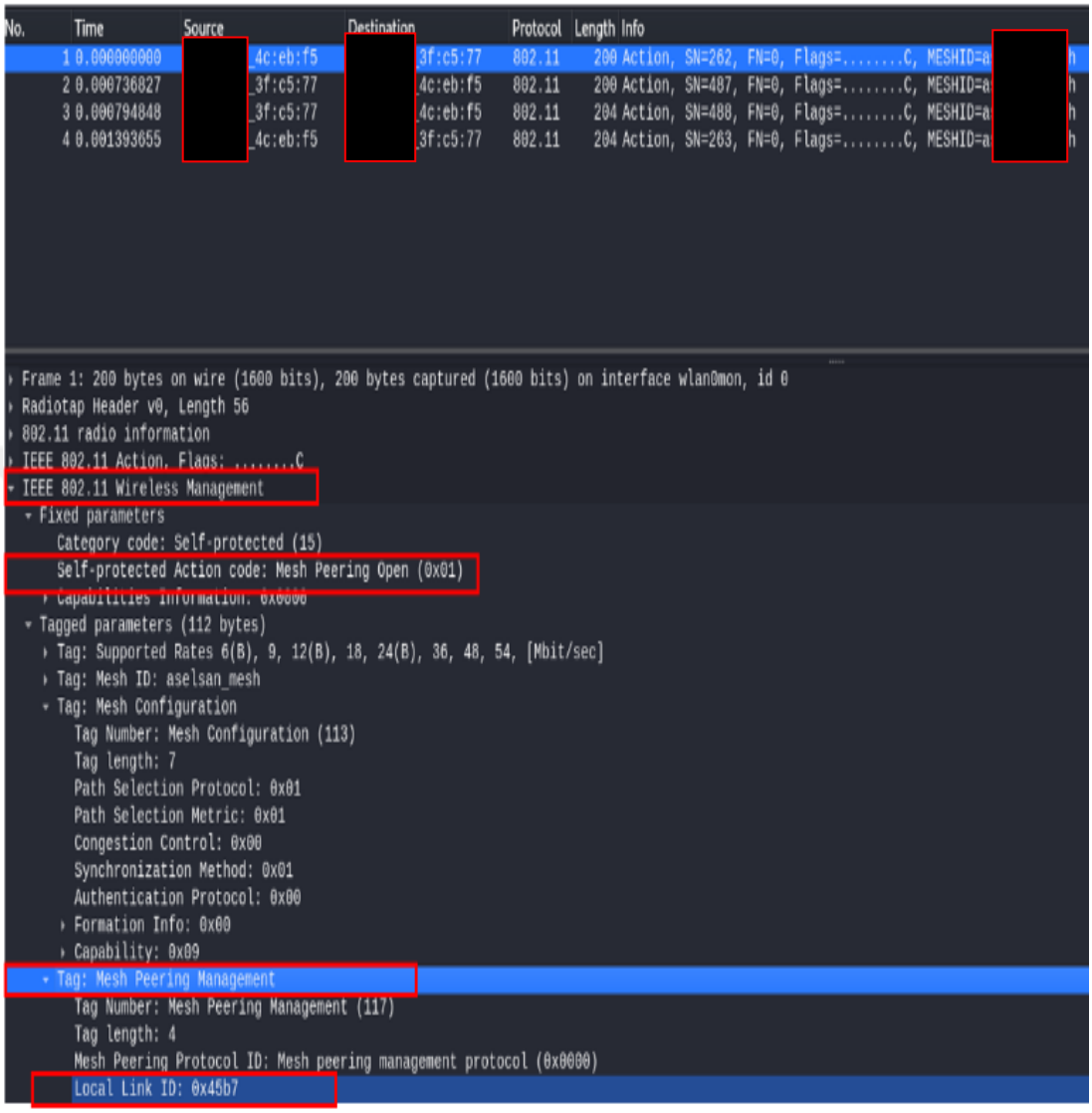
Sahte Kimlik Doğrulama saldırısının gerçeklenmesinin temeli, kimlik doğrulama sürecinin uygun bir şekilde taklit edilmesiyle gerçekleştiği için, öncelikle iki Örgü Noktası arası, Örgü Değiş-Tokuş Yönetim sürecine dair trafik analizi yapılmıştır. Analizi yapılması istenen trafiğin elde edilebilmesi için deney ortamda kurulan topoloji aşağıdaki şekilde gösterilmiştir.



Şekil 3.9: Deney Düzeneğinde Kimlik Doğrulama Sürecinin Dinlenmesi ve Kayıt Altına Alınması İçin Oluşturulan Topoloji

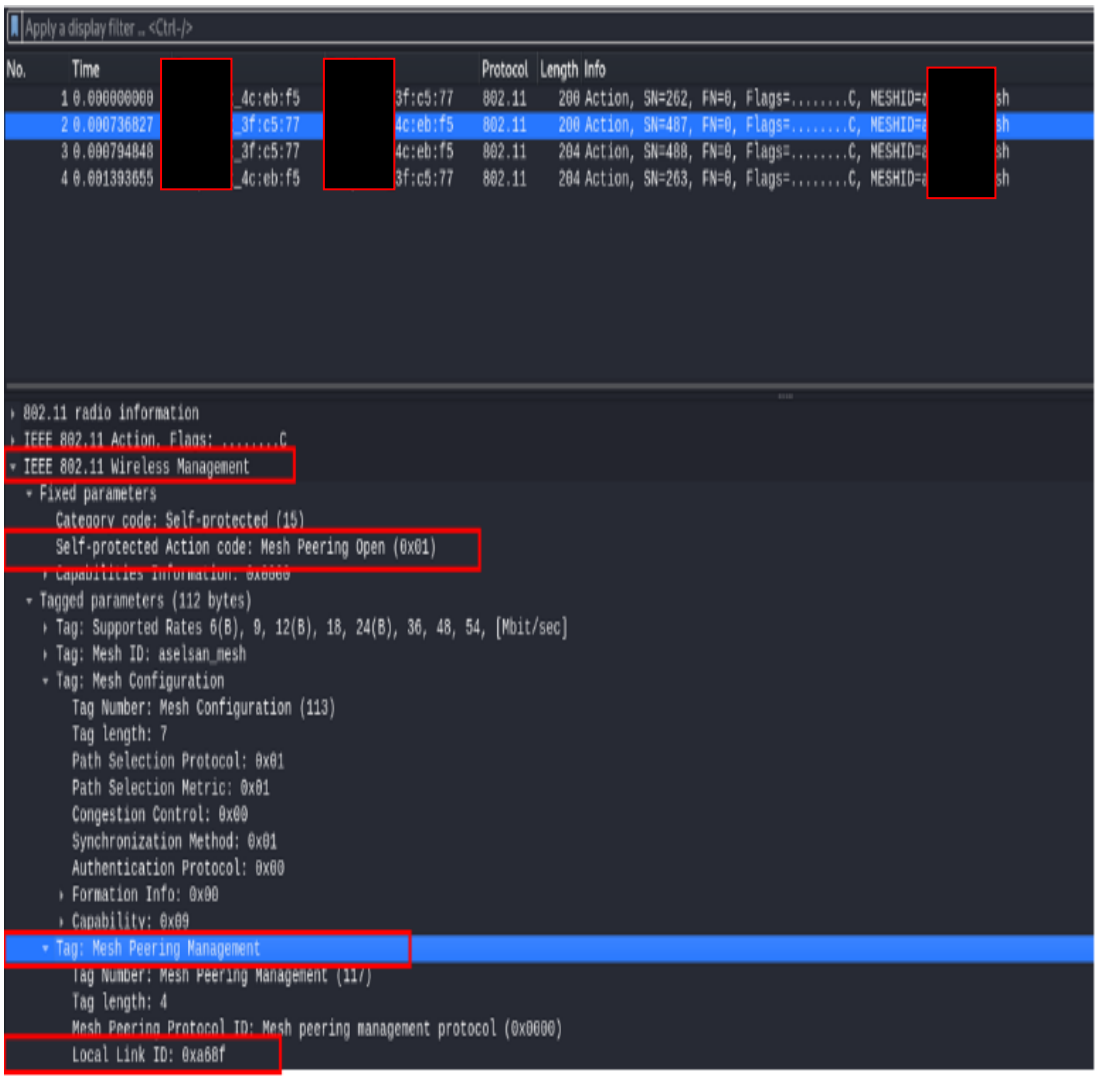
Kablosuz arayüz olarak USB Wi-Fi Adaptörün monitör modda kullanıldığı saldırgan bilgisayar üzerinde çalıştırılan "airmon-ng" aracı ile 802.11ac'nin kapsadığı 5 GHz frekans bandında kanallar arası ağ aktivitesi taranmaya başlanır ve aktivitenin olduğu frekans bandı tespit edilir. USB Wi-Fi adaptör, aktivitenin tespit edildiğini frekans bandına uyumlanır (tune) ve ilgili frekansta bulunan Örgü Noktalarına dair MAC adres bilgileri elde edilir. Frekans bandı belirlendikten sonra, Wi-Fi Örgü noktaları arası Kimlik Doğrulama sürecinin başlaması gerekmektedir. Fakat birbirleriyle daha öncesinde kimlik doğrulamış Örgü Noktaları, ağda bir sebepten ötürü iletişimini kaybetmezler ise kimlik doğrulama süreci tekrarlanmamaktadır. Bu nedenle, aşama gereği Örgü Noktalarına radyo modüllerine işletim sistemi üzerinden "yeniden başlat" komutu gönderilmiştir. Sonrasında çerçeve dinleme işlemine devam edilmiştir. Böylelikle, Wireshark aracılığıyla yakalanan Örgü Değiş-Tokuş Yönetim sürecine dair tüm çerçeveler aşağıda sırasıyla gösterilmiştir.

Şekil 3.10'da başlatıcı Örgü Noktası, destekleyici örgü noktasına gönderdiği "Mesh Peering Open" işlem kodlu çerçeve gösterilmiştir.



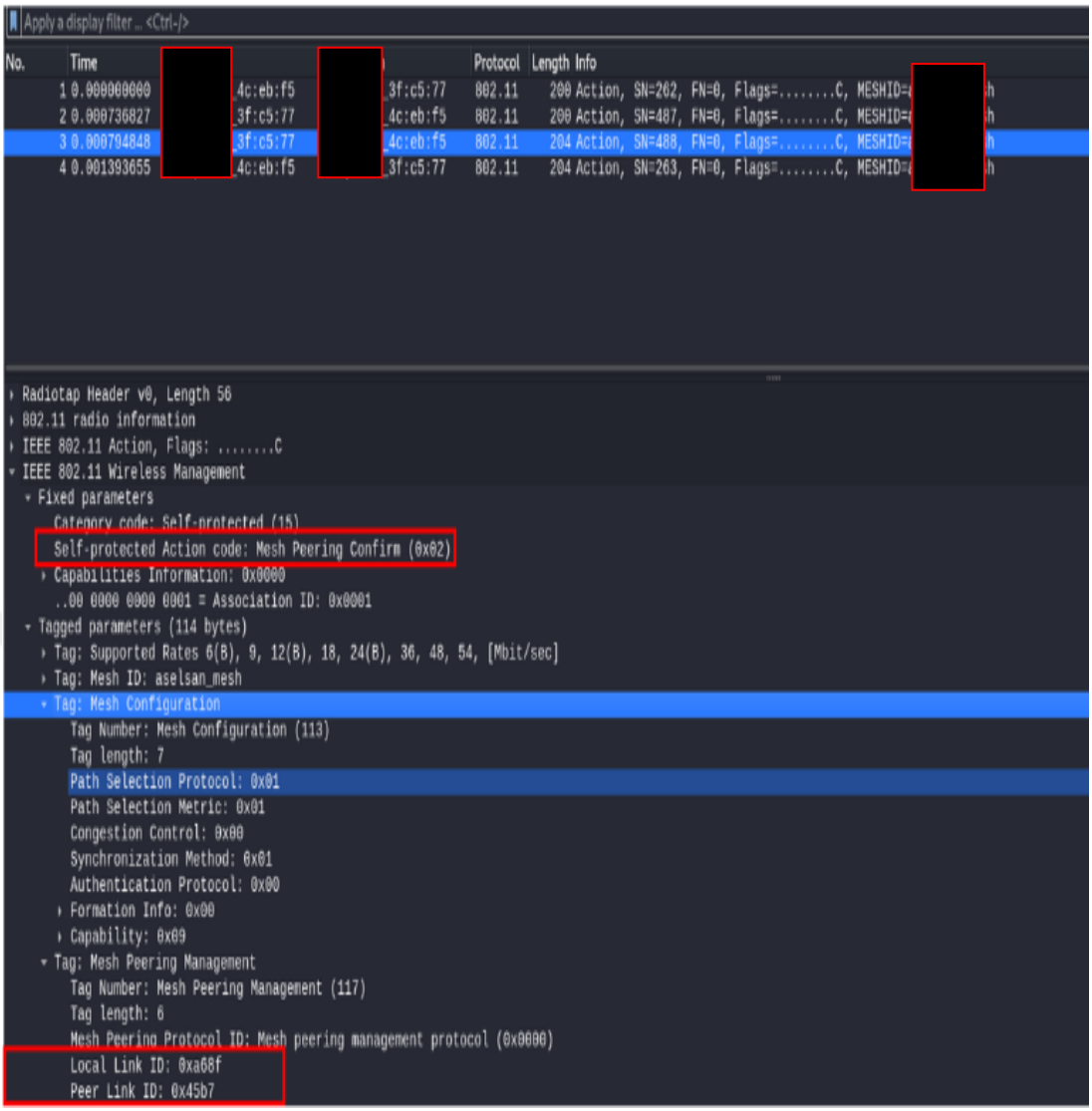
Şekil 3.10: Örgü Değiş-Tokuş Yönetimi Sekansında Yakalanan Çerçeve-1 (Mesh Peering Open)

Şekil 3.11'de destekleyici Örgü Noktasının süreci devam ettirdiğine dair çerçeve gösterilmiştir.



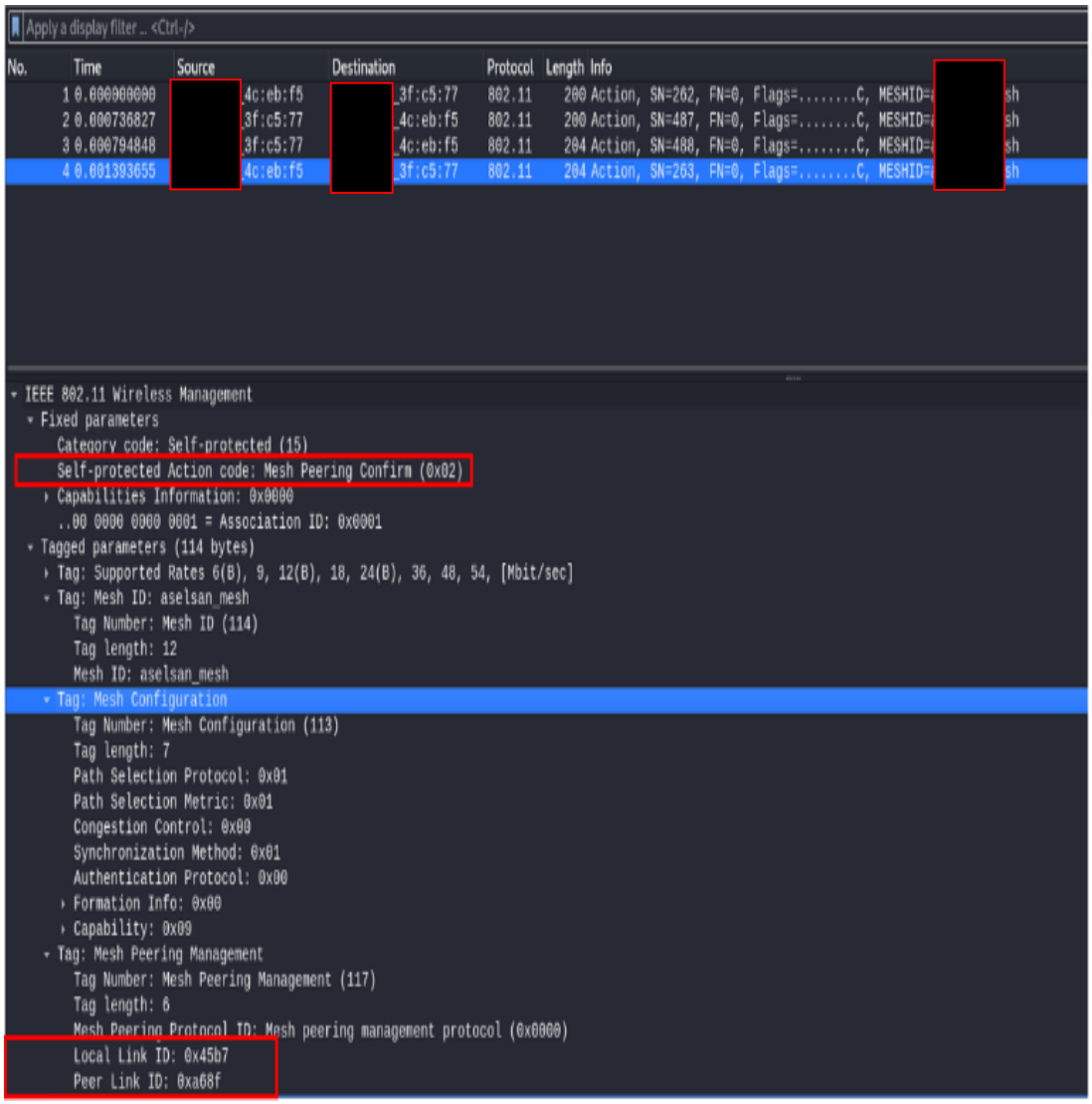
Şekil 3.11: Örgü Değiş-Tokuş Yönetimi Sekansında Yakalanan Çerçeve-2 (Mesh Peering Open)

Şekil 3.12'de destekleyici örgü noktasının Mesh Peering Confirm çerçevesini gönderdiği gösterilmiştir.



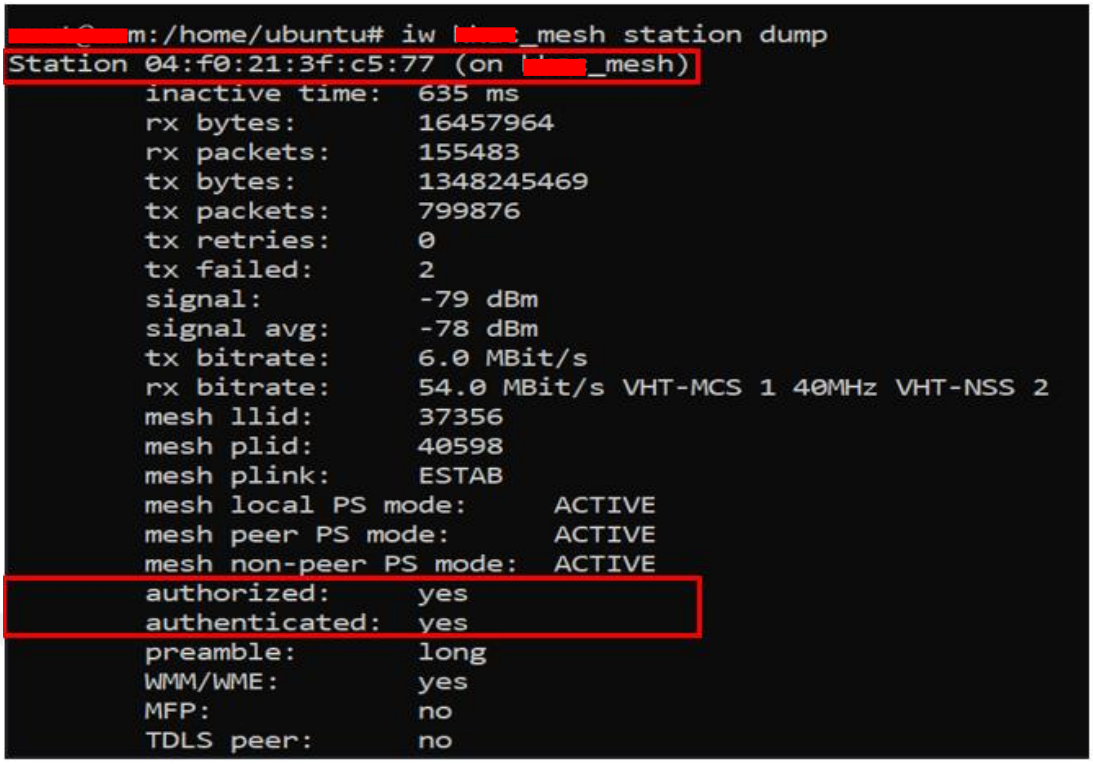
Şekil 3.12: Örgü Değiş-Tokuş Yönetimi Sekansında Yakalanan Çerçeve-3 (Mesh Peering Confirm)

Şekil 3.13'de son aşama olan başlatan Örgü Noktası ile diğer Örgü Noktası arasındaki süreci sonlandıran Mesh Peering Confirm çerçeveleri gösterilmiştir.



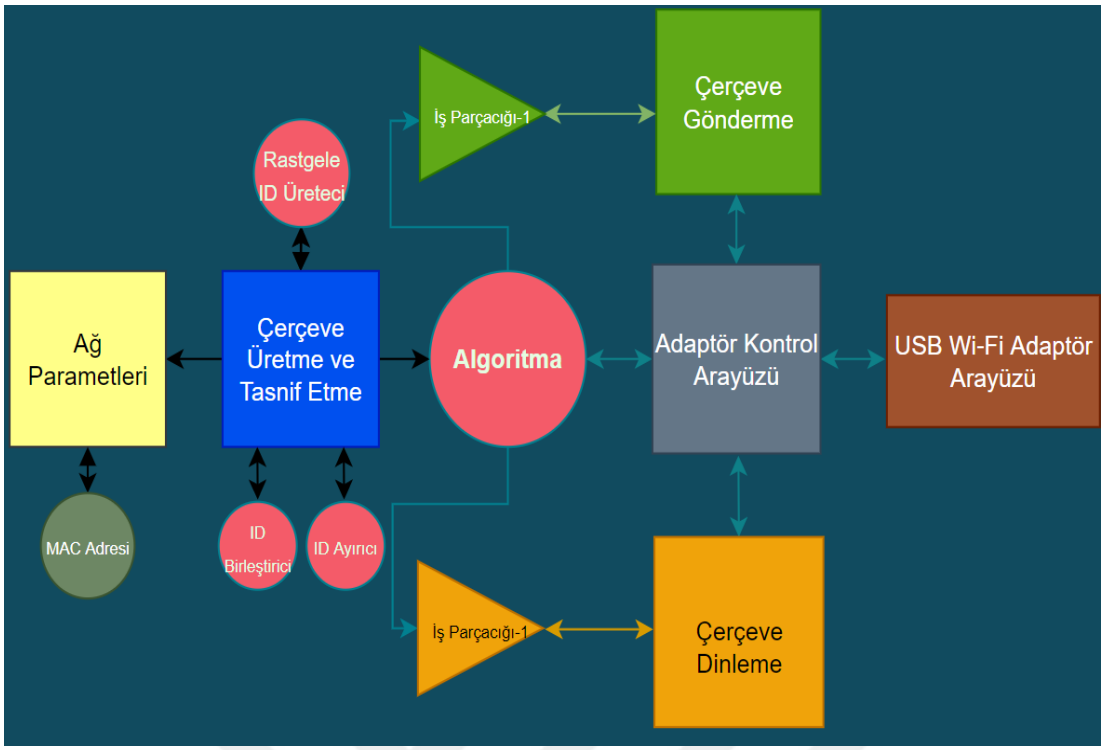
Şekil 3.13: Örgü Değiş-Tokuş Yönetimi Sekansında Yakalanan Çerçeve-4 (Mesh Peering Confirm)

Bu sürecin ardından, Örgü Noktalarının birbirleriyle başarılı bir şekilde kimlik doğrulaması yaptığının kontrolü için herhangi Örgü Noktasının çalıştığı işletim sisteminin "debug" arayüzü kullanılmıştır. Bu arayüz üzerinden "iw *mesh_interface* station dump" komutu çalıştırılarak birbirine bağlı olan istasyonların bilgileri alınmaktadır.



Şekil 3.14: İşletim Sistemi Debug Arayüzünden Örgü Noktalarının Kimlik Doğrulama Bilgilerine Ait Çıktı

Örgü Değiş-Tokuş Yönetim süreci ve bu süreçten elde edilen trafik bilgilerinin ışığında, Sahte Kimlik Doğrulama saldırısı yapabilmek adına bir saldırı yazılım mimarisi oluşturulmuştur. Mimarinin ana bileşenleri Şekil 3.15'te gösterilmiştir.



Şekil 3.15: Bu Çalışma Kapsamında Oluşturulan Sahte Kimlik Doğrulama Saldırısı Yazılım Mimarisi

Saldırı yazılımının tüm bileşenleri "Algoritma" bloğu üzerinden yönetilmektedir. Saldırı yapılacak hedef MAC adresi bilgileri dışarıdan bir parametre olarak sisteme verilmekte ve Ağ Parametreleri bloğu tarafından işlenmektedir.

Ağ parametrelerine uygun olarak çerçeve üretme ve dinlenen çerçeveleri tasnif etmek için "Çerçeve Üretme ve Tasnif Etme" bloğu oluşturulmuştur.

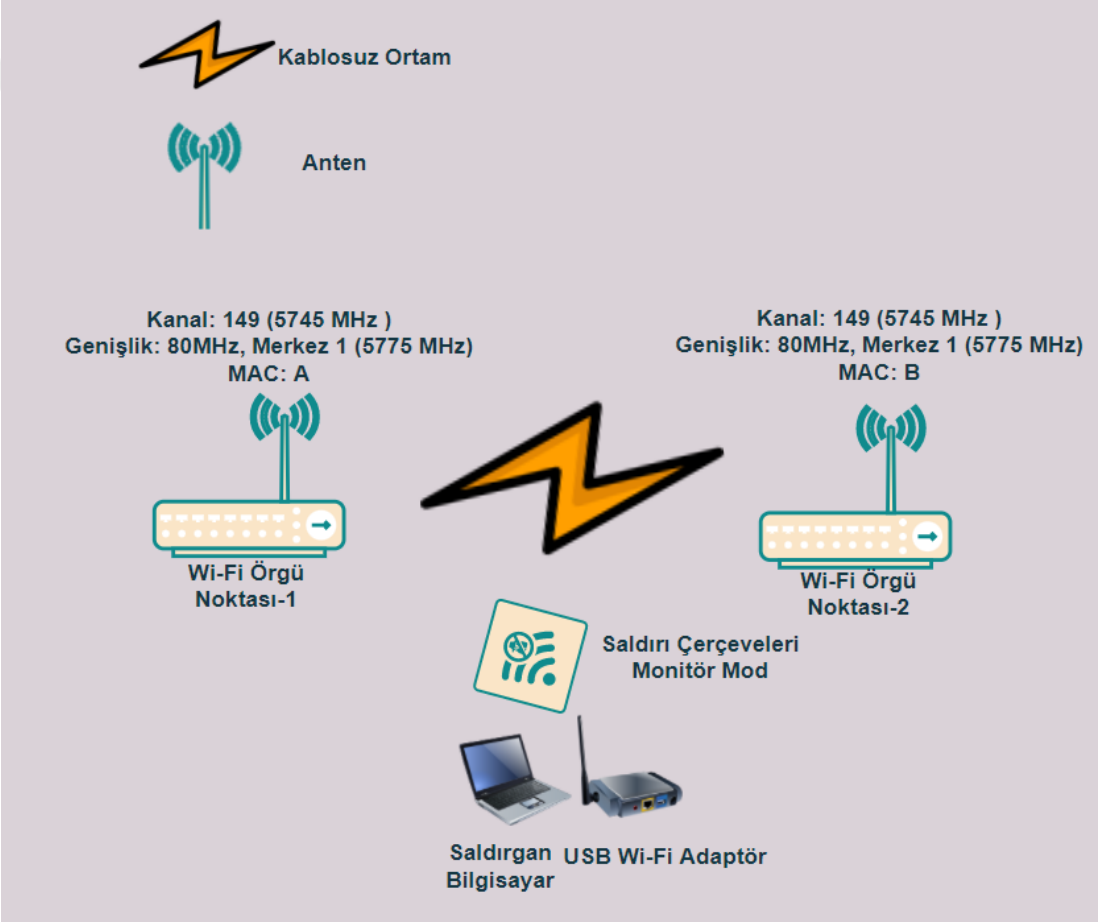
Sahte kimlik doğrulama saldırısında, Örgü Değiş-Tokuş çerçevelerini göndermek ve dinlemek için ayrı bloklar oluşturulmuştur. Bu bloklar iş parçacıkları (thread[3]) mekanizmasıyla, işlemler eş zamanlı olarak gerçekleştirilmektedir. Eş zamanlı işleme kararının sebebi, Kimlik Doğrulama süreci başladığında, bir Örgü Noktası belli bir zaman kadar gönderdiği çerçevelere cevap alamadığı takdirde, "Mesh Peering Close" çerçevesiyle beraber süreci sonlandırmaktadır. Bu nedenle çerçeve gönderirken, aynı

[3] Thread mekanizması, bir işlem zamanında tamamlanacak işin, aynı işlem zamanı içerisinde farklı kaynaklara ayrılarak paralel olarak yapılmasına denmektedir.

zamanda da dinleme modunu açık tutarak çerçeveler arası zaman aşımı bariyerine takılmamak amaçlanmıştır.

“Adaptör Kontrol Arayüzü” ise; Algoritma bloğunun takip ettiği işlemlerin sonunda çerçeveleri USB Wi-Fi Adaptöre göndermek ya da USB Wi-Fi adaptörden ilgili bilgileri almak için oluşturulan bloktur.

Bu aşama sonucunda ilgili sürecin temellerini kullanarak saldırıyı uygulamak için aşağıdaki şekilde gösterilen topoloji oluşturulmuştur.



Şekil 3.16: Deney Düzeneğinde Sahte Kimlik Doğrulama Saldırısının Yapılması İçin Oluşturulmuş Ağ Topolojisi

Kurulan bu topoloji ile birlikte, Saldırgan Bilgisayar üzerinde çalışan saldırı yazılımı, USB Wi-Fi adaptörü aracılığıyla istenilen Örgü Noktasını hedef alarak başlatılır. Saldırı adımları aşağıda sırasıyla maddeler halinde gösterilmiştir.

- “Ağ Parametreleri” bloğuna, hedeflenen MAC adresi bilgisi parametre olarak verilir.

- “Rastgele ID Üreteci” alt bloğu, saldırı için rastgele oluşturulmuş bir “Local Link ID” yaratır.

- “Paket Üretme ve Tasnif Etme” bloğu, parametre olarak girilen MAC adres ve “Local Link ID” bilgilerini, trafik analizi sırasında kaydedilen “Mesh Peering Open” taslak çerçevesini kullanarak oluşturulmuş yeni bir “Mesh Peering Open” çerçevesine ekler.

- “İş parçacığı-1” ve “iş parçacığı-2”, “Çerçeve Gönderme” ve “Çerçeve Dinleme” bloklarını paralel şekilde çalışma moduna geçirir. Aynı zamanda “Algoritma” birimi de Adaptör Kontrol Arayüzünü çerçeve göndermek için aktif hale getirir.

- “İş parçacığı-1” üretilen çerçeveyi, “Çerçeve Gönderme” bloğu vasıtasıyla hedef Örgü Noktasına iletmek için USB Wi-Fi Adaptör arayüzüne gönderir.

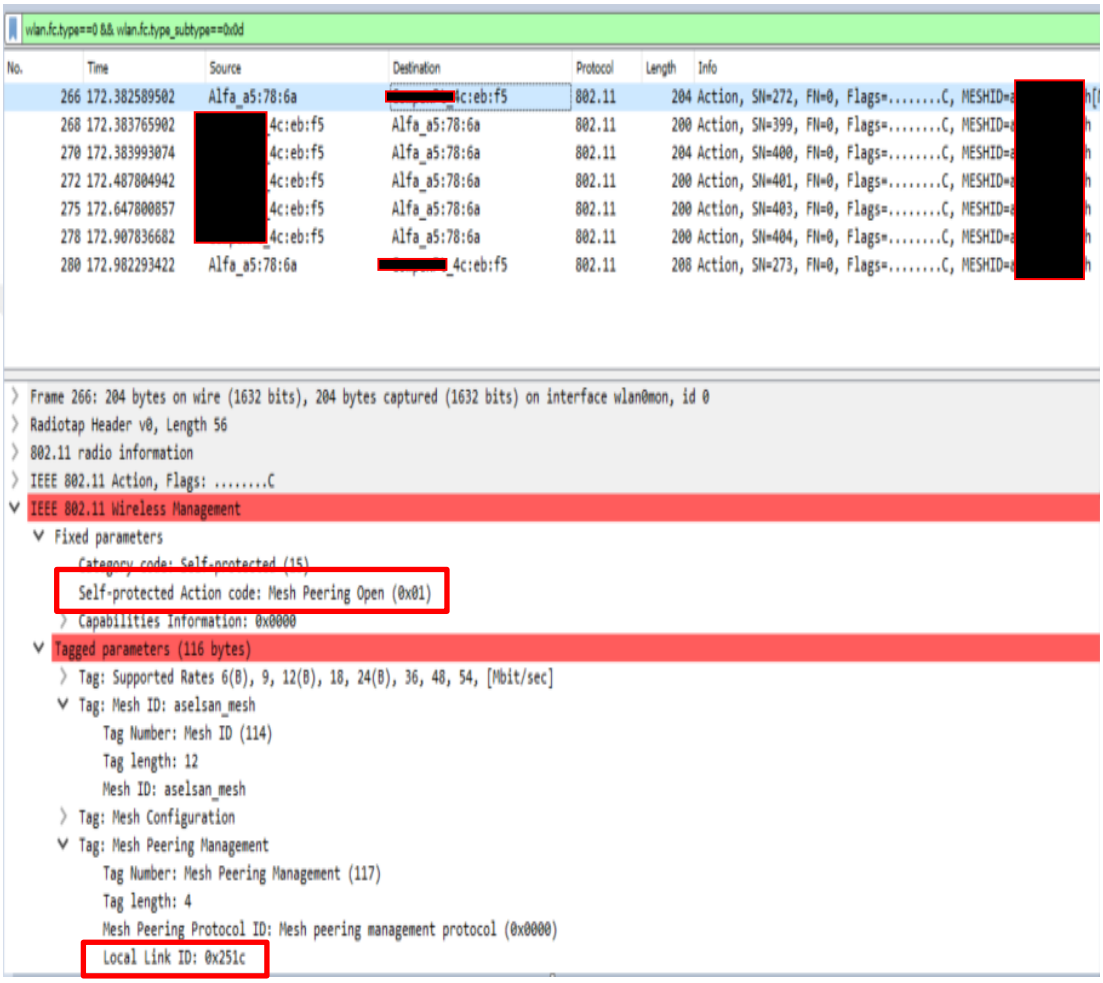
- Hedef örgü noktasından cevap olarak alınan iki adet çerçeve (Mesh Peering Open ve Mesh Peering Confirm), “Çerçeve Dinleme” bloğu üzerinden “Paket Üretme ve Tasnif Etme” bloğuna gönderilir. “ID Ayırıcı” bloğu dinlenen çerçevelerdeki Örgü Noktasına ait “Lokal Link ID” bilgisini elde eder.

- Hedef Örgü Noktasına ilişkin ID ve saldırı sırasında üretilen ID bilgileri, “ID birleştirici” alt bloğu sayesinde, üretilen Mesh Peering Confirm çerçevesinin içine eklenir.

- Oluşturulan çerçeve, İş Parçacığı-1 vasıtasıyla “Çerçeve Gönderme” bloğu üzerinden, USB Wi-Fi Adaptör arayüzüne gönderilir.

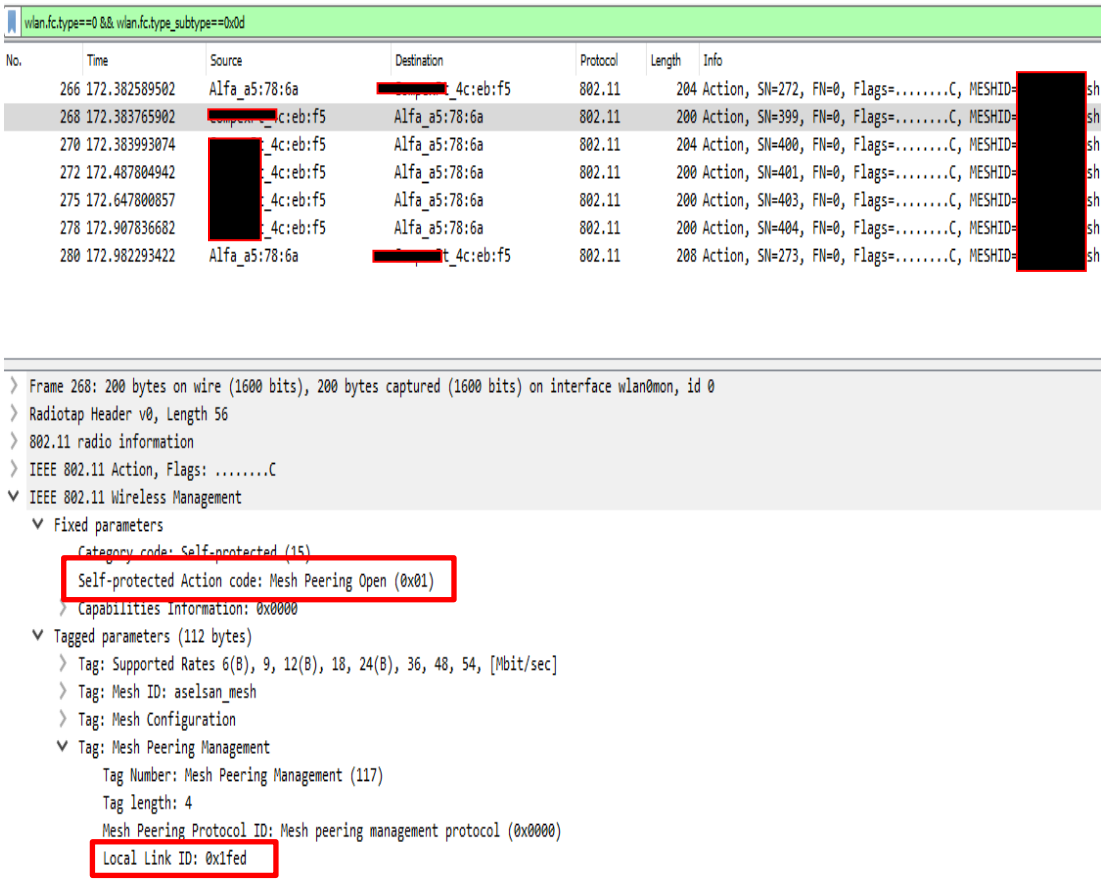
Başarılı saldırı sürecinden sonra, USB Wi-Fi Adaptör ile bir Örgü Noktası sahte bir şekilde kimlik doğrulaması yapabilmektedir.

Şekil 3.17'de USB Wi-Fi Adaptör ile hedef Örgü Noktası arasındaki süreci başlatan Mesh Peering Open çerçevesi gösterilmiştir.



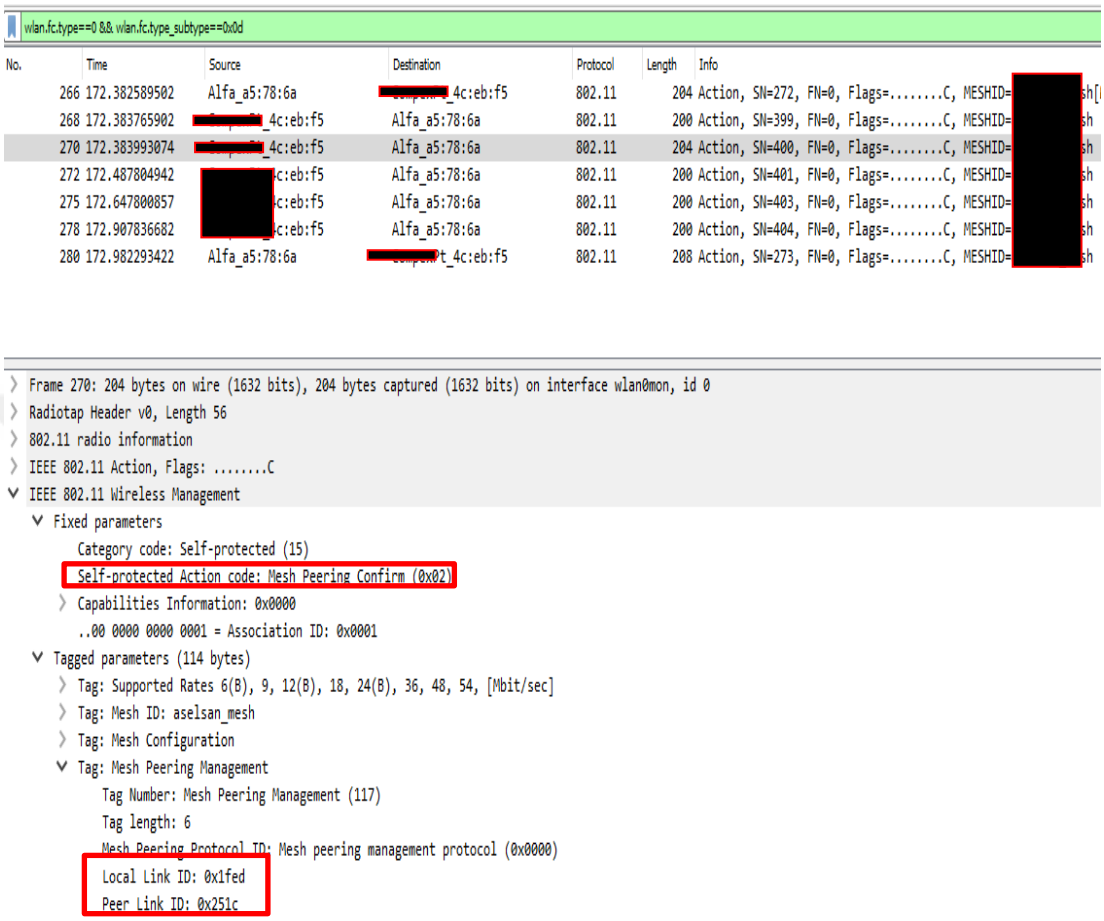
Şekil 3.17: Sahte Kimlik Doğrulama Saldırısında Örgü Değiş-Tokuş Yönetimi Sürecinde Yakalanan Çerçeve-1 (Mesh Peering Open)

Şekil 3.18'de hedef Örgü Noktası ile USB Wi-Fi Adaptör arasındaki süreci devam ettiren Mesh Peering Open çerçevesi gösterilmiştir.



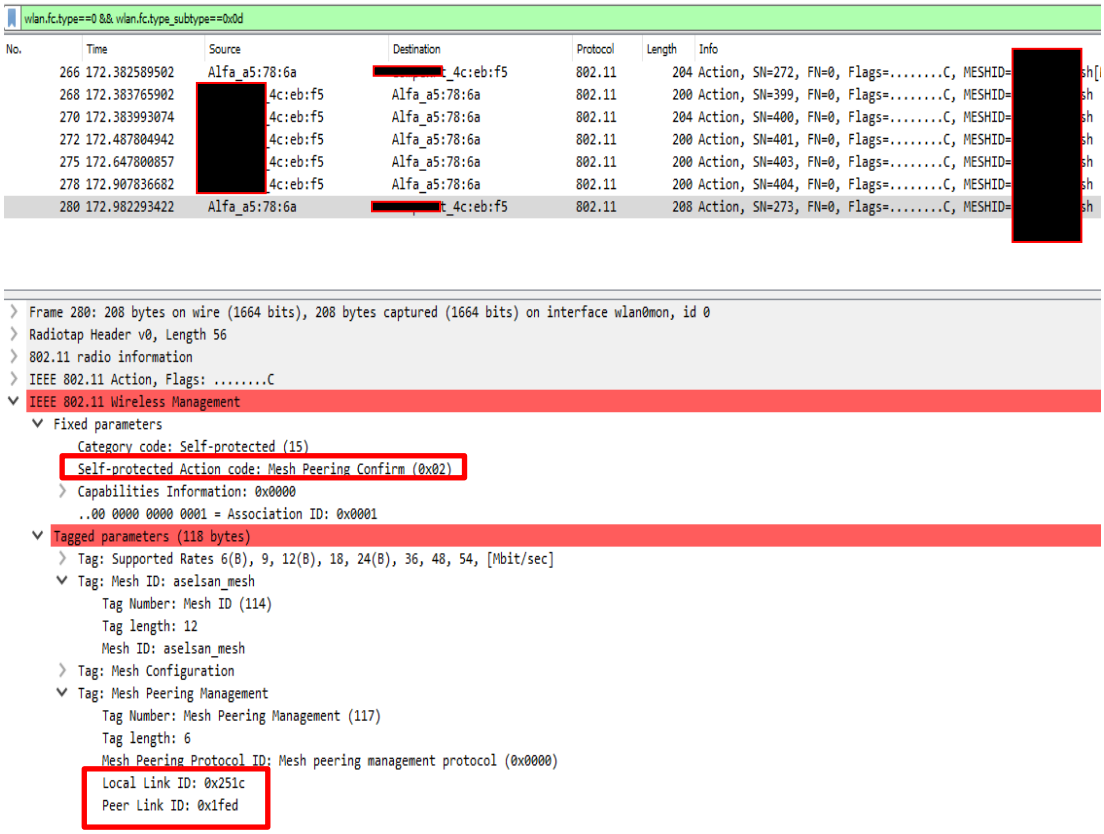
Şekil 3.18: Sahte Kimlik Doğrulama Saldırısında Örgü Değiş-Tokuş Yönetimi Sürecinde Yakalanan Çerçeve-2 (Mesh Peering Open)

Şekil 3.19'da hedef Örgü Noktası ile USB Wi-Fi Adaptör arasındaki süreci devam ettiren Mesh Peering Confirm çerçevesi gösterilmiştir.



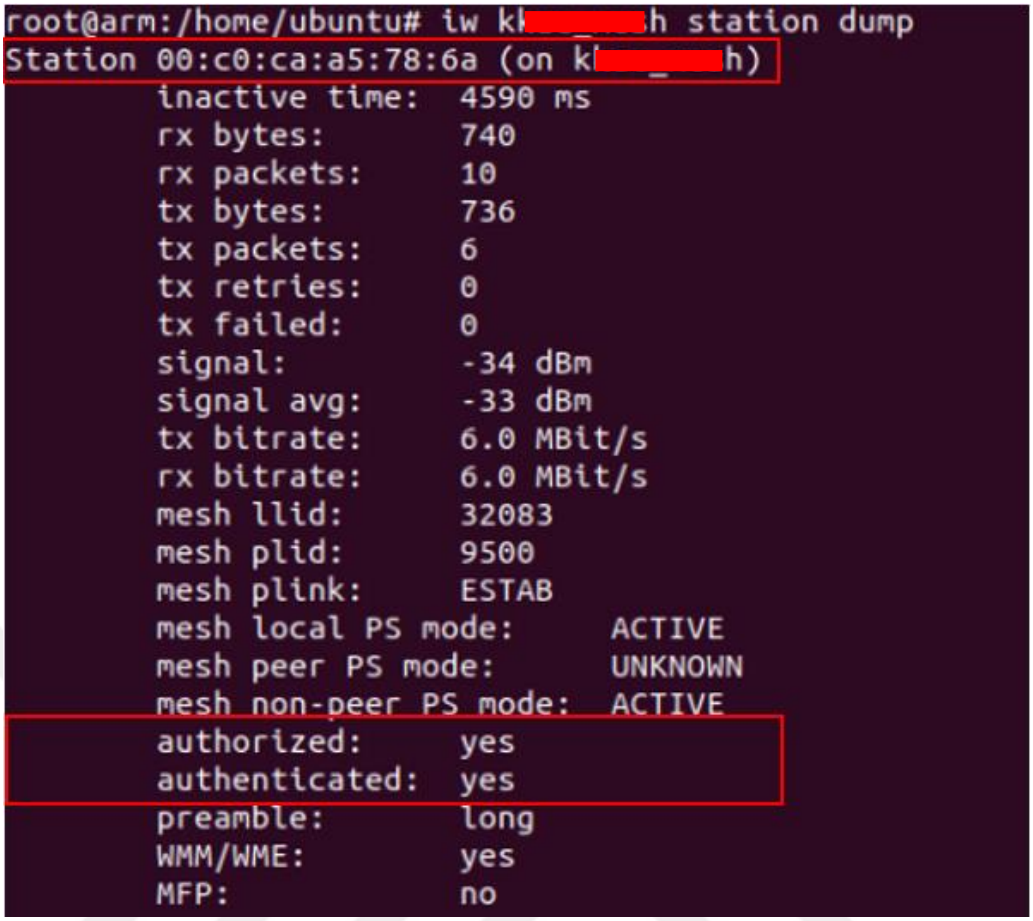
Şekil 3.19: Sahte Kimlik Doğrulama Saldırısında Örgü Değiş-Tokuş Yönetimi Sürecinde Yakalanan Çerçeve-3 (Mesh Peering Confirm)

Şekil 3.20'de USB Wi-Fi Adaptör ile hedef Örgü Noktası arasındaki süreci sonlandıran Mesh Peering Confirm çerçevesi gösterilmiştir.



Şekil 3.20: Sahte Kimlik Doğrulama Saldırısında Örgü Değiş-Tokuş Yönetimi Sürecinde Yakalanan Çerçeve-4 (Mesh Peering Confirm)

Saldırının sonucunu kontrol etmek için, hedef Örgü Noktasının işletim sistemi arayüzü üzerinde "iw *mesh interface* station dump" komutu çalıştırılır.

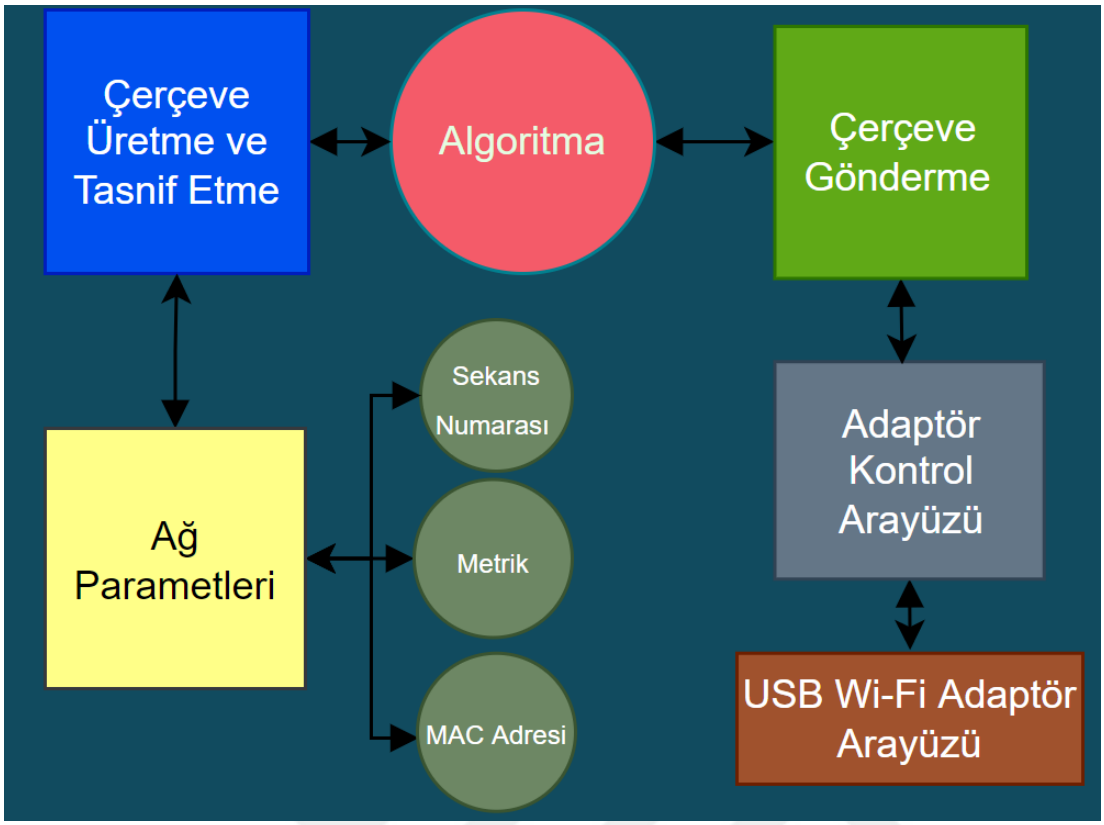


Şekil 3.21: İşletim Sistemi Debug Arayüzünden Saldırının Başarısını Kontrol Eden Örgü Noktalarının Kimlik Doğrulama Bilgilerine Ait Çıktı

Şekil 3.21'de görüldüğü üzere; USB Wi-Fi Adaptör'ün MAC adresi, hedef Örgü Noktasının Kimlik Doğruladığı MAC olarak gösterilmektedir ve böylelikle Sahte Kimlik Doğrulama saldırısı başarıyla gerçeklenmiştir.

3.5.3 Yol Saptırma Saldırısının Gerçeklenmesi

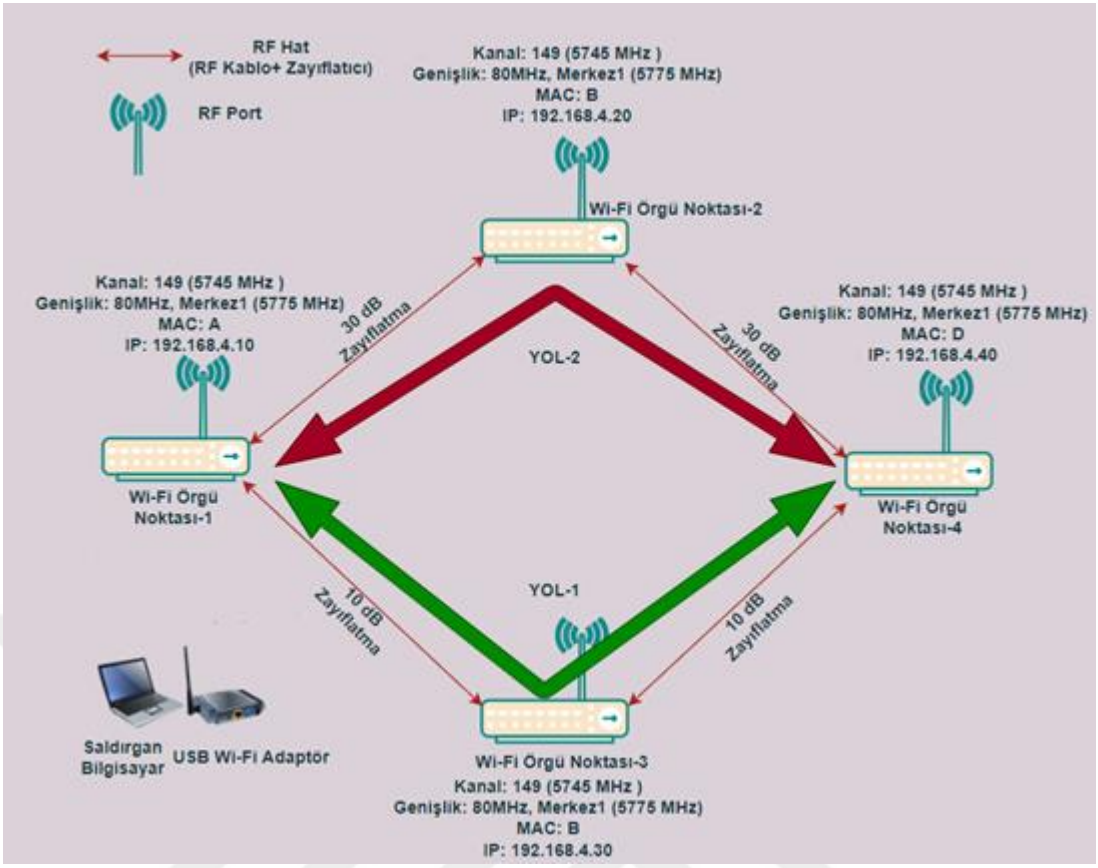
Yol Saptırma saldırısının gerçeklenme aşamasında, Örgü Noktalarının PREQ çerçevelerini işlemesi için, bu paketlerin sıra numarasının ağdaki diğer paketlerden güncel olması gerekmektedir. Bu nedenle PREQ çerçevesinin ağ içerisindeki güncel değerini öğrenebilmek ve Örgü Noktalarının MAC adresini elde edebilmek gerekmektedir. Ayrıca ağa enjekte edilen sahte metrik bilgileriyle de yönlendirme manipülasyonu yapılabilmesi için uygun metrik seçimi yapılmaktadır. Bu saldırının gerçeklenmesi için oluşturulan yazılım mimarisi aşağıdaki şekilde gösterilmiştir.



Şekil 3.22: Bu Çalışma Kapsamında Oluşturulan Yol Saptırma Saldırısı Yazılım Mimarisi

Sahte Kimlik Doğrulama saldırı mimarisinden farklı olarak, bu mimaride paralel yapıda çalışacak "iş parçacıkları" yapısı, ya da ID'ler ile alakalı alt bloklar yer almamaktadır. Bu saldırı tipinde hedef Örgü Noktasına sadece çerçeve gönderimi yapılmaktadır. Bu mimaride Hedef MAC adresine ek olarak ise, Metrik ve Sekans numarası bilgilerine ihtiyaç duyulmaktadır.

Şekil 3.23'te görülen, 802.11ac tabanlı kablosuz test ortamında, Wi-Fi Örgü Noktaları kullanılarak RF zayıflatıcı ve kablolar yardımıyla "YOL-1" en kısa yol olacak metrik değeri ile beraber oluşturulan topoloji aşağıdaki şekildeki gibi kurulmuştur. Metrik değeri her hattaki RF seviyesi ve atlama yapılan Örgü Noktası özelinde değişiklik göstermekte ve Örgü Noktaları tarafında otomatik olarak hesaplanmaktadır.



Şekil 3.23: Yol Saptırma Saldırısı Yapılmadan Önce Örgü Noktalarının Trafik Akışını Gösteren Deney Düzeneği

YOL-1'in en kısa yol olarak seçilmesi için, YOL-2'de daha fazla zayıflatma seviyesine sahip RF zayıflatıcılar kullanılmaktadır. (YOL-1'in her bağlantısı için 10 dB, YOL-2'nin her bağlantısı için 30 dB zayıflatıcı kullanılmıştır.)

Aralarında doğrudan bir bağlantı olmayan Wi-Fi Cihazı-1'den Wi-Fi Cihazı-4'e veri akışı başlatıldığında, sonuçların beklenildiği üzere en kısa yol olarak "YOL-1" seçildiği görülmüştür. "YOL-1'in" en kısa yol olarak seçildiği bilgisi Örgü Noktalarının işletim sistemi arayüzünden kontrol edilmiştir.

Aynı topoloji üzerinde, saldırgan bilgisayar monitör mod aracılığıyla dinlediği ağdaki HWMP paketlerini analiz etmektedir. Analiz edilen paketler sonucu, YOL-1(en kısa yol) ve YOL-2'ye ait metrikler, Örgü Noktalarına ait MAC adresleri ve trafik devam ettikçe artan sekans numaraları elde edilmiştir.

Elde edilen bu bilgilerle beraber saldırıya başlanabilmektedir. Bu kapsamda Saldırgan Bilgisayar aracılığı ile Wi-Fi Örgü Noktası-1'e, Wi-Fi Örgü Noktası-2'nin MAC adresi taklit edilerek YOL-1'in metrik değerlerinde daha düşük sahte metrik bilgileri gönderilmeye başlanmıştır. Oluşturulan saldırı mimarisine göre bu süreç aşağıdaki sırayla anlatılmaktadır.

- "Ağ Parametreleri" birimine MAC, metrik ve sekans numarası girişi yapılır.

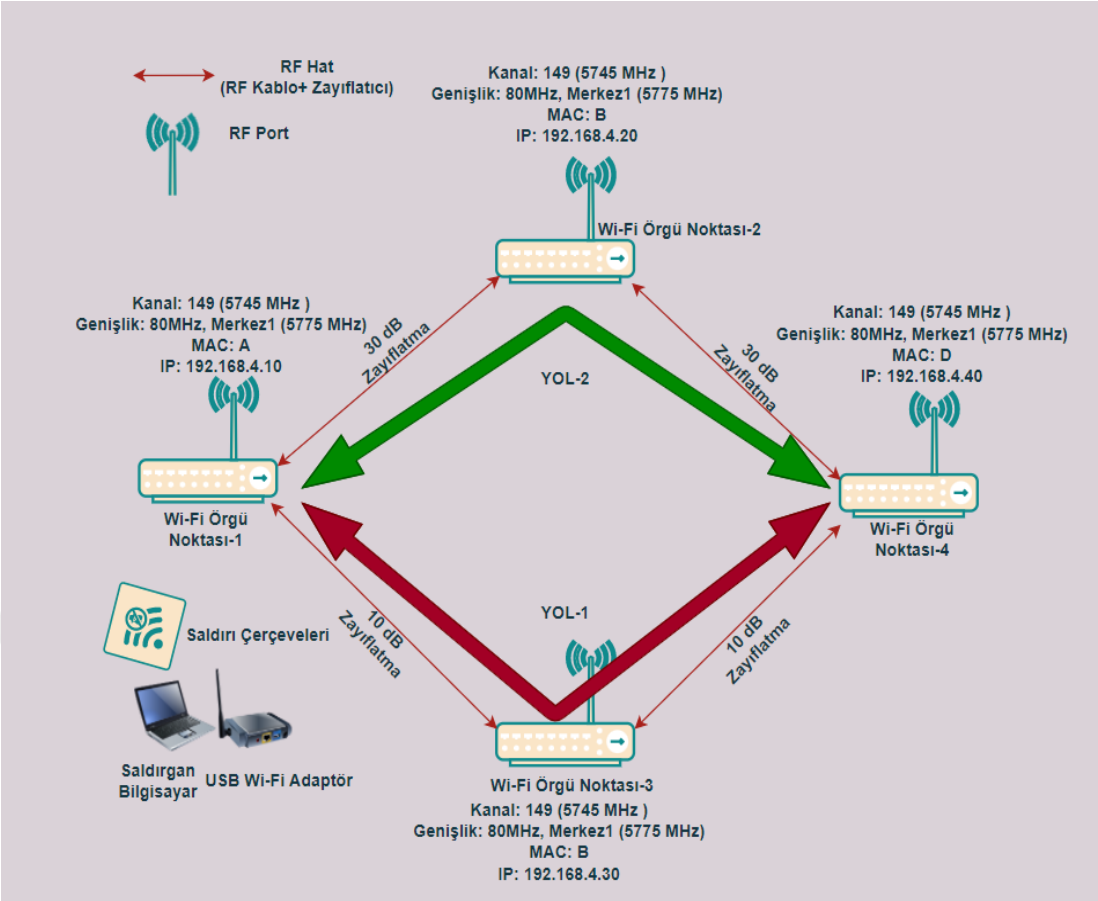
- "Çerçeve Üretme ve Tasnif Etme" bloğu aracılığıyla parametre girişinin ardından trafik analizi sırasında elde edilen taslak PREP çerçeveleri temel alınarak, HWMP PREP çerçevelerini oluşturulur. Parametre olarak alınan bilgiler, bu çerçevelere eklenir.

- Algoritma birimi Adaptör Kontrol Arayüzünü çerçeve göndermek için aktif hale getirir.

- "Çerçeve Gönderme" bloğu PREP çerçevelerini, Hedef Örgü Ağını adreslemesi için USB Wi-Fi Adaptör Arayüzüne gönderir.

- Saldırı sürekli devam ederken, gönderilecek her PREP çerçevesi için sekans numarası Algoritma bloğu tarafından arttırılır.

Saldırı başlatıldıktan sonra cihazların işletim sistemi arayüzünden trafiğin seyri kontrol edilmiştir. İncelenen trafikte Wi-Fi Örgü Noktası-1'in, Wi-Fi Örgü Noktası-4'e ulaşmak için artık Wi-Fi Örgü Noktası-2'yi seçtiği görülmüştür. İlgili topoloji Şekil 3.24'de gösterilmiştir.



Şekil 3.24: Yol Saptırma Saldırısı Esnasında Örgü Noktalarının Trafik Akışını Gösteren Deney Düzeneği

Yapılan saldırı adımların sonunda, en kısa yol olmayan “YOL-2” saldırgan tarafından hedeflenen Wi-Fi Örgü Noktasına istenilen ölçüde seçtirilebilmektedir. Bu sayede hazırlanan saldırı kodları adaptör üzerinden ağa gönderilerek istenilen yol yönlendirmesi başarılı bir şekilde yapılabilmektedir.

3.5.4 Karadelik Saldırısının Gerçeklenmesi

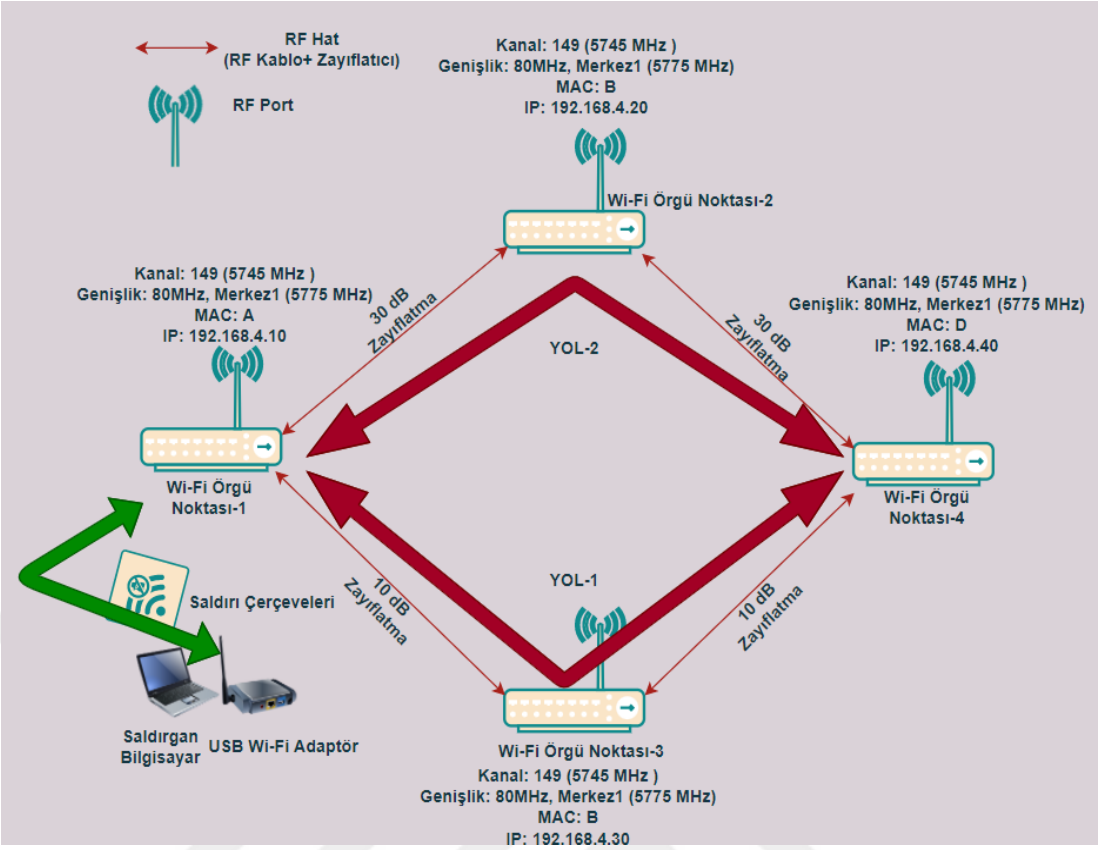
Bu bölümde anlatılacak Karadelik saldırısının yazılım mimarisi, bir önceki bölüm olan 3.5.3’deki Yol Saptırma saldırısı yazılım mimarisi ile aynıdır. Ayrıca Saldırıların gerçeklenme prensiplerinde ise sadece kullanılan MAC adresi bilgileri farklılık göstermektedir. Yol Saptırma Saldırısında, ağda bulunan ve Hedef Örgü Noktasıyla kimlik doğrulamış noktalar arası yol saptırmalar gerçekleştirilmiştir. Bu da taklit edilen MAC adreslerinin Hedef Örgü Noktasının kimlik doğrulama tablosunda yer aldığını göstermektedir.

Karadelik saldırısında farklı olan konsept, Wi-Fi Örgü Noktası mimarilerinin doğası gereği, işlenecek HWMP çerçevelerinin "kaynak" MAC adresi ile, hedeflenen Wi-Fi Örgü Noktasının Kimlik doğrulamış olması gerektiğidir. Çünkü ağda Karadelik yaratacak cihaz saldırgan bilgisayara bağlı USB Wi-Fi adaptördür.

Saldırıya başlamadan önce, Bölüm 3.5.3, Şekil 3.23'teki ağ topolojisi kurulur. Wi-Fi Örgü Noktası-1 ile Wi-Fi Örgü Noktası-4 arasında ağ trafiği başlatılır. Ağ trafiği Örgü Noktalarını "debug" arayüzünden kontrol edildiğinde beklendiği üzere yine YOL-1'in seçildiği görülmüştür. Sonrasında ise, Karadelik Saldırısı için aşağıda verilen iki temel adım gerçekleştirilir.

a) 3.5.2'de anlatılan Sahte Kimlik Doğrulama saldırısı ile Karadelik yaratılacak MAC adresine sahip USB Wi-Fi Adaptör hedef Wi-Fi Örgü noktası kimlik doğrular.
b) Bölüm 3.5.3'de anlatılan Yol Saptırma Saldırısında, kaynak MAC adresi olarak USB Wi-Fi Adaptör'ün MAC adresi seçilir ve saldırı başlatılır.

Şekil 3.25'te görüldüğü gibi, USB Wi-Fi Adaptör aracılığıyla saldırının başlatıldığı Wi-Fi Erişim Noktası-1'e sahte PREP çerçeveleri gönderilmektedir. Bu çerçeveler, yukarıda tekrarlanan "b" adımından elde edilmiş olan en düşük metrik bilgileri olmakla beraber, saldırı devam ettiği sürece PREP çerçeveleri Hedef Örgü Noktası tarafından işlenmekte ve herhangi bir hedefe ulaşmak için ilk anahtarlanan yolun USB-Wi-Fi Adaptör üzerinden geçtiği görülmektedir.



Şekil 3.25: Karadelik Saldırısı Yapılmadan Önce Örgü Noktalarının Trafik Akışını Gösteren Deney Düzeneği

Şekil 3.25'teki topolojide, saldırının devam ettiği süre zarfında hedef Wi-Fi Örgü Noktasını ağdaki hiçbir Wi-Fi Örgü Noktası ile haberleşemediği görülmüştür.

4. SONUÇ VE GELECEK ÇALIŞMALAR

Bu tez, Temel Servis Seti mimarisinde tanımlı en yaygın saldırılardan olan Ağ Bağlantısını Kesme saldırısı özelinde modüler yapıda oluşturulmuş uçtan uca bir Kablosuz Saldırı Tespit Sistemi çözümünü sunmuş ve gerçeklemiştir. Ayrıca 802.11s uyumlu Kablosuz Örgü Ağlarına ait saldırılarından olan Sahte Kimlik Doğrulama, Yol Saptırma ve Karadelik saldırıları için yazılım mimarisini anlatmış, saldırı gerçekleme evrelerini aşama aşama göstermiştir.

Tezin ikinci bölümünü oluşturan Kablosuz Saldırı Tespit Sistemi, donanım üzerine ağ bağlantısı yapılarak çalışabilen mimaride gerçeklenirken, bu mimari içerisinde başta Ağdan Düşürme Saldırıları için kullanılabilecek, modüler yapısıyla beraber farklı tespit algoritmalarıyla entegre olabilecek uçtan uca çalışabilen bir saldırı tespit sistemi elde edilmiştir.

Tezin üçüncü bölümde ise, Kablosuz Örgü Ağlarına özel olarak bahsedilen üç tip saldırının her biri için yazılım mimarisi ve başarılı sonuç elde edilen gerçekleme konseptleri sunmuştur. Yapılan çalışmalar, literatür araştırmaları sırasında gelişime oldukça açık olduğu görülen bu alan için 802.11s uyumlu Dağıtık Ağlarda kullanılabilecek bir çeşit ağ test yazılımı olarak çıktı sağlamaktadır.

Bu tezin temelini oluşturduğu gelecekte yapılması planlanan çalışmalar ise, Temel Servis Setinde kullanılan Kablosuz Saldırı Tespit Sisteminin, 802.11s Kablosuz Örgü Ağları saldırıları özelinde geliştirilmesi olacaktır. Böylelikle Kablosuz Saldırı Tespit Sisteminin hem Temel Servis Setini hem de Dağıtık Yapıyı kapsayan gelişmiş bir çözüm olarak sunulması planlanmaktadır.

KAYNAKLAR

[1] "Wi-Fi Alliance 2020 Annual Report".

[2] "Cisco Annual Internet Report 2020, White Paper".

[3] **Ong, E. H., Kneckt, J., Alanen, O., Chang, Z., Huovinen, T., & Nihtilä, T**. (2011, September). "IEEE 802.11 ac: Enhancements for very high throughput WLANs." *In 2011 IEEE 22nd International Symposium on Personal, Indoor and Mobile Radio Communications (pp. 8).*

[4] **Akyildiz, Ian F., Xudong Wang, and Weilin Wang.** "Wireless mesh networks: a survey." *Computer networks 47.4 (2005): 445-487.*

[5] **E. Chatzoglou, G. Kambourakis and C. Kolias,** "Empirical Evaluation of Attacks Against IEEE 802.11 Enterprise Networks: The AWID3 Dataset", *in IEEE Access, vol. 9, pp. 34188-34205, 2021, doi: 10.1109/ACCESS.2021.3061609*.

[6] **Thing, V. L.** (2017, March). "IEEE 802.11 network anomaly detection and attack classification: A deep learning approach." *In 2017 IEEE Wireless Communications and Networking Conference (WCNC) (pp. 1-6). IEEE.*

[7] **Bicakci, K., & Tavli, B.** (2009). "Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks." *Computer Standards & Interfaces, 31(5), 931-941.*

[8] https://www.aircrack-ng.org/. alındığıtarih:10.12.2021

[9] **Abdelrahman, Ramia Babiker Mohammed, Amin Babiker A. Mustafa, and Ashraf A. Osman.** "A Comparison between IEEE 802.11 a, b, g, n and ac Standards". *IOSR Journal of Computer Engineering (IOSR-JEC) 17 (2015): 26-29.*

[10] **Kurose, J. F.** (2005). Computer networking: "A top-down approach featuring the internet", *3/E. Pearson Education India.*

[11] **Gast, M. S.** (2013). 802.11 ac: a survival guide: "Wi-Fi at gigabit and beyond" *O'Reilly Media, Inc.*

[12] **Bejarano, O., Knightly, E. W., & Park, M.** (2013). "IEEE 802.11 ac: from channelization to multi-user MIMO." *IEEE Communications Magazine, 51(10), 84-90.*

[13] **Lashkari, A. H., Danesh, M. M. S., & Samadi, B.** (2009, August). "A survey on wireless security protocols (WEP, WPA and WPA2/802.11 i)." *In 2009 2nd IEEE international conference on computer science and information technology (pp. 48-52). IEEE.*

[14] **Chen, J. C., & Wang, Y. P.** (2005). "Extensible authentication protocol (EAP) and IEEE 802.1 x: tutorial and empirical experience." *IEEE communications magazine, 43(12), supl-26.*

[15] **Kolias, C., Kambourakis, G., Stavrou, A., & Gritzalis, S.** (2015). "Intrusion detection in 802.11 networks: empirical evaluation of threats and a

public dataset." *IEEE Communications Surveys & Tutorials, 18(1), 184-208.*

[16] **Thanthrige, U. S. K. P. M., Samarabandu, J., & Wang, X.** (2016, May). Machine learning techniques for intrusion detection on public dataset. *In 2016 IEEE Canadian conference on electrical and computer engineering (CCECE) (pp. 1-4). IEEE.*

[17] **Vijayakumar, D. S., & Ganapathy, S.** (2018). Machine Learning Approach to Combat False Alarms in Wireless Intrusion Detection System. *Comput. Inf. Sci., 11(3), 67-81*.

[18] **Kasongo, S. M., & Sun, Y.** (2020). "A deep long short-term memory based classifier for wireless intrusion detection system." *ICT Express, 6(2), 98-103*.

[19] **Kasongo, S. M., & Sun, Y.** (2020). A deep learning method with wrapper based feature extraction for wireless intrusion detection system. *Computers & Security, 92, 101752.».*

[20] **Kasongo, S. M., & Sun, Y.** (2019). A deep learning method with filter based feature engineering for wireless intrusion detection system. I*EEE Access, 7, 38597-38607.*

[21] https://wireless.wiki.kernel.org/en/users/drivers/ath10k. alındığıtarih:10.12.2021

[22] https://www.kali.org/." alındığıtarih:10.12.2021

[23] **Marback, A., Do, H., He, K., Kondamarri, S., & Xu, D.** (2013). A threat model-based approach to security testing. *Software: Practice and Experience, 43(2), 241-258.*

[24] **Ahmad, M. S., & Tadakamadla, S.** (2011, June). Short paper: security evaluation of IEEE 802.11 w specification. *In Proceedings of the fourth ACM conference on Wireless network security (pp. 53-58).*

[25] **Vanhoef, M., & Ronen, E.** (2020, May). Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd. *In 2020 IEEE Symposium on Security and Privacy (SP) (pp. 517-533). IEEE.*

[26] **Chatzoglou, E., Kambourakis, G., & Kolias, C.** (2022). How is your Wi-Fi connection today? DoS attacks on WPA3-SAE. *Journal of Information Security and Applications, 64, 103058.*

[27] https://www.aircrack-ng.org/ alındığıtarih:10.12.2021

[28] https://crack.sh/ alındığıtarih:10.12.2021

[29] https://icsdweb.aegean.gr/awid/awid2 alındığıtarih:10.12.2021

[30] https://icsdweb.aegean.gr/awid/attributes.html alındığıtarih:10.12.2021

[31] https://colab.research.google.com/?utm_source=scs-index alındığıtarih:10.12.2021

[32] https://www.python.org/ alındığıtarih:10.12.2021

[33] **Shilpa Bhandari, Avinash K Kukreja, Alina Lazar, Alex Sim, and Kesheng Wu.** 2020. Feature Selection Improves Tree-based Classification for

Wireless Intrusion Detection. *In Proceedings of the 3rd International Workshop on Systems and Network Telemetry and A.*

[34] **Sweta B., Praveen K. R. M., Rajesh K., Saurabh S, Tippa R. G., Mamoun A., Usman T., et almbox**. 2020. A novel PCA-firefly based XGBoost classification model for intrusion detection in networks using GPU. El.

[35] **Leo Breiman.** 2001. Random Forests. Mach. Learn., *Vol. 45, 1 (Oct. 2001), 5--32.*

[36] **Lazar, A., Sim, A., & Wu, K.** (2020). GPU-based Classification for Wireless Intrusion Detection. *In Proceedings of the 2021 on Systems and Network Telemetry and Analytics (pp. 27-31).*

[37] **A Reyes, A., D Vaca, F., Castro Aguayo, G. A., Niyaz, Q., & Devabhaktuni, V.** (2020). A machine learning based two-stage Wi-Fi network intrusion detection system. *Electronics, 9(10), 1689.*

[38] **Mohammed, M., Khan, M. B., & Bashier, E. B. M.** (2016). Machine learning: algorithms and applications. *Crc Press*.

[39] https://docs.python.org/3/library/pickle.html alındığıtarih:10.12.2021

[40] https://www.wireshark.org/docs/dfref/w/wlan.html alındığıtarih:10.12.2021

[41] https://www.wireshark.org/ alındığıtarih:10.12.2021

[42] https://github.com/KimiNewt/pyshark alındığıtarih:10.12.2021

[43] **Luckham, D. C., & Vera, J.** (1995). An event-based architecture definition language. *IEEE transactions on Software Engineering, 21(9), 717-734.*

[44] https://socket.io/ alındığıtarih:10.12.2021

[45] https://nodejs.org/en/ alındığıtarih:10.12.2021

[46] https://www.javascript.com/ alındığıtarih:10.12.2021

[47] https://www.w3schools.com/html/html_intro.asp alındığıtarih:10.12.2021

[48] https://www.w3schools.com/css/css_intro.asp alındığıtarih:10.12.2021

[49] **Camp, J. D., & Knightly, E. W.** (2008). The IEEE 802.11 s extended service set mesh networking standard. *IEEE Communications Magazine, 46(8), 120-126.*

[50] **Hiertz, G. R., Max, S., Zhao, R., Denteneer, D., & Berlemann, L.** (2007, August). Principles of IEEE 802.11 s. *In 2007 16th International Conference on Computer Communications and Networks (pp. 1002-1007). IEEE*.

[51] **Carrano, R. C., Magalhães, L. C., Saade, D. C. M., & Albuquerque, C. V.** (2010). IEEE 802.11 s multihop MAC: A tutorial. *IEEE Communications Surveys & Tutorials, 13(1), 52-67.*

[52] F**lammini, A., Sisinni, E., & Tramarin, F.** (2017, May). IEEE 802.11 s performance assessment: From simulations to real-world experiments. *In 2017 IEEE International Instrumentation and Measurement Technology Conference (I2MTC) (pp. 1-6). IEEE.*

[53] **Henry, J., & Burton, M.** (2011). 802.11 s mesh networking. certified wireless network professional.

[54] **Perkins, C., Belding-Royer, E., & Das, S.** (2003). RFC3561: Ad hoc on-demand distance vector (AODV) routing.

[55] **Guesmia, M., Guezouri, M., & Mbarek, N.** (2012, March). Performance evaluation of the HWMP proactive tree mode for IEEE 802.11 s based wireless mesh networks. *In Third International Conference on Communications and Networking (pp. 1-7). IEEE.*

[56] **Bari, S. M. S., Anwar, F., & Masud, M. H.** (2012, July). Performance study of hybrid Wireless Mesh Protocol (HWMP) for IEEE 802.11 s WLAN mesh networks. *In 2012 international conference on computer and communication engineering (ICCCE) (pp. 712-716). IEEE.*

[57] **Wang, X., & Lim, A. O.** (2008). IEEE 802.11 s wireless mesh networks: Framework and challenges. *Ad Hoc Networks, 6(6), 970-984.*

[58] **Tan, W. K., Lee, S. G., Lam, J. H., & Yoo, S. M.** (2013). A security analysis of the 802.11 s wireless mesh network routing protocol and its secure routing protocols. *Sensors, 13(9), 11553-11585.*

[59] **Szott, S.** (2014). Selfish insider attacks in IEEE 802.11 s wireless mesh networks. *IEEE Communications Magazine, 52(6), 227-233.*

[60] https://www.wireshark.org/docs/man-pages/tshark.html 10.12.2021

[61] https://scapy.net/ alındığıtarih:10.12.2021

[62] https://github.com/morrownr/8812au alındığıtarih:10.12.2021

[63] **Harkins, D.** (2008, August). Simultaneous authentication of equals: A secure, password-based key exchange for mesh networks. *In 2008 Second International Conference on Sensor Technologies and Applications (sensorcomm 2008) (pp. 839-844). IEEE.*

[64] **Yi, P., Wu, Y., Zou, F., & Liu, N.** (2010). A survey on security in wireless mesh networks. *IETE Technical Review, 27(1), 6-14.*