T.C.
İSTANBUL ÜNİVERSİTESİ-CERRAHPAŞA
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

ABONELİK YÖNETİCİSİ GÜVENLİ YÖNLENDİRME SUNUCULARI ARASINDA GÖMÜLÜ EVRENSEL TÜMLEŞİK DEVRE KARTI PROFİLİ TAKAS İŞLEMLERİNİN OPTİMİZASYONU

Nazif Güray GÜNGÖRDÜ

DANIŞMAN
Dr. Öğr. Üyesi Bahattin KARAKAYA

Elektrik-Elektronik Mühendisliği Anabilim Dalı

Elektrik-Elektronik Mühendisliği Programı

Haziran-2022

TEZ KABUL VE ONAYI

Bu çalışma, 5.01.2022 tarihinde aşağıdaki jüri tarafından Elektrik-Elektronik Mühendisliği Anabilim Dalı, Elektrik-Elektronik Mühendisliği Programında Yüksek Lisans tezi olarak kabul edilmiştir.

Tez Jürisi

Dr. Öğr. Üyesi Bahattin KARAKAYA(Danışman)
İstanbul Üniversitesi-Cerrahpaşa
Fakülte

Doç. Dr. Muhammed Emin Başak
Yıldız Teknik Üniversitesi
Gemi İnşaatı ve Denizcilik Fakültesi

Dr. Öğr. Üyesi Mahmut Öztürk
İstanbul Üniversitesi Cerrahpaşa
Mühendislik Fakültesi

Doç. Dr. Adı SOYADI
Üniversite
Fakülte

Dr. Öğr. Üyesi Adı SOYADI
Üniversite
Fakülte

BEYAN

Bu tez çalışmasının kendi çalışmam olduğunu, tezin planlanmasından yazımına kadar bütün aşamalarda etik dışı davranışımın olmadığını, bu tezdeki bütün bilgileri akademik ve bilimsel etik kuralları içinde elde ettiğimi, bu tez çalışmasıyla elde edilmeyen bütün bilgi ve yorumlara kaynak gösterdiğimi ve bu kaynakları da kaynaklar listesine aldığımı, yine bu tezin çalışılması ve yazımı sırasında patent ve telif haklarını ihlal edici bir davranışımın olmadığını ve her türlü hukuki sorumluluğu aldığımı kabul ederim.

Nazif Güray Güngördü

BÜTÇE DESTEKLERİ

ABONELİK YÖNETİCİSİ GÜVENLİ YÖNLENDİRME SUNUCULARI ARASINDA GÖMÜLÜ EVRENSEL TÜMLEŞİK DEVRE KARTI PROFİLİ TAKAS İŞLEMLERİNİN OPTİMİZASYONU

Bu tez çalışması için herhangi bir kurumdan bütçe desteği alınmamıştır.

TEŞEKKÜR

Yaklaşık 5 yıldır çalışmakta olduğum otomotiv sektöründe işin en önemli parçalarından biri haline gelmiş olan araç içi eğlence ve bağlantı sistemleri, otonom elektrikli araç sitemleri ile sektörün ilgisini ve odağını üzerine almış durumdadır.

Otomotiv sektörü, bundan böyle makine mühendislerinin ağırlıkta olduğu bir sektör olmaktan ziyade, elektrik elektronik ve bilgisayar mühendislerinin işin odağında olduğu bir sektör haline dönüşmüştür. Bu teknolojilerle ilgilenirken kullandığım çok kez programlanabilen gömülü SIM kartların sektörün geleceği açısından çok önemli bir role sahip olduğunu gördüm. Bağlantılı araçların içerisinde bulunan bu uzaktan programlanabilir SIM kartlar ile ilgili deneyimlerimde yurt dışında ve Türkiye'de güvenlik ihtiyaçlarının karşılanması için gerekli olan bazı eklemelere ve tanımlamalar ihtiyaç olduğunu fark ettim. Bu çalışmamda bağlantılı araçların geleceği ile ilgili olan yeni nesil tekrar programlanabilir SIM kart teknolojisinin yönetmeliklerini, bu yönetmelikleri belirleyen GSMA standarda tanımlanmayan bir prosedürü, SIM kart üreticisi olmayan SM-SR serverlara SIM kartların profillerinin transferini anlatacağım.

Bu çalışmamda bana yardımlarını hiçbir zaman esirgemeyen eşime ve aileme, bana ayırdığı her bir saniyesi için minnettar olduğum çok değerli hocam Sayın Dr. Bahattin Karakaya'ya ve bana anlayış gösteren tüm arkadaşlarıma çok teşekkür ederim.

Haziran 2022 Nazif Güray Güngördü

İÇİNDEKİLER

Sayfa No

TEŞEKKÜR ..... **v**
İÇİNDEKİLER ..... **vi**
ŞEKİL LİSTESİ ..... **viii**
TABLO LİSTESİ ..... **x**
SİMGE VE KISALTMA LİSTESİ ..... **xi**
ÖZET ..... **xv**
SUMMARY ..... **xvi**
1. GİRİŞ **1**
2. HÜCRESEL HABERLEŞMENİN VE GSMA **3**
2.1. İLETİŞİM 3
2.1.1. İletişim Katmanları 5
2.1.2. IoT Protokolleri 6
MQTT *6*
COAP *7*
XMPP *8*
SOAP *9*
UPNP *9*
2.1.3. Çoğullama (Multiplexing) 10
2.1.4. Frekans Bölmeli Çoklu Erişim (FDMA) 10
2.1.5. Zaman Bölmeli Çoklu Erişim (TDMA) 11
2.1.6. Kod Bölmeli Çoklu Erişim (CDMA) 12
2.1.7. Dik Frekans Bölmeli Çoklu Erişim (OFDMA) 13
2.1.8. NOMA 14
Noma Temelleri *15*
Süper-Pozisyon Kodlaması (SC) *16*
Ardışık Girişim İptali (SIC) *17*
2.1.9. SODEMA 20
3. MALZEME VE YÖNTEM **26**

3.1. IOT, M2M VE BAĞLANTILI ARAÇLAR 31
3.2. BAĞLANTILI ARAÇLAR 31
3.2.1. Uzaktan Kilitleme/Açma 33
3.2.2. Uzaktan Çalıştırma 34
3.2.3. Uzaktan Araç Durumu Sorgulama 35
3.2.4. Uzaktan Güncelleme 36
3.2.5. Eğlence Sitemleri 37
3.2.6. Bölgesel Çit 37
3.2.7. Araç Konum Bilgileri 38
3.2.8. Sürücü Performans Bilgileri 38
3.2.9. Acil Durum Çağrıları 38
3.3. GSMA 39
3.3.1. SIM Kartlar 40
3.3.2. eSIM 42
3.3.3. eUICC 42
Havadan Kontrol Edilebilme (OTA) *43*
3.3.4. SM-DP 43
3.3.5. SM-SR 44
3.4. SIM KART ÜRETİCİSİ SM-SR SUNUCUSUNDAN SIM KART ÜRETİCİSİ OLMAYAN SM-SR SUNUCUSUNDA PROFİL TRANSFERİ 44
4. BULGULAR 46
5. TARTIŞMA VE SONUÇ 51
KAYNAKLAR 53
EKLER 57
5.1. TURNİTİN TARAMASI 57

ŞEKİL LİSTESİ

Sayfa No

Şekil 2-1 Temel İletişim 4

Şekil 2-2 OSI Katmanları [2] 5

Şekil 2-3 MQTT Protokolü Haberleşme Mimarisi [4] 6

Şekil 2-4 CoAP Haberleşme Mimarisi [7] 7

Şekil 2-5 XMPP Protokolü Haberleşme Mimarisi [8] 8

Şekil 2-6 SOAP Protokolü Haberleşme Mimarisi [9] 9

Şekil 2-7 FDMA Çalıma Prensibi [11] 10

Şekil 2-8 TDMA (frekans genişliği temsilidir) [14] 11

Şekil 2-9 CDMA [15] 12

Şekil 2-10 OFDMA zaman frekans düzlemi [17] 13

Şekil 2-11 OFDMA-2 [17] 13

Şekil 2-12 NOMA Temelleri 15

Şekil 2-13 SC Süper-Pozisyon örneği(a) kullanıcı 1 (b) kullanıcı 2 x ise süprepoze sinyal olarak tanımlanır. 17

Şekil 2-14 SIC ile izole edilmiş sinyaller [31] 18

Şekil 2-15 NOMA SIC Kullanım Görseli [31] 19

Şekil 2-16 SoDeMA Bağlantılı Araçlar Farklı Yoğunluklarda Gösterimi 20

Şekil 2-17 Bant ve güç dağılımı karşılaştırması OFDMA ve NOMA [32] 22

Şekil 2-18 Verici Tarafı NOMA 23

Şekil 2-19 Kullanıcı cihazına dışarıdan bakış [18] 23

Şekil 2-20 SIC Alıcı Tarafı [18] 23

Şekil 2-21 NOMA SIC ve OMA üzerinde 2 kullanıcılı sistemde veri hızı karşılaştırması [18] 24

Şekil 2-22 NOMA SIC ve OMA Güç ve Verileri Karşılaştırması [18] 24

Şekil 3-1 Başlangıçta Yerli MNO ve SM-SR Profili İle Başlayan Senaryo 27

Şekil 3-2 SM-SR Taşıma İşlemi 27

Şekil 3-3 DDT2000 Hücresel Ağ Ara Yüzü Boş 30

Şekil 3-4 Bağlantılı Araç [34] 33

Şekil 3-5 Uzaktan Kilitleme 33

Şekil 3-6 Uzaktan Çalıştırma 34

Şekil 3-7 Uzaktan Diagnostik Sorgulama [35] 35

Şekil 3-8 Uzaktan Güncelleme FOTA[36] 36

Şekil 3-9 Renault Multimedya 37

Şekil 4-1 Transfer İşlemi Başlangıcı 48

Şekil 4-2 Transfer İşlemi Sonucu 49

TABLO LİSTESİ

Sayfa No

Tablo 1 Çoğullama Karşılaştırma Tablosu 22

Tablo 2- SIM Kartlar 41

SİMGE VE KISALTMA LİSTESİ

1G, 2G, 3G, 4G, 5G, 6G : Birinci, İkinci, Üçüncü, Dördüncü, Beşinci, Altıncı Nesil [First, Second, Third,Fourth,Fifth Generation]

ACK : Bilgilendirme [Acknowledgement]

AWGN : Eklenir Beyaz Gause Gürültüsü [Additive White Gaussian Noise]

AI : Yapay Girişim [Artificial Interference]

AN : Yapay Gürültü [Artificial Noise]

AES : Gelimiş Şifreleme Standardı [Advanced Encryption Standard]

AMPS : Gelişmiş Mobil Telefon Sistemi [Advanced Mobile Phone Systems]

AMQP : Gelişmiş Mesaj Sıralama Protokolü [Advanced Messaging Queuing Protocol]

API : Uygulama Programlama Arayüzü [Application Programming Interface]

BLE : Bluetooth Düşük Enerji [Bluetooth Low Energy]

BER : Bit Hata Oranı [Bit Error Rate]

BTK : Bilgi Teknolojileri Kurumu

CAN : Control Alan Ağı [Controller Area Network]

CC : Kanal Katsayı [Channel Coefficients]

CE : Kanal Tahmini [Channel Estimation]

CFO : Taşıyıcı Frekans Ofseti [Carrier Frequency Offset]

CFR : Kanal Frekans Tepkis [Channel Frequency Response]

CP : Tekrarlı Önişaret [Cyclic Prefix]

CSI : Kanal Durum İşareti [Channel State Information]

CCN : İçerik Merkezi Ağı [Content Centric Network]

CDMA : Kod Bölmeli Çoklu erişim [Code Division Multiple Access]

CDF : Kümülatif dağıtım Fonksiyonu [Cumulative Distribution Function]

CRC : Tekrarlayan Kararlılık Testi [Cyclic Redundancy Check]

CoAP : Yoğunlaşmış Uygulama Protokolü [Constrained Application Protocol]

DDoS : Dağıtılmış Ret Servisi [Disturbed Denial of Service]

DoS : Servis Reddi [Denial of Service]

DAC : Dijitalden Anoloğa Çevirici [Digital-to-Analog Converter]

DFT : Ayrık Furiyer Dönüşümü [Discrete Fourier Transform]

DTLS : Datagram Taşıyıcı Katman Güvenliği [Datagram Transport Layer Security]

EID : eUICC Kimliği [eUICC-ID]

EIS : eUICC Veri Seti [eUICC Information Set]

EOT : Nesnelerin Extraneti [Extranet of Things]

ETSI :Avrupa Telekomünikasyon Standartlar Komitesi (European Telecommunications Standard Institute)

EVM : Hata Vektörü Büyüklüğü [Error Vector Magnitude]

FDMA : Frekans Bölmeli Çoklu Erişim [Frequency Division Multiplexing Access]

FD : Sürekli İki Yönlü İletim [Full-duplex Transmission]

GPS : Global Pozisyonlama Sistemi [Global Positioning System]

GSM : Global Mobil Sistem [Global System for Mobile]

GSMA : Global Mobil Sistem Kurumu [Global System for Mobile Association]

HDFS : Hadoop Dosya Sistemi [Hadoop File System]

HMI : İnsan Makine Arayüzü [Human Machine Interface]

HTML : Hypertext Markup Language

HTTP : Hypertext Transport Protocol

ICT : BTK [Information and Communication Technology]

ICCID : Entegre Devre Kartı Kimliği [Integrated Circuit Card ID]

IMS : IP Multimedya Sistemi [IP Multimedia Subsystem]

IMSI : Uluslararası Mobil Abone Kimliği [International Mobile Subscriber Identity]

IoT : Nesnelerin İnterneti [Internet of Things]

ISI : Çoklu-sembol Arayüzü [Intersymbol Interference]

IEEE : Elektrik Elektrnik Mühendisleri Kurumu [Institute of Electrical and Electronics Engineers]

IMSI : Uluslararası Mobil Abone Kimliği [International Mobile Subscriber Identifier]

IP : İnternet Protokolü [Internet Protocol]

IPv4 : İnternet Protokolü Dördüncü Versiyon[Internet of Protocol version 4]

IPv6 : İnternet Protokolü Altıncı Versiyon [Internet of Protocol version 6]

ITU : Uluslararası Telekomünikasyon Kurum [International Telecommunication Union]

JMS : Java Mesaj Servisi [Java Message Service]

LPWAN : Düşük Güçlü Dar Alan Ağı [Low Power Wide Area Network]

LTE : Uzun Dönem Evrim [Long Term Evolution]

LoS : Görüş Doğrultusu [Line-of-Sight]

MAN : Metropolitan Alan Ağı [Metropolitan Area Network]

MCKS : Mobil Cihaz Kayıt Sistemi

MNO : Mobil Ağ Operatörü [Mobile Network Operator]

MPA : Mesaj İletme Algoritması [Message Passing Algorithm]

MSISDN : Mobil İstasyona Entegre Dijital Ağ Servisi [Mobile Station Integrated Services Digital Network]

MQTT : Mesaj Sıralayıcı Telemetri Taşıma [Message Queuing Telemetry Transport]

M2M : Makinadan Makinaya [Machine to Machine]

M2X : Makinadan Herhangiye [Machine to Any]

MIMO : Çoklu Girdi Çoklu Çıktı [Multiple Input Multiple Output]

MVN : Mobil Sanal Ağ Operatörü [Mobile Virtural Network Operator]

NACK : Olumsuz Bildirim [Negative-Acknowledgement]

NB-IoT : Dar Bant Nesnelerin İnterneti [Narrow Band Internet of Things]

NOMA : [Dikey Olmayan Çoklu Erişim [Non-orthogonal Multiple Access]]

OEM : Orijinal Ekipman Üreticisi [Original Equipment Manufacturer]

OSI : Açık Sistem Ara Bağlantı [Open System Interconnection]

OFDM : Dikey Frekans Bölmeli Çoklayıcı [Orthogonal Frequency Division Multiplexing]

OFDMA : Dikey Frekans Bölmeli Çoklu Erişim [Orthogonal Frequency Division Multiple Access]

OMA : Dikey Çoklu Erişim [Orthogonal Multiple Access]

OTA : Havada [Over The Air]

QAM : Dördün Genlik Modülasyonu [Quadrature Amplitude Modulation]

QoS : Servis Kalitesi [Quality of Service]

PSD : Güç Sanal Yoğunluğu [Power Spectral Density]

RAN : Radyo Erişim Ağı [Radio Access Network]

RFID : Radyo Frekans Kimliği [Radio Frequency Identification]

SDN : Yazılım Tanımlamalı Ağ [Software Defined Network]

SC-OFDM : Süperpozisyon Kodlamalı Dikey Frekans Bölmeli Çoğullama [Superposition Coded Orthogonal Frequency Division Multiplexing]

SIC : Kendicil Yayılım İptali [Self/Successive Interference Cancellation]

SDR : Yazılım Tanımlamalı Radyo [Software Defined Radio]

SNR : Sinyal Gürültü Oranı [Signal to Noise Ratio]

SSH : Güvenli Kabuk [Secure Shell]

TCP : İletim Kontrol Protokolü [Transmission Control Protocol]

TO : Zamanlama Ayarı [Timing Offset]

UDP : Kullanıcı Veri Birimi Protokolü [User Datagram Protocol]

UMTS : Genel Mobil Telekomünikasyon Sistemi [Universal Mobile Telecommunication System]

URI : Tektip Kaynak Tanımlayıcı [Uniform Resource Identifier]

UFMC : Genel Çok Taşıyıcılı Filtre [Universal Filter Multi-Carrier]

USRP : Genel Yazılım Radyo Ortamı [Universal Software Radio Peripheral]

WAP2 : Kablosuz Ağ Korumalı Erişim2 [Wi-fi Protected Access 2]

WebOS : Ağ İşletim Sistemi [Web Operating System]

XMPP : Genişletilebilir Mesaj ve Yapı Protokolü [Extensible Messaging and Presence Protocol]

V2X : Araçtan Herhangibir Yere [Vehicle to Any-Destination]

VNF : Sanal Ağ Fonksiyonu [Virtual Network Function]

VI : Sanal Araç [Virtual Instrument]

ÖZET

ABONELİK YÖNETİCİSİ GÜVENLİ YÖNLENDİRME SUNUCULARI ARASINDA GÖMÜLÜ EVRENSEL TÜMLEŞİK DEVRE KARTI PROFİLİ TAKAS İŞLEMİNİN OPTİMİZASYONU

YÜKSEK LİSANS TEZİ

Nazif Güray GÜNGÖRDÜ

İstanbul Üniversitesi-Cerrahpaşa

Lisansüstü Eğitim Enstitüsü

Elektrik-Elektronik Mühendisliği Anabilim Dalı

Danışman: Dr. Öğr. Üyesi Bahattin KARAKAYA

Bu yüksek lisans tezi, yeni nesil programlanabilir kullanıcı kimlik kartı profillerinin saklandığı sunucudan yeni sunucuya taşınmasının özel bir prosedürünü anlatmaktadır. Bu tez prosedürün standart üzerinde tanımlanmayan bir metodun doğruluğunu anlamamıza yardımcı olacaktır. EUICC üreticisi olmayan ülkelerde yasal zorunluluklardan dolayı SM-SR sunucusu lokal olmak zorunda olursa, ihtiyaç duyulan profillerin yönetildiği ve kontrol edildiği sunuculardan yerli sunuculara taşınmasını sağlamaktır.

Haziran 2022, 58 sayfa.

Anahtar kelimeler: IoT Bağlantılı Araçlar GSMA Swap eUICC eSIM SM-SR SM-DP

SUMMARY

Optimization of Embedded Universal Integrated Circuit Card Profile Swap Operations in Subscription Manager Secure Routing Servers

M.Sc. THESIS

Nazif Güray GÜNGÖRDÜ

Istanbul University-Cerrahpasa

Institute of Graduate Studies

Department of Electrical and Electronic Engineering

Supervisor: Assist. Prof. Dr. Bahattin KARAKAYA

This is the master thesis aims to explains a special procedure of transferring subscriber identity card profiles from saved servers to the new servers. This thesis will help us to understand the accuracy of a method that is not defined on the standard. If the SM-SR server must be local due to legal obligations in countries that are not EUICC manufacturers, it is to ensure that the required profiles are swapped from the servers where they are managed and controlled to local servers.

June 2022, 58 pages.

Keywords: IoT Connected Cars GSMA Swap eUICC eSIM SM-SR SM-DP

1. GİRİŞ

İletişim, Türk Dil Kurumu sözlüğünde "Duygu, düşünce veya bilgilerin akla gelebilecek her türlü yolla başkalarına aktarılması" olarak tanımlanmaktadır. Yine TDK'nin teknik terim olarak iletişim tanımı ise "Telefon, telgraf, televizyon, radyo vb. araçlardan yararlanarak yürütülen bilgi alışverişi" olarak yapılmıştır. İletişimin temel ögeleri ise, 1) Kaynak, 2) İleti, 3) Kanal, 4) Bağlam, 5) Geri bildirim ve 6) Şifre olarak kabul edilir.

Bu noktada kablosuz iletişimin temel dayanak noktası, iletişimin ana ögelerinden olan kanalın niteliğiyle alakalıdır. Doğada temel iletişim halihazırda canlıların temel duyularından olan duyma kablosuz iletişime güzel bir örnektir. Kaynaktan çıkan ses dalgalarının alıcı tarafından anlamlandırılmasıyla doğada sesle iletişim, hayvanlar arasında gerçekleştirilmektedir. İnsanların kullandığı dumanla iletişim de kablosuz iletişime örnek olarak verebilir.

Teknik tanımıyla iletişimin kablolu telefon, telgraf vb. araçlarla başlayan serüveni, 1897 yılında G. Marconi'nin icat ettiği ve patentini aldığı "kablosuz telgraf" teknolojisi ile ileride yerini bırakacağı kablosuz veri aktarımının gelişkin yöntemlerine doğru değişimini başlatmıştır. Özellikle yirminci yüzyılın son çeyreğinde artmaya başlayan mobil veya diğer bir tanımıyla gezgin iletişimin yarattığı ihtiyaçlar çerçevesinde hücresel haberleşme hususuna talep ciddi miktarda yükselişe geçmiştir. Bu zaman diliminin başlangıcından günümüze kadar gelen süreçte, 1G (yani 1. Jenerasyon), 2G, 3G, 4G teknolojileri geliştirilmiş ve nihayetinde 5G teknolojisi hali hazırda pek çok ülkede kullanılmaya başlamıştır ve üzerinde geliştirmeler devam etmektedir. Hatta günümüzde 6G Çalıştayları [1] yapılmaktadır. Bu yıl ülkemizde Medipol Üniversitesinin ev sahipliğinde ve Aselsan Elektronik A.Ş. sponsorluğunda gerçekleştirildi.

Tarihçesine bakacak olursak, 1G teknolojisi, temelde hareketli telefon görüşmeleri noktasındaki ihtiyacı karşılamak için tasarlanmış, temel taşı ses iletimi olan bir teknolojidir. 1978 yılında ilk örneklerinden birisi ABD'de test edilmeye başlanmıştır. Gelişmiş Taşınabilir Telefon Servisi isimli bu sistemin özellikleri olarak, analog veri akışı olması, parazitlere dayanıklı olmaması, ses harici bir veri taşınmasına ve şifrelemeye elverişli olmayan yapısı

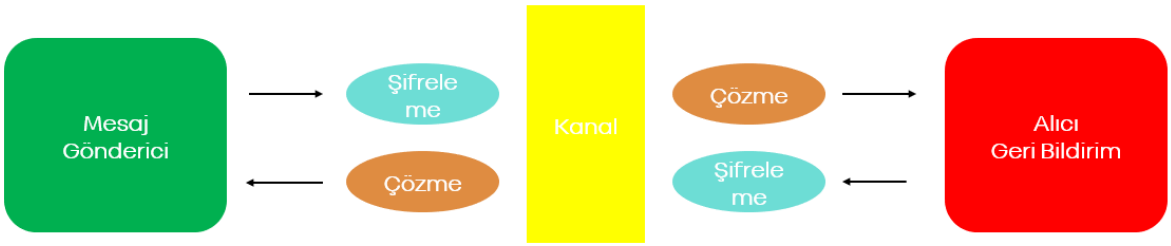
sıralanabilir. Zamanla artan hareketli iletişim ihtiyaçları ve servis kalitesindeki gelişim ihtiyaçlarıyla ortaya çıkan 2G ise sesin yanında kilobayt/saniye düzeyinde veri transferine de olanak sağlamış bu sayede yazılı mesaj iletimleri mümkün kılınmıştır. 3G teknolojisi ise modern çağımızın ihtiyaçları olan video izleme, görüntülü konuşma, müzik dinleme gibi hızlı veri transferi gerektiren işlemler yapılabilir olmaya başlamıştır. Kullanıcı mobil cihaz kullanıcı sayısındaki keskin artış, sosyal medyanın yaygınlaşması, akıllı cihazların kullanımının artması gibi sebeplerle insanların ihtiyaçları ses iletiminden ziyade internet hızı eksenine kaymıştır. 4G teknolojisi bu ihtiyaçları karşılamak doğrultusunda geliştirilmiş olup, öncüllerine göre daha gelişmiş altyapılar ve daha geniş frekans bantları kullanmaya başlanmıştır. Bu aşamada veri hızı günlük ihtiyaçları karşılamakta ancak artan veri trafiği ve veri trafiğinin gün geçtikçe ihtiyacı olan trafik tipi çeşitliliğinin ve karmaşıklığının da artmasıyla birlikte daha yüksek içerikli bir nesle geçişin gerçekleşmesi planlanmaktadır. 5G teknolojisi ise günümüzde ihtiyaç duyulan M2M, IoT ve internet, sesli ve diğer tüm geçmişten devreden kullanıcı ihtiyaçlarını karşılamak üzere ETSI tarafından hazırlanmıştır. 6G teknolojisi ise daha ileri seviyede kullanım alanları henüz oluşturulmakta olan V2X, M2X, HMI teknolojilerinin anlık olarak uygulanması için gerekecek yüksek ve hızlı bant ihtiyaçlarını karşılaması için tartışmaya açılmıştır. Tüm bu ihtiyaçların karşılanması için uygun platformlar ve anlık profil değişikliklerine karşılık verebilecek olan donanım ihtiyacını doğurmuştur. Hem üretim aşamasında hem de sahada kullanım sırasında teknolojinin yarattığı yeni ihtiyaçlara karşılık verebilmesi için önce eSim, daha sonrasında ise eUICC teknolojileri hayatımıza girmiştir. Tüm yeniliklerde olduğu gibi bu yeniliklerde de güvenlik açıkları, güvenlik ihtiyaçları, belirli bir standart ile çalışma ihtiyacı ortaya çıkmış ve bu gereksinimler ve riskler otaya yepyeni standartlar ortaya koymuştur. Yeni tanımlanan senaryolara cevap verilmeye çalışılmış ve prosedürler, profiller, kullanıcı bilgileri garanti altına alınmak istenmiştir. Tezimizde Türkiye ve benzeri siber güvenlik gereksinimi yüksek bölgelerde ortaya çıkan SM-SR, SM-DP sunucularının güven altına alınması ihtiyacından ortaya çıkan, SM-SR sunucular arası profil transferi prosedürü tanımlanmıştır.

2. HÜCRESEL HABERLEŞMENİN VE GSMA

2.1. İLETİŞİM

İletişim, basitçe bir yerden, kişiden veya gruptan diğerine bilgi aktarma eylemidir. Her iletişim (en az) bir gönderici, bir mesaj ve bir alıcı içerir. Bu kulağa basit gelebilir, ancak iletişim aslında çok karmaşık bir konudur. Mesajın göndericiden alıcıya iletilmesi çok çeşitli nedenden etkilenebilmektedir. Tüm bu mesajlar duyguları, kültürel durumu, iletişim kurmak için kullanılan ortamı ve hatta konumu içerir. Bu tanımın da netleştirdiği gibi, iletişim, bilginin iletilmesinden daha fazlasıdır. İster bilgi ister fikir veya duygu olsun, bir mesajı iletmek veya iletmek için bir başarı unsuru gerektirir. Dolayısıyla bir başarılı iletişimin üç bölümü vardır: gönderen, mesaj ve alıcı. Gönderici, mesajı genellikle kelimelerin ve sözlü olmayan iletişimin bir karışımıyla 'kodlar'. Bir şekilde iletilir (örneğin, konuşma veya yazma yoluyla) ve alıcı onu "çözer". Elektronik haberleşme için de iletişim aslında yüz yüze iletişimde olduğu gibi aynen konuşmamızın hava da titreşimler yayarak belirli bir frekansta seslerin anlamlı dizeler halinde iletilerek karşı tarafta dinleyici tarafından çözülmesi gibi gerçekleşmektedir.

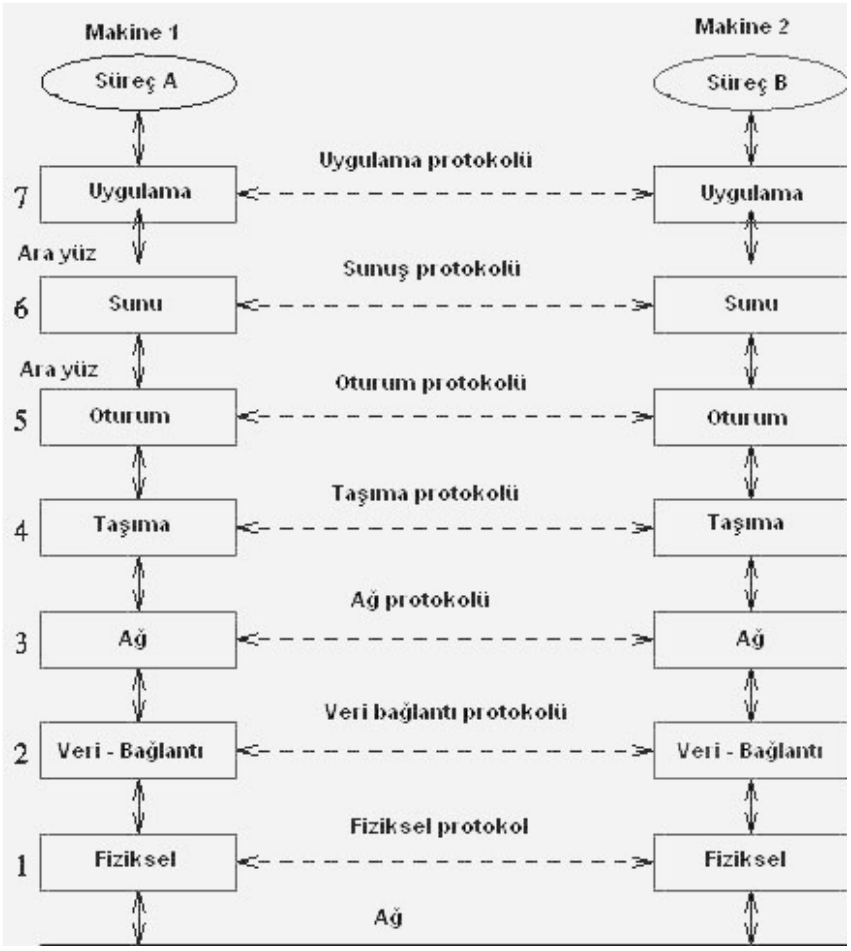
Bu iletişim artık sadece insandan insana değil, makineden makineye (M2M) insandan makineye makineden insana (H2M) ve makinelerde kendi aralarında ayrışıma giderek çok yoğun bir iletişim ağı oluşturmaktadır. Bu iletişim kanalları içerisinde kablolu haberleşme türleri olduğu gibi kablosuz haberleşme türleri de vardır. Örnek olarak WLAN, WiFi, BLE, Hücresel Haberleşme, LoraWPAN ve daha niceleri kablosuz haberleşme türlerine örnek olarak verilebilir. Ancak günümüzde kablosuz haberleşme denildiğinde en önemli ve en yaygın sistem hücresel haberleşmedir.



Şekil 2-1 Temel İletişim

Bu hücresel haberleşmenin doğru ve güvenli bir şekilde gerçekleşmesi için uyulması gereken kriterler ve yöntemler vardır. Öncelikle bu iletişimin hangi katmanlardan geçerek gerçekleştiğini görmek gerekir. Burada iletişim katmanları arasındaki ilişkileri ve katmanların konuları açmak gereklidir, çünkü bağlantılı araç teknolojilerinde kullanılan sistemlerin altyapısında yer alan OSI seviyesi iletişim katmanları, farklı modülasyon teknolojilerinin gelişimiyle birlikte hızların ve bant kapasitelerinin yükselişi anlatılacaktır. Her bir yeni nesil hücresel iletişimin modülasyon yazılım ve donanım ihtiyaçları değişmektedir. Bu tezimde özellikle dördüncü nesil hücresel haberleşme teknolojisinin hayatımıza girmesinden sonra abone profillerinin yönetilmesi için daha pratik ve hızlı araçlara ihtiyaç duyulmuştur. Tekil ve çoğul abonelerin profillerinin insan hatasından arındırılmış ve çok daha hızlı bir şekilde yönetildiği sunucular ve bu sunucuların dünya genelinde standart bir şekilde hizmet alabildiği içerik de tarihsel olarak beraberinde hücresel haberleşme sisteminde konumlandırılmıştır.

2.1.1. İletişim Katmanları



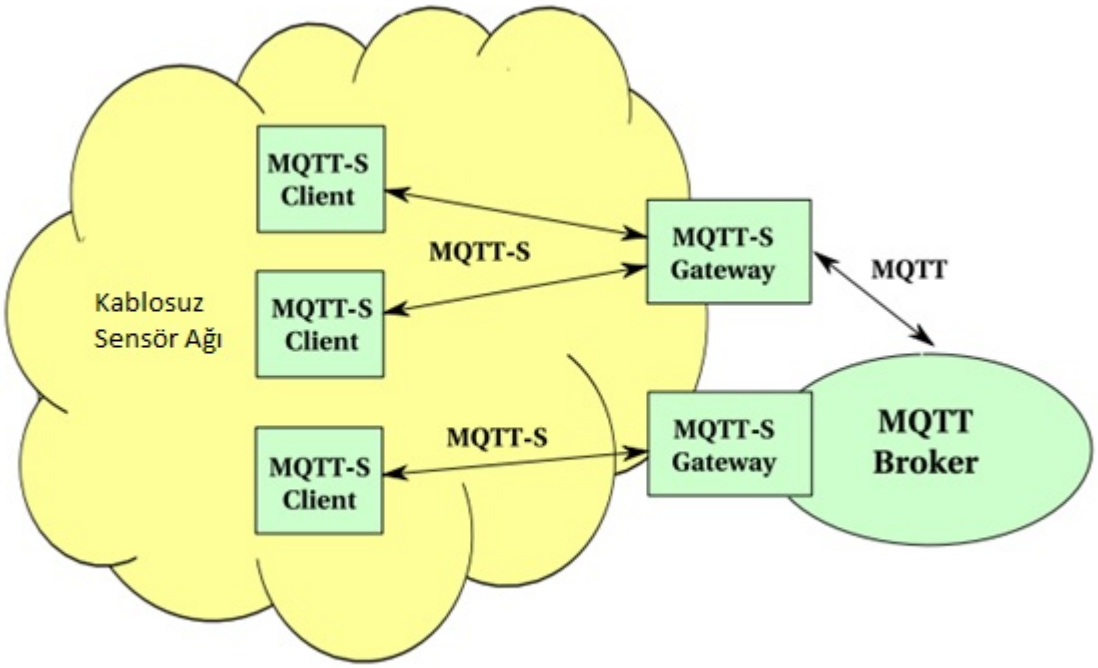
Şekil 2-2 OSI Katmanları [2]

OSI katmanları bizim konumuzun anlaşılması için önem taşımaktadır. Bu katmanlar Şekil 2-1'de gösterilmektedir. Modülasyonun uygulanacağı verinin yapısı büyüklüğü gönderilme hızı sistemin ihtiyaçları karşılayabilmesi açısından önem taşımaktadır. Bahsi geçen sistem 5G olduğundan dolayı fiziksel katmanımız Wireless yani kablosuz haberleşme altyapısıdır. Wireless üzerinde bizim modülasyonumuzun en çok etkileneceği katman "Transport Layer" yani taşıma katmadır. Bu katmanda verinin bir transfer mi yoksa akış mı olacağı kullanılacak protokolün TCP/UP mi UDP/IP mi olacağını belirleyecektir. Akış verileri UDP ile, transfer bilgileri ise TCP ile taşınacağından dolayı iletim hızları ve doğrulama yapıları değişecektir. Tüm bu ekosistem içerisinde farklı kapsama alanlarındaki farklı üyeler farklı ihtiyaçlar ve farklı talepler ile ekosistemden faydalanacaklardır.

2.1.2. IoT Protokolleri

IoT Protokolleri aşağıda detaylı olarak anlatılmaktadır [3].

MQTT

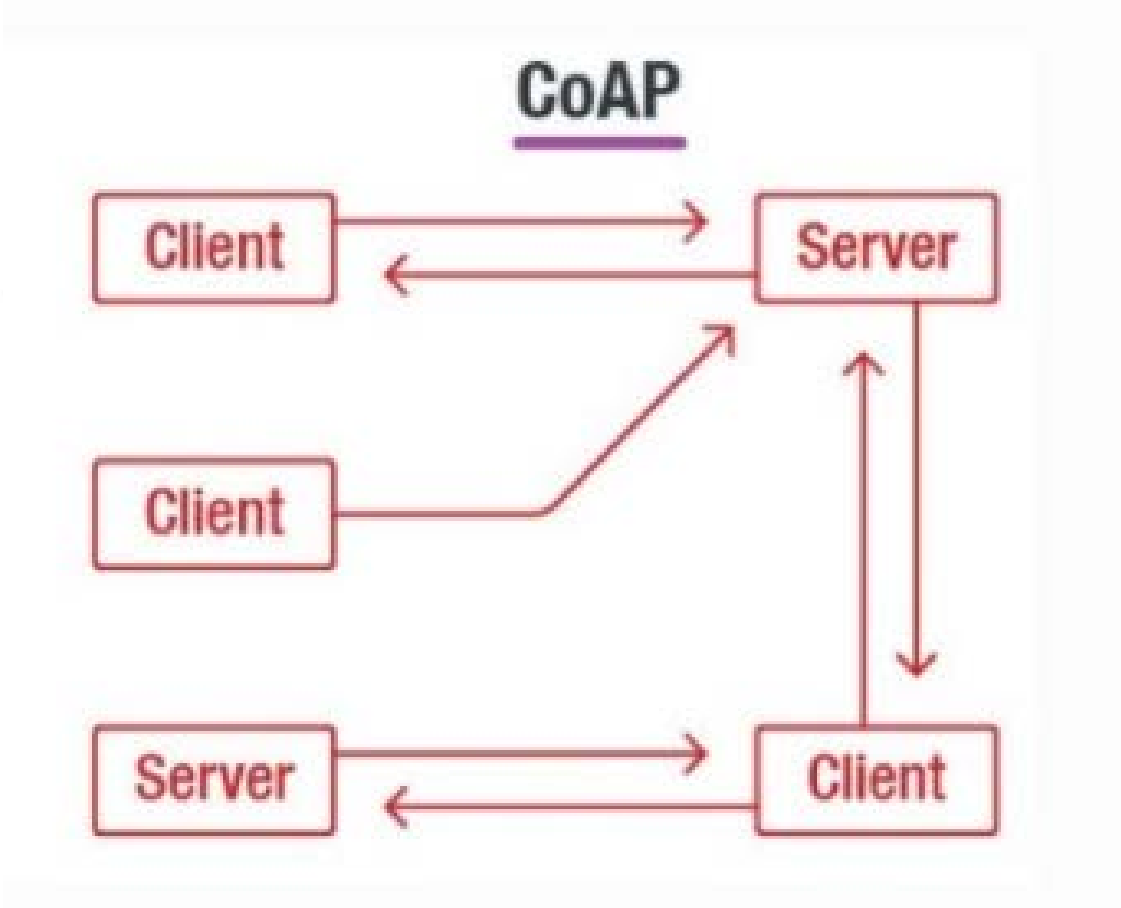


Şekil 2-3 MQTT Protokolü Haberleşme Mimarisi [4]

MQTT, uygulama katmanında çalışan fiziksel olarak dağınık cihazlar arasında asenkron veri alışverişi için her kullanıcının kullanımına uygun, açık bir protokoldür [4]. MQTT ön tanımlı olarak 1883 portu ile iletişime geçmektedir [5]. Soket bağlantısı kurulurken 1883 portunu kullanmasına rağmen SSL için 8883 portu kullanılarak ön tanım ayarlarından ulaşılabilmektedir. Ses veya video verilerini aktarmak için uygun değildir. MQTT, veri paketi boyutunu küçültme ihtiyacı olduğunda ve kanal bant genişliği sınırlamaları olduğunda kullanılır. Bu nedenle MQTT genellikle endüstriyel IoT çözümleri ve M2M sistemleri için temel olarak kullanılır. Bizim de konumuz olan bağlantılı araçlarda MQTT protokolü kullanılmaktadır. Bu protokol, veri paketlerini küçülterek sistem üzerindeki baskıyı azaltmaktadır. Kaotik ağ bağlantılarında, zayıf anten gücü (alıcı ya da verici) ortamlarında dahi yüksek performans ve enerji tasarrufu altında çalışabilmektedir. Servis kalitesinin birkaç seviyesini desteklemektedirler. Bu sayede farklı seviyelerdeki veri güvenliği ACK ve NACK yapılarını destekleyebilmektedirler. Yeni cihazların entegrasyonunu hızlı ve basit hale

getirmektedirler. Veri aktarımının güvenli olmasını sağlamak için MQTT, abone kimlik doğrulamasını, abone üzerinden müşteri erişim kontrolünü ve TLS / SSL bağlantısını etkinleştirir.[6]

COAP



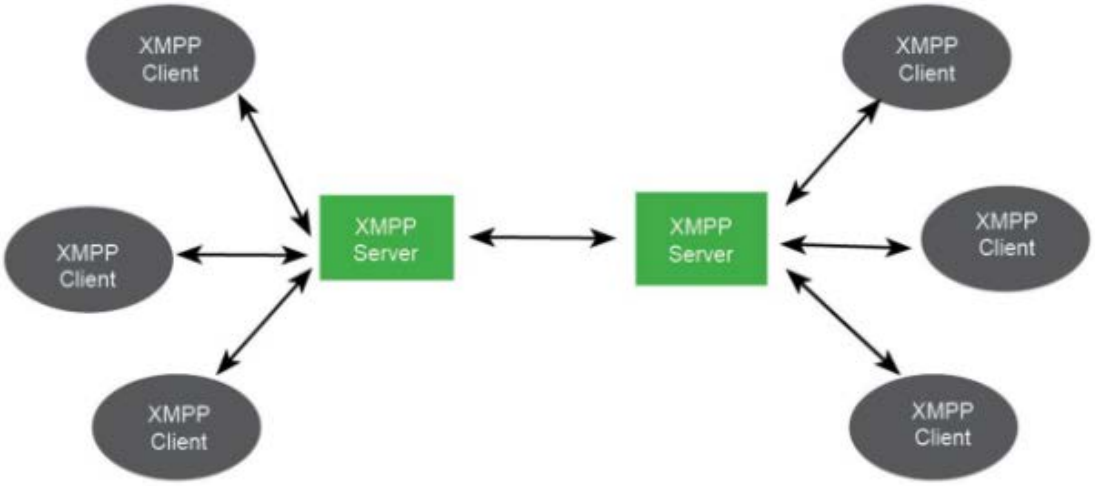
Şekil 2-4 CoAP Haberleşme Mimarisi [7]

CoAP (Sınırlı Uygulama Protokolü), sınırlı kontrol işlevselliği ve RAM içeren cihazlar tarafından kullanılmak üzere yaratılmıştır. Genel olarak IoT çözümleri ve özellikle M2M'ler bu tip iletişim protokolünü kullanmaktadırlar. Varsayılan olarak, CoAP protokolünde verilerin güvenliğini sağlamak için DTLS tekniği kullanır.

Bu protokol REST modeline dayanmaktadır. GET, PUT, POST ve DELETE yöntemlerini kullanarak bir URL'yi ayrıştırma gibi standart işlemlerin yürütülmesine izin vermektedir. Protokolün IoT çözümlerine uygun olmasının temel nedeni, CoAP protokolünün, 100 KB’den

daha az RAM'a sahip cihazların özelliklerini dikkate alacak şekilde tasarlanmış olmasıdır. CoAP, UDP protokolünü kullanır. Bu nedenle, sunucuların durumları kaydetmesi ve saklaması gerekmez.

XMPP



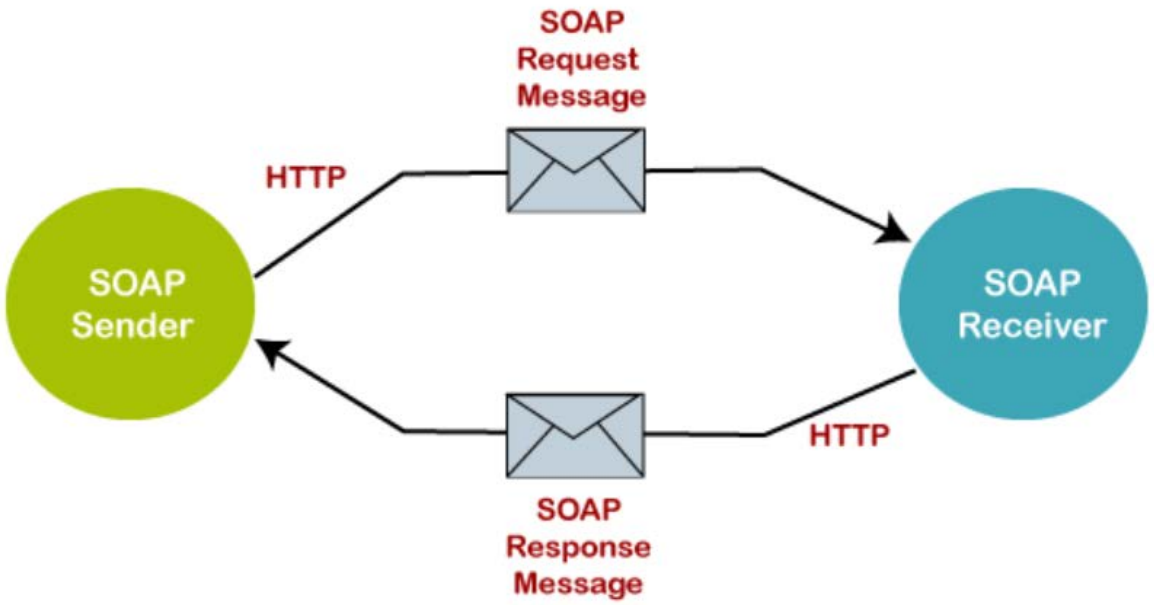
Şekil 2-5 XMPP Protokolü Haberleşme Mimarisi [8]

Şekil 2-5'te XMPP (Genişletilebilir Mesajlaşma ve Durum Protokolü) genellikle veri paketi alışverişlerinde gerçek zamanlı olarak kullanılır. XML formatını desteklemesi sayesinde, IoT çözümlerinde kullanım için mükemmeldir. XMPP protokolüne dayanan ağlar, yüksek hata toleranslarını gerçekleyebilmek için merkezden uca doğru önem sırasına göre dizilmiştir. İletişimin merkezinde her zaman server vardır. Aboneler ise bu server yapılarına kaydolarak iletişimlerini sağlamaktadır.

Güvenlik için, XMPP ağları genellikle SASL ve TLS protokollerinin yardımını kullanmaktadır. Bunun yanı sıra, bazı XMPP tabanlı IoT çözümleri şifreleme amacıyla PGP / GPG de kullanabilmektedir.

XMPP, son derece esnek çözümler için temel olarak kullanılabilir. XMPP Software Foundation, kaynak dağıtmaya, IoT cihazlarıyla çalışmaya ve durumlarını izlemeye vb. Dahil olmak üzere çok sayıda uzantıyı destekler.

SOAP



Şekil 2-6 SOAP Protokolü Haberleşme Mimarisi [9]

Sekil 2.6'da görüldüğü üzere SOAP (Basit Nesne Erişim Protokolü), dağıtılmış bir bilgi işlem sisteminde yapılandırılmış XML mesajları biçiminde veri alışverişinde bulunmak için daha yaygın olarak kullanılan bir protokoldür. SOAP, XML diline dayanır ve HTTP, FTP ve SMTP gibi uygulama katmanında çalışan bazı protokolleri genişletir. Dahili hata tespiti, bu protokolün en önemli özelliğidir.

Ancak, gereksiz yere büyük bir mesaj boyutu SOAP'ın dezavantajıdır. Bu protokolün yerel çözümler için daha uygun olmasının nedeni budur.

Kullanım durumlarına gelince, SOAP iş başvurusu gereksinimleri için mükemmel bir eşleşmedir. Bunun nedeni, bu protokolün veri alışverişi güvenliği için yüksek ayarlanmış bir çubuğa sahip olmasıdır.

UPNP

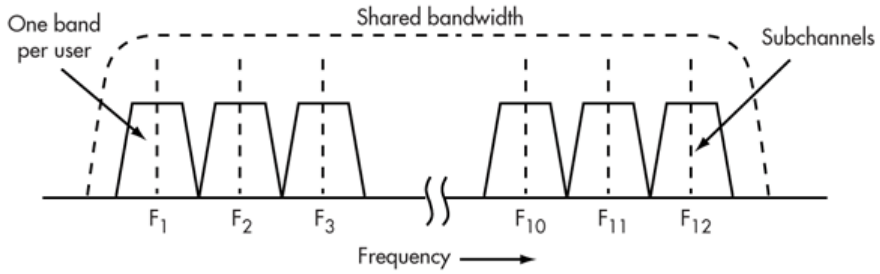
UPnP (Evrensel Tak ve Kullan), Tak ve Kullan izinlerinin ve protokollerinin bir uzantısıdır. TCP / IP, HTTP ve DHCP gibi veri aktarımı için standart protokolleri kullanır [10]. Evrensel yaklaşım, UPnP'nin herhangi bir ek sürücü gerektirmeden hem kablolu (örneğin Ethernet,

Firewire) hem de kablosuz (örneğin WiFi, Bluetooth) bağlantı kurmasını sağlar. Bu, işletim sistemi, programlama dili, ürün tipi veya üreticisine bakılmaksızın UPnP ile uyumlu tüm cihazların veri aktarımında yer almasını sağlar. Bununla birlikte, bu protokolün bütün avantajlarına rağmen, belirli güvenlik riskleriyle birlikte gelir. Sorun şu ki, Evrensel Tak ve Çalıştır, ağdaki her cihazın varsayılan olarak güvenilir ve kolay olduğu varsayımıyla oluşturulduğundan herhangi bir kimlik doğrulama gerektirmez. Bu nedenle, bir aygıta kötü amaçlı yazılım bulaşırsa, tüm sistem tehlikeye girer ve veri paketleri ele geçirilir.

2.1.3. Çoğullama (Multiplexing)

Elektronik, telekomünikasyon veya bilgisayar ağlarında birden fazla analog sinyallerinin veya dijital bilgi aktarımlarının (Dijital Data Akışı) birleştirilip tek bir sinyal haline getirilmesidir. Örneğin elektronik cihazlarda çoğullama birden fazla analog sinyallerinin dijital sinyale evirilip (analogdan dijitale ADC) işlenmesini sağlanır. Birden fazla kullanıcının aynı bağlantı üzerinden haberleşmesi sağlanmaktadır. OSI seviyelerinde çoğullama TCP ve UDP seviyesinde gerçekleşmektedir. Çoklu erişimin temelinde çoğullama mantığı yatmaktadır.

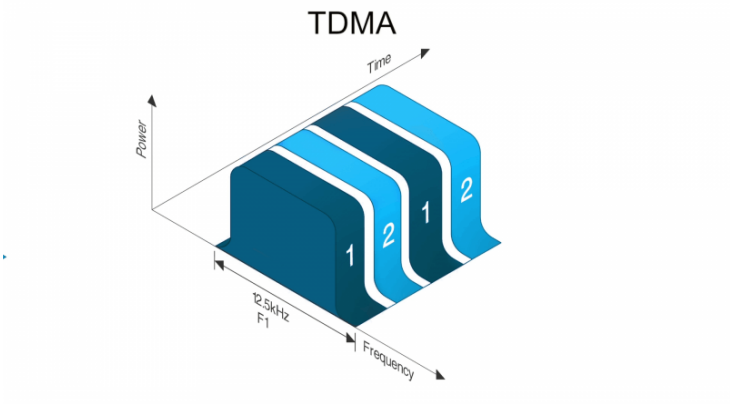
2.1.4. Frekans Bölmeli Çoklu Erişim (FDMA)



Şekil 2-7 FDMA Çalıma Prensibi [11]

Bu tip modülasyonlar iletişimde gerçek anlamda veri transferinin gerçekleştirilmesinin başlangıcı oldu diyebiliriz [12, 13]. Frekans üzerinde bandı kullanıcılara bölerek bandın kullanıcılar arasında paylaşılmasını sağlamaktadır. Bir kanalı veya bant genişliğini, her biri tek bir kullanıcı tarafından kullanılmak üzere çoklu bireysel bantlara bölme işlemidir Şekil 2-7. Her bir bant veya kanal, yayılacak olan iletimlerin sinyal spektrumlarını barındıracak kadar geniştir. İletilecek veriler her bir alt taşıyıcıya modüle edilir ve hepsi birlikte doğrusal olarak karıştırılır.

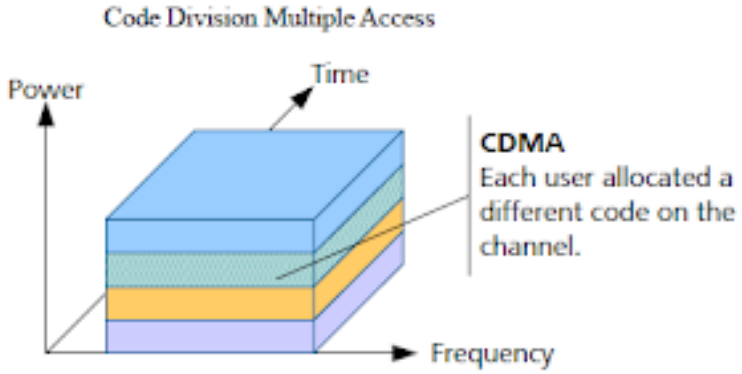
2.1.5. Zaman Bölmeli Çoklu Erişim (TDMA)



Şekil 2-8 TDMA (frekans genişliği temsilidir) [14]

TDMA sisteminde kanallar yani haberleşme bantları kullanıcılara frekans düzleminde değil, zaman düzleminde paylaştırılır Şekil 2-8. Tüm kullanıcı cihazlarına ayrı ayrı bir kanal atanır ve her zaman parçacığının kullanıcılara nasıl atanacağını belirlenmesi ilkesine dayanır. Bu kanallar da sonrasında bir TDMA içerisinde erişime açılır. Bu durumda TDMA kapasitesi TDMA içerisindeki zaman dilimini bölme yeteneğimize bağlı olacaktır. Sistemdeki tüm cihazlara bir zaman dilimi tahsis edilmelidir. TDMA sistemleri normalde dijitaldir ve bu nedenle şifreleme ve bütünlük gibi ek özellikler sunar. Bu, sistemin gürültüye ve parazite daha dayanıklı olmasını sağlar ve bu nedenle FDMA sistemlerine kıyasla daha yüksek spektral verime sahiptir.

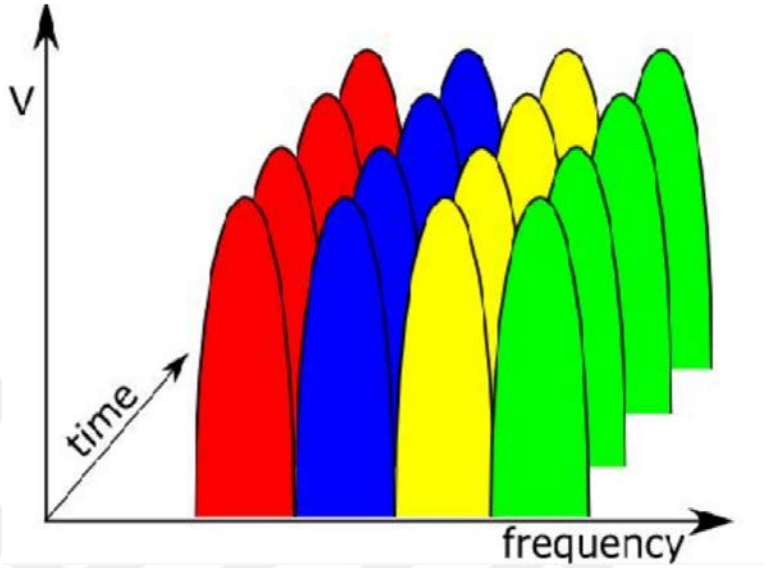
2.1.6. Kod Bölmeli Çoklu Erişim (CDMA)



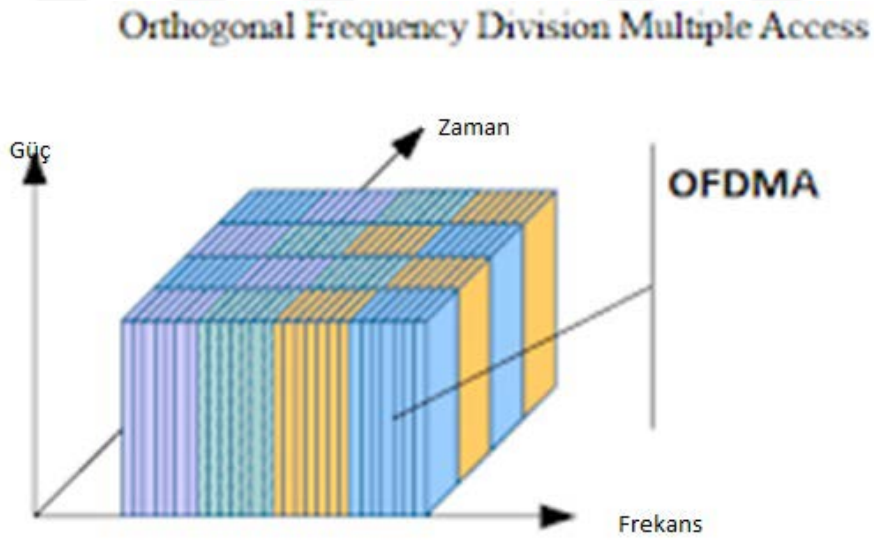
Şekil 2-9 CDMA [15]

Kod Bölmeli Çoklu Erişim sistemi zaman ve frekans çoğullama işleminden çok farklıdır. Bu sistemde, bir kullanıcı, tüm süre boyunca bütün bant genişliğine erişebilmektedir. Temel ilke, farklı kullanıcıları ayırt etmek için farklı CDMA [16] Şekil 2-9 kodlarının kullanılmasıdır. Kullanıcı hem zaman düzleminde hem de frekans düzleminde yer alabilir. Burada kullanıcıya ayrılan alan kullanıcın kodunun işaretli olduğu zaman ve frekansın işaret edildiği alanı seçebilen kod tanımlı alanlardır. Şekil 2-9 üzerinde görüleceği üzere her kullanıcı zaman bölgesinin ve frekans bölgesinin her yerinde yer alabilmektedir.

2.1.7. Dik Frekans Bölmeli Çoklu Erişim (OFDMA)



Şekil 2-10 OFDMA zaman frekans düzlemi [17]



Şekil 2-11 OFDMA-2 [17]

OFDMA LTE'nin temel öğelerinden biridir. OFDM'ye (Ortogonal Frekans Bölmeli Çoklama) dayanan çoklu erişim tekniği sağlar. Bant genişliğinin “alt taşıyıcılar” olarak bilinen daha küçük

birimlere bölündüğü görülebilir. Bunlar birlikte gruplandırılır ve bir aygıta kaynak olarak atanır. Bir cihazın hem zaman hem de frekans alanında farklı kaynaklar tahsis edilebileceği de görülebilir Şekil 2-10. OFDMA 4G temelli haberleşmenin bel kemiğidir. Günümüz dünyasında GSM teknolojisinin sağladığı yüksek hızlı veri erişimine olanak sağlamaktadır. Bu modülasyon ile FDMA ve TDMA melezi bir modülasyona gerçek anlamda her kullanıcı için ayrı ayrı imkân verilmiştir. Kullanıcılara kanallar tek bir zaman adımı ya da frekans bandı üzerinden verilmez. Her kullanıcının hem zamanda hem de frekansta ataması değişkendir ve böylece birim zamanda gönderilebilen veri miktarı maksimize edilmiş olunur. Burada Şekil 2-11'de göreceğimiz üzere her kullanıcı için zaman ve Frekans alanı değişkendir. Ancak kullanıcı başına çıkış gücü her biri için sabittir. Yani erişim için ayrılan kaynaklar üçüncü düzlem olan güç alanında her kullanıcı için ortogonaldir yani her bir zaman frekans alanı kullanıcı başına dağıtılmıştır.

2.1.8. NOMA

Buraya kadar bahsettiğimiz tüm modülasyon tekniği örneklerinde sitemlerin tamamı dikleştirilmiş (Ortogonal) sitemlerdi. FDMA 1G, TDMA 2G, CDMA 3G, OFDMA ise 4G teknolojilerinin temel yapı taşı sayılmaktaydı [18]. FDMA ve TDMA 1 boyutta, CDMA ve OFDMA iki boyutta kullanıcı ayrımı yapabiliyordu. Şimdi ise NOMA ile 3 boyutlu bir kullanıcı ayırt etme imkânımız ve buna bağlı olarak kanalı çok daha yüksek hızlarda, çok daha verimli kullanma imkânımız bulunmaktadır.

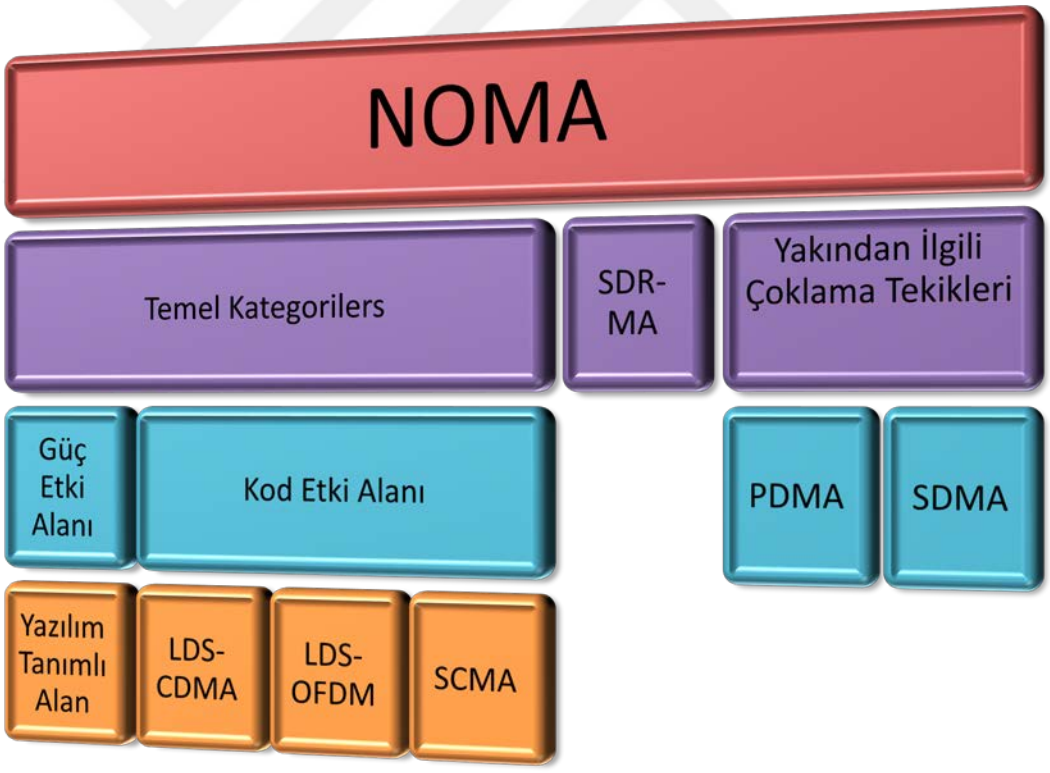
NOMA'yı ele aldığımız zaman karşımıza temel olarak iki farklı tipte inceleme metodu çıkmaktadır. Bunlar "Güç Alanı Çoğullama" ve "Kod Alanı Çoğullama" metotlarıdır. Güç ekseninde farklılık gösterdiğimiz dikleştirilmemiş çoklu erişim sistemlerinde, gücü farklı kullanıcılara farklı katsayılar ile sunmayı planlamaktayız. Bu durumda çok sayıda abonenin bilgi sinyalleri güç ekseni üzerinde üst üste binmektedir. Alıcı tarafında SIC (Ardışık Girişim İptali) ile gerekli filtrelemeler elemeler yapılarak, sinyaller çözümlenir. Böylece hem sistem daha verimli şekilde kullanılmış olacaktır, hem de aboneler arasında denge kurulmuş olacaktır.

Kod alanı çoğullama işleminde, farklı kullanıcılara farklı kodlar atanır ve çok kullanıcılı paylaşılan erişim (MUSA) [19, 20] seyrek kod çoklu erişim (SCMA) ve düşük yoğunluklu yayılma (LDS) [21] gibi aynı zaman-frekans kaynakları üzerinde çoklanır. Kod alanı çoğullama, spektral verimliliği arttırma potansiyeline sahip olmasına rağmen, yüksek bir

aktarım bant genişliği gerektirir ve mevcut sistemlere kolayca uygulanamaz. Öte yandan, güç etki alanı çoklaması, mevcut ağlarda önemli değişiklikler gerekmediğinden basit bir uygulamaya sahiptir. Ayrıca, spektral verimi arttırmak için ek bant genişliği gerektirmez.

Noma Temelleri

NOMA için temel olarak iki ayrı yaklaşım bulunmaktadır. Şekil 2-7 üzerinde göreceğimiz mevcut NOMA tekniklerinin basit bir sınıflandırmasını sunumunu görebiliriz. Güç etki alanında çoklama sağlayan NOMA çeşidinin [7] aksine kod etki alanında çoklama sağlayan NOMA kod etki alanında çoklama sağlamaktadır. CDMA sistemleri gibi kod etki alanında etkili NOMA mevcut tüm bileşenlerini sitemde kullanır. Buna karşılık, kod-alanı NOMA, seyrek diziler veya düşük korelasyon katsayısının ortogonal olmayan çapraz-korelasyon dizileri olan kullanıcıya özel yayılma dizilerini kullanır. Bu durum bize farklı CDMA metotlarını kullanma imkânı sağlayabilir.



Şekil 2-12 NOMA Temelleri

Düşük yoğunluklu kod etki alanlı çoğullama CDMA (LDS-CDMA) [18, 20], düşük yoğunluklu OFDM (LDS-OFDM) [21, 22] ve seyrek kod gibi birkaç farklı sınıfa ayrılabilir çoklu erişim (SCMA) [23, 19] bunlara örneklerdir. Düşük yoğunluklu yayılma dizilerinin kullanılması,

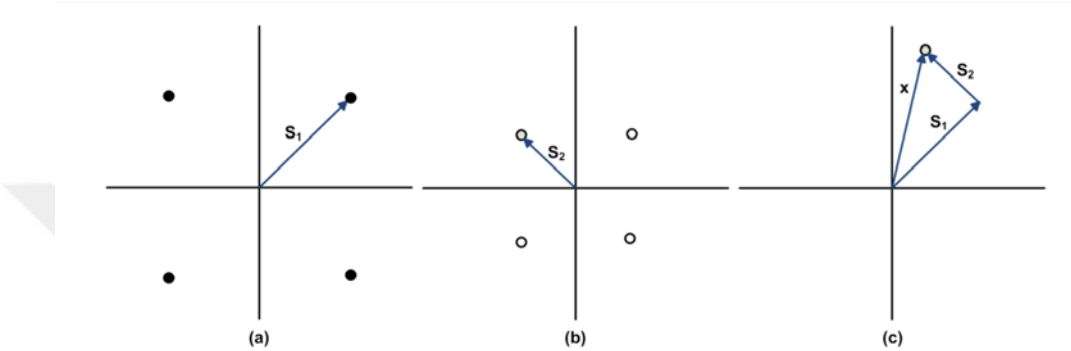
LDS-CDMA'nın, her bir temel CDMA sistemi çipi üzerindeki girişimin etkisini sınırlamasını sağlar. LDS-OFDM, bilgi sembollerinin ilk önce düşük yoğunluklu yayılma dizilerine yayıldığı ve sonuçta ortaya çıkan çiplerin bir dizi alt taşıyıcıya iletildiği LDS-CDMA ve OFDM'nin bir birleşmesi olarak düşünülebilir. SCMA [23, 24], LDS-CDMA'yı temel alan yeni bir kod alanı NOMA tekniğidir. LDS-CDMA'nın aksine, bilgi bitleri doğrudan farklı seyrek kodlayıcırlar ile eşleştirilebilir, çünkü hem bit eşlemesi hem de bit yayılımı birleştirilir. LDS-CDMA ile karşılaştırıldığında, SCMA performans olarak daha iyidir ve alıcı tarafındaki karmaşıklığı düşüktür.

Bunların dışında desen bölmeli çoklu erişim (PDMA) [25] ve mekânsal bölmeli çoklu erişim (SDMA) [26 - 29] dahil olmak üzere NOMA ile de yakından ilişkili başka çoklu erişim teknikleri de vardır. Örnek olarak PDMA, çeşitli alanlarda gerçekleştirilebilir. Verici tarafında, PDMA ilk önce çeşitliliği maksimuma çıkarır ve ortogonal olmayan desenler tasarlamak için birden fazla kullanıcı arasındaki örtüşmeyi en aza indirir. Çoklama daha sonra kod alanında, uzaysal alanda veya bunların bir kombinasyonunda gerçekleştirilir. SDMA için çalışma prensibi, temel CDMA sistemlerine benzetilmiştir. Kullanıcıya özgü yayılma dizileri kullanmak yerine, SDMA, kullanıcıya özel kanal dürtü yanıtları (CIR'ler) kullanarak farklı kullanıcıları ayırt eder. Bu teknik özellikle yukarı bağlantı kullanıcılarının sayısının BS'deki karşılık gelen alıcı antenlerin sayısından oldukça fazla olduğu durumlarda faydalıdır. Ancak, doğru CIR tahmini çok sayıda kullanıcı için zorlu hale gelir. Çoklu erişim için yazılım tanımlı radyo (SDR-MA) kavramı, çeşitli NOMA planlarının bir arada bulunmasına izin verir [25]. Bu teknik, 5G'deki heterojen hizmetleri ve uygulamaları desteklemek için çoklu erişim programlarına katılan esnek bir yapılandırma sağlar. Yukarıda belirtilen erişim tekniklerinin henüz çalışma aşamasında olan NOMA'nın farklı biçimleridir. Bu çalışmamızda NOMA'nın tanımlanmış kısmı olan, güç etki alanı altındaki konuları incelenmiştir.

Süper-Pozisyon Kodlaması (SC)

İlk kez [24]'da önerilen SC, bilgiyi aynı anda birkaç alıcıya tek bir kaynaktan iletme tekniğidir. İngilizce olarak "Fan-Out" olarak nitelendirilen haberleşme yapısıdır [30]. Başka bir deyişle, vericinin aynı anda birden fazla kullanıcının bilgilerini iletmesine izin verir. Buna örnek olarak televizyon yayınlarını verebiliriz. Üst üste bindirilmiş kanallardan her kullanıcı kendi istediği bilgiyi ayıklayarak alır. Aynı şekilde otomobillerin içerisinde kullanılan CAN hattı tüm mesajı taşırken ilgili modüller istedikleri ve bağlı oldukları bilgiyi süzerek almaktadırlar. SC'yi pratik

yapmak için, vericinin her kullanıcıyla ilgili bilgileri kodlaması gerekir. Örneğin, iki kullanıcılı bir senaryoda, vericinin ilgili girişlerini iki kullanıcılı sinyalin karmaşık değerli sekanslarına eşleyen iki noktadan noktaya kodlayıcı içermesi gerekir. SC'nin nasıl gerçekleştirildiğini göstermek için, Şekil 2-13'de şematik bir diyagram verilmiştir, burada yüksek iletim gücüne sahip olan kullanıcı 1'in dörtlü faz-kaydırma (QPSK), düşük iletim gücüne sahip olan kullanıcı 2'nin üzerine bindirilmiştir.



Şekil 2-13 SC Süper-Pozisyon örneği(a) kullanıcı 1 (b) kullanıcı 2 x ise süprepoze sinyal olarak tanımlanır.

[31]'e göre SC'nin skaler bir Gauss yayın kanalında kapasiteye ulaşan, ortogonal olmayan tanınmış bir şema olduğu söylenebilir. Süper-pozisyon kodlama aşamasında, iki noktadan noktaya kodlayıcı, $f1:\{0,1\}^{|2^{TR_1}|} \rightarrow c^T$ ve $f2:\{0,1\}^{|2^{TR_2}|} \rightarrow c^T$ilk önce ilgili giriş bitlerini sırasıyla blok çıkış uzunluğunun her biri olan iki çıkış bit dizisine S_1(n) ve S_2(n) işler. Burada, sırasıyla kullanıcı 1 ve kullanıcı 2'nin iletim hızlarını ve (and .) yer operatörünü temsil eder. C bir kod kütüphanesinden başka bir şey değildir. Ardından sinyaller üst üste toplanarak aşağıdaki gibi bir seri elde edilir [31].

$$X(n) = \sqrt{P\beta_1}S_1(n) + \sqrt{P\beta_2}S_2(n) \qquad (2.1)$$

Burada P toplam güç β_1 ve β_2 örnekte verilen iki sinyalin toplan güce oranını vermektedir.

Ardışık Girişim İptali (SIC)

Üstteki bilgilerin her alıcıda kodunun çözülmesi için, SIC yöntemi önerilmiştir. İlgilenilen sinyaller arasındaki sinyal gücündeki farklılıklar kullanılarak sinyallerin ayrıştırılması sağlanabilmektedir [31]. SIC'in temel fikri, kullanıcı sinyallerinin art arda kodunun çözülmüş olmasıdır. Bir kullanıcının sinyalinin kodu çözüldükten sonra, bir sonraki kullanıcının

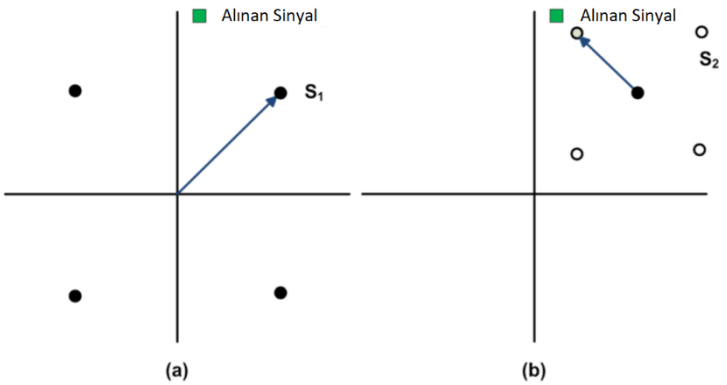
sinyalinin kodu çözülmeden önce birleşik sinyalden çıkarılır. SIC uygulandığında, kullanıcı sinyallerinden biri çözülür, ilk çözülen sinyal geri kalan sinyal dizisine gürültü olarak eklenmiş gibi düşünülerek sinyaller toplamından çıkartılır. Bu işlem son sinyal elde edilene kadar tekrarlanarak bütün sinyal dizisi elde edilmiş olur. Bununla birlikte, SIC'den önce, kullanıcılar sinyal güçlerine göre sıralanırlar, böylece alıcı önce daha güçlü sinyalin kodunu çözebilir, onu birleştirilmiş(X(n)) sinyalden çıkarabilir ve zayıf olanı kalan sinyal bileşeninden ayrıştırabilir. Şekil 2-14, alıcı taraftaki üst üste gelen sinyalin Şekil 2-13 kodunu çözme tekniğini göstermektedir. Öncelikle birinci sinyal çözümlenmiş ve tüm sinyalden çıkartılmıştır. Daha sonrasında kalan sonuncu sinyal ilk sinyale göre çözümlenebilmiştir. SIC'in genel olarak kablosuz iletişimde ve OFDM'de (ve MIMO) sıklıkla kullanıldığından bahsedilmiştir [31]. Kısaca, üst üste gelen mesajların kodunun çözülmesine dahil olan belirli süreç matematiksel olarak şu şekilde ifade edilebilir:

Birinci kullanıcıyı çözümlemek için tek kullanıcılı kod çözücü sisteme uygulanarak: $g_1: C^T \rightarrow \{0,1\}^{2^{TR_1}}$ $S_1(n)$ sinyali ve $S_2(n)$ gürültü olarak algılanarak çözümlenecektir. Birinci sinyalin güç bileşeni $\sqrt{P\beta_1}S_1(n)$ sinyalin tamamından çıkartılır [31].

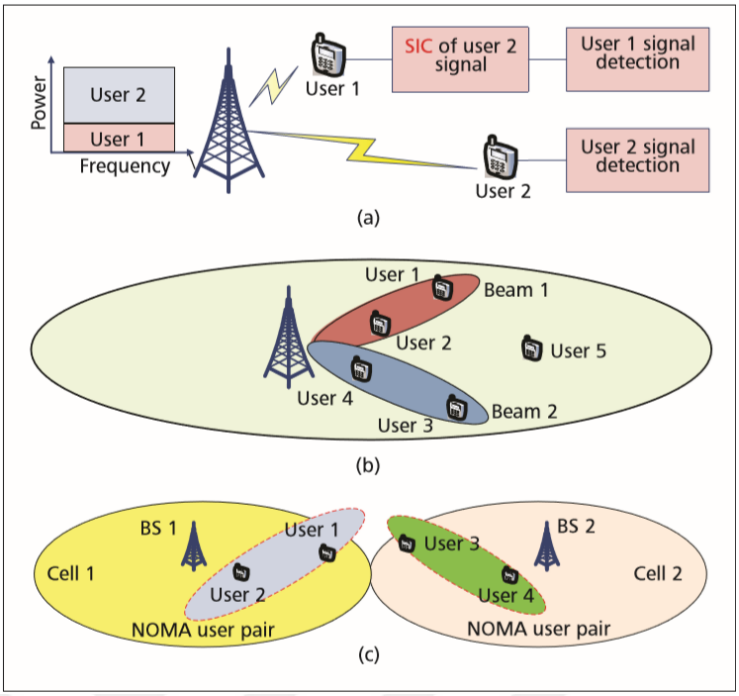
$$\gamma_2'(n) = \gamma_2(n) - \sqrt{P\beta_1}S_1(n)h_2 \tag{2.1}$$

Burada h_2 ikinci sinyal üzerindeki kanal kazancını belirtmek için kullanılmıştır.

Burada ikinci sinyali $S_2(n)$ ise $g_2: C^T \rightarrow \{0,1\}^{2^{TR_2}}$ $\gamma_2'(n)$ üzerinde tek kullanıcılı kod çözücü uygulayarak çözümleyebiliriz.



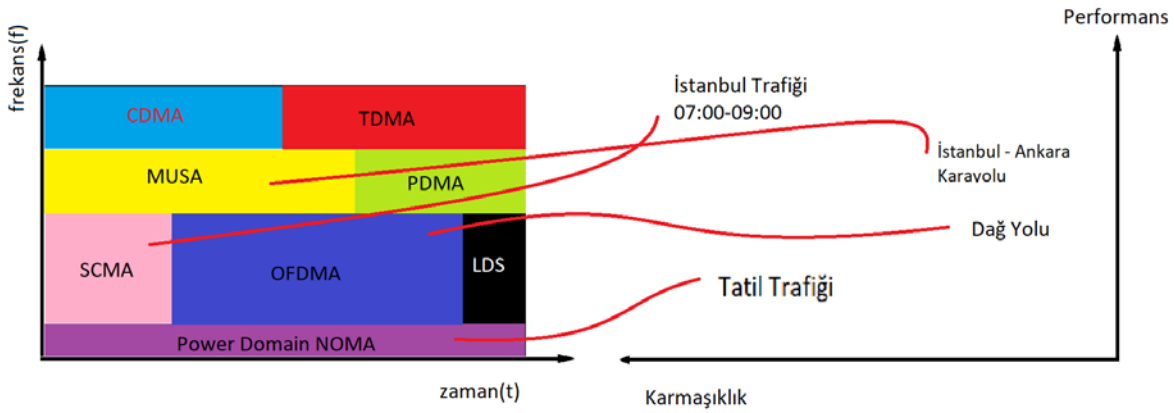
Şekil 2-14 SIC ile izole edilmiş sinyaller [31]



Şekil 2-15 NOMA SIC Kullanım Görseli [31]

2.1.9. SODEMA

Bahsettiğimiz gibi NOMA bağlantılı araç teknolojilerinin içinde bulunduğu ağın kapasitesinin arttırılmasında ve 5G'deki çok büyük ölçekli bağlantılar için kullanılabilir bir yöntem olarak görülmektedir. Bununla birlikte, bu, gelecekteki 5G ağlarında geleneksel OMA şemalarının NOMA ile tamamen yer değiştirileceği ve NOMA'nın tamamen OMA'nın yerini alacağı anlamına gelmemektedir. Örnek olarak, kullanıcı sayısının çok az olduğu ve hücre alanlarının küçük olduğu kullanımlarda, OMA daha iyi bir seçim olacaktır. Bu bağlamda hem OMA hem de NOMA, farklı servis ve uygulamaların farklı gereksinimlerini karşılamak için 5G'de bir arada bulunacaktır. Bu amaçla, farklı NOMA şemalarının hepsinin 5G standartlarında belirtileceğini varsayarak bir sistemde bir arada bulunabileceğini Şekil 2-16'da gösterildiği gibi 5G için SoDeMA konseptini önermek üzere çoklu erişim tasarımı için yazılım tanımlı radyo (SDR) fikrini ödünç alıyoruz. SoDeMA, 5G'deki farklı hizmetleri ve uygulamaları desteklemek için çok sayıda erişim düzeninin çok esnek bir konfigürasyonunu sunar. Örneğin, hücre merkezi kullanıcıları veya ultra yüksek tanımlı video gibi gerçek zamanlı hizmetler için, dikgenlik ve senkronizasyondan faydalanan yüksek veri hızı iletimini desteklemek için geleneksel OMA şemaları kullanılabilir. Öte yandan, bazı pratik senaryolarda (örneğin, yoğun nüfus alanları ve mobil sosyal uygulamalar) yüksek spektral verimlilik, büyük bağlantı ve sık sık küçük paketlere erişim gerektiğinde, NOMA planları seçilebilir.



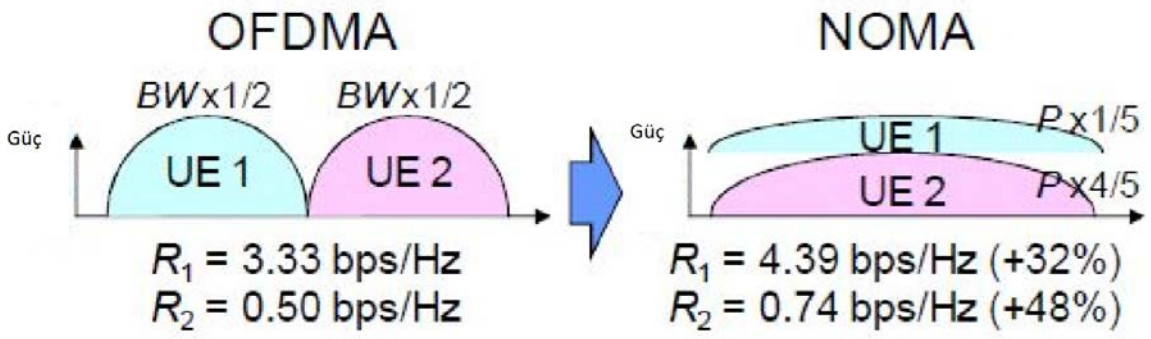
Şekil 2-16 SoDeMA Bağlantılı Araçlar Farklı Yoğunluklarda Gösterimi

Ayrıca, farklı NOMA veya OMA şemaları kendi uygun uygulama durumlarına sahiptir ve uyumluluk ve uygulama karmaşıklığı arasındaki dengeyi sağlamak için uyarlamalı olarak yapılandırılabilir. Örneğin, yakın kanal etkisi veya hareketli ağlarda, kullanıcıların kanal koşulları arasında büyük bir fark varsa, SIC alıcılı güç etki alanlı NOMA nispeten düşük karmaşıklıkta kullanılabilir. Öte yandan, özellikle kanal koşulu kötü olduğunda veya kullanıcıların konum dağılımı yoğunlaştığında, yüksek güvenilirlik garanti edilirse, SCMA, şekillendirme kazancı ve yaklaşık optimum MPA (mesaj iletme algoritmaları) nedeniyle uygun bir çözümdür. Çünkü, kullanıcı sayısı yeterince büyük olduğunda, her kullanıcı için bir kod çizelgesi tasarlamak zor olabilir ve bu durumda, LDS-OFDM veya MUSA, verici veya alıcıdaki tasarım karmaşıklığını azaltmak için de kullanılabilir. Bazı sinyal işleme modülleri, bazı NOMA şemaları için ortaktır, bu genel amaçlı modüller, farklı şemaları uygulamak için yazılım seviyesinde farklı formlarda birleştirilebilir. NOMA şemaları arasında geçiş, yazılım tanımlı donanım mimarisi ile hızlı ve esnektir. Ayrıca tam kapasiteye ulaşmadan farklı iletişim senaryolarına hızlı bir şekilde uyum sağlayabilir. SoDeMA'yı etkinleştirmek için, çerçeve yapısı yeterince esnek olmalı, böylece zaman ve frekans kaynakları farklı servisler ve kullanıcılar için serbestçe farklı bloklara ayrılmalıdır. Her kaynak bloğunda, belirli bir çoklu erişim şeması, belirli dalga formu, çift yönlü modülasyon, pilot sinyalleri, güç seviyesi vb. ile yapılandırılmıştır. Önerilen SoDeMA konsepti, farklı hizmetleri ve uygulamaları desteklemek için çoklu erişim şemalarının esnek bir konfigürasyonunu sağlar. SoDeMA'nın, gelecekteki 5G ağlarında “hizmet olarak herhangi bir bileşenin sistem tasarım hedefini desteklemek üzere çeşitli uygulama senaryolarına uyum sağlamak için dikkatlice tasarlanması gerekmektedir.

Tablo 1 Çoğullama Karşılaştırma Tablosu

	SDN	NOMA	OMA	SoDeMA
Esneklik	Fazla	Fazla	Düşük	Fazla
Sistem Yönetimi	Kolay	Normal	Kolay	Çok Zor
Programlanabilirlik	Fazla	Fazla	Düşük	Fazla
Uygulamalar	Fazla	Fazla	Düşük	Çok Fazla
Kaynak İhtiyacı	Orta	Fazla	Düşük	Fazla
Enerji Verimliliği	Fazla	Fazla	Düşük	Orta

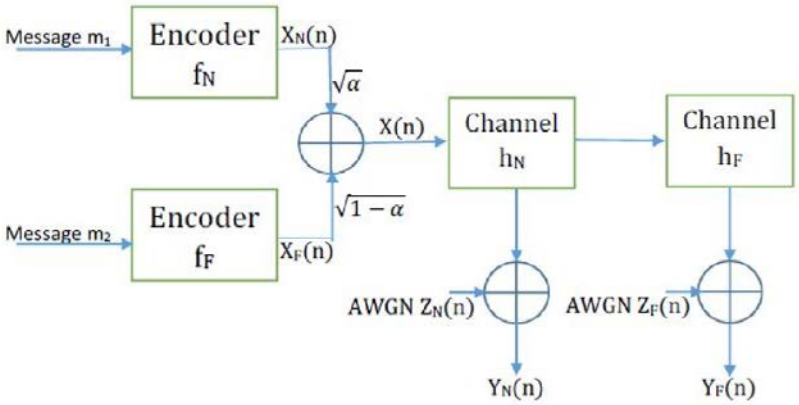
Şekil 2-2-17 ve Tablo 1 üzerinde görüleceği üzere diğer sistemlere nazaran SoDeMA Çok fazla uygulama alanına olanak sağlamaktadır. SoDeMA üçüncü bölümde incelediğimiz bağlantılı araç fonksiyonların çeşitliliğine cevap verebilecek nitelikte bir iletişim sistemidir. Çünkü fonksiyonlar farklı veri hızı ve kalitesi seviyelerinde değişkenlik göstermektedirler.



Şekil 2-17 Bant ve güç dağılımı karşılaştırması OFDMA ve NOMA [32]

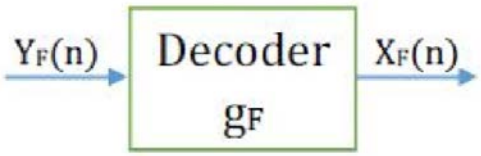
Şekilden de anlaşılacağı gibi, NOMA sisteminin toplam kapasitesi (veya toplam kapasitesi) her zaman OMA sistemlerinin toplam kapasitesini aşıyor. Kullanıcı verim adaletinde, OMA sınırına göre bir gelişme var. NOMA ve OFDMA şemalarının spektrumu, Şekil 2-17'de gösterilmiştir. İki şema için çeşitli güç tahsisleri altında ulaşılabilir oranları göstermektedir.

Şekil 2-18, Şekil 2-19 ve Şekil 2-20 bize NOMA SC ve NOMA SIC kanallarının yapısını göstermektedir. Bu şekilde oluşturacağımız kanalların test edilmesi ile elde edeceğimiz grafikler ise Şekil 2-21 ve Şekil 2.22 üzerinde görüldüğü gibidir.



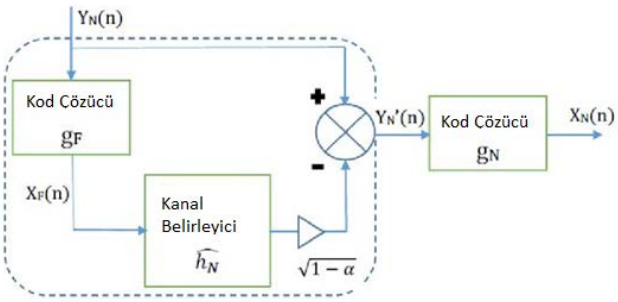
Şekil 2-18 Verici Tarafı NOMA

Burada Şekil 2-18 üzerinde 2 sinyalin daha önceki bölümlerde işlendiği gibi güç oranı etki alanı ile birleştiği sistemi (SC iletici) görmekteyiz. Bu sinyalin oluşturulduğu kısımdır

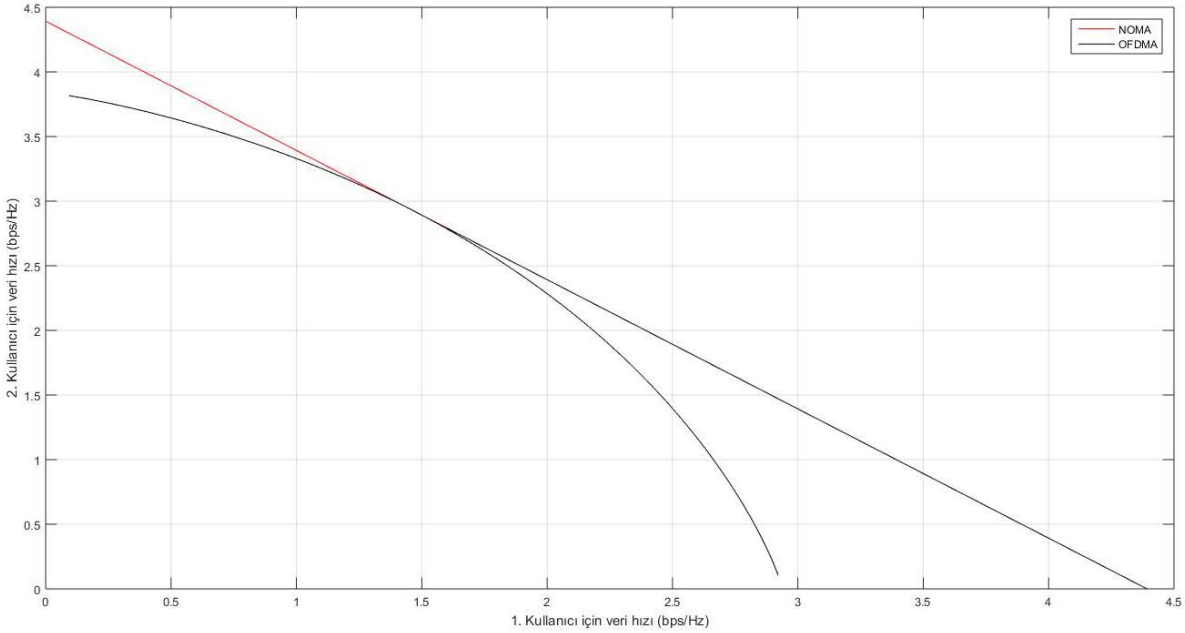


.

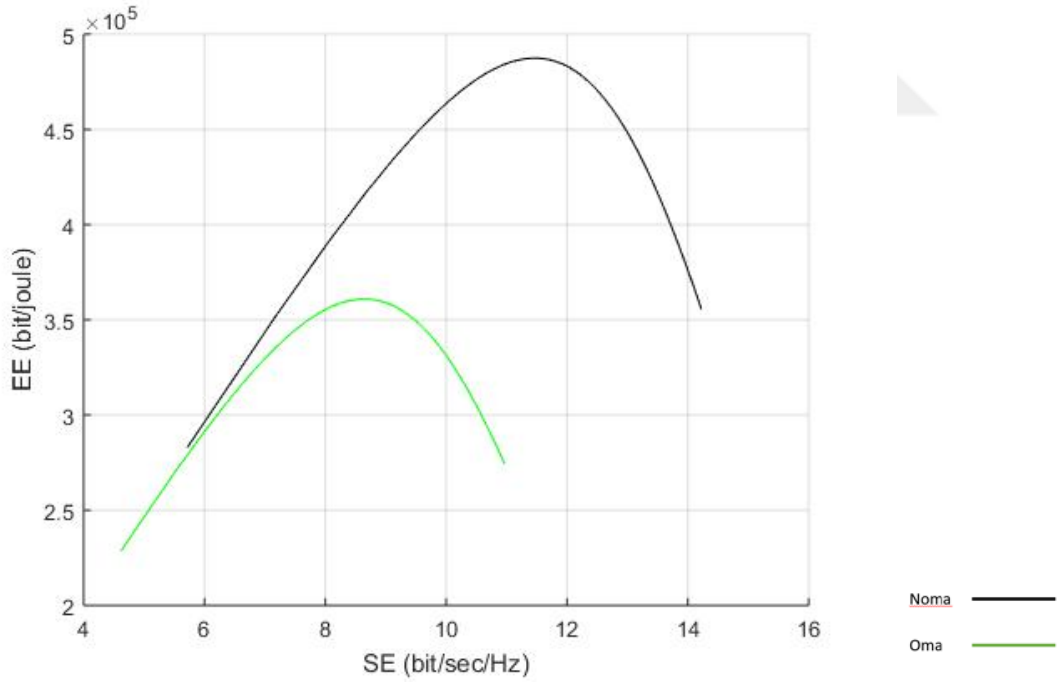
Şekil 2-19 Kullanıcı cihazına dışarıdan bakış [18]



Şekil 2-20 SIC Alıcı Tarafı [18]



Şekil 2-21 NOMA SIC ve OMA üzerinde 2 kullanıcılı sistemde veri hızı karşılaştırması [18]



Şekil 2-22 NOMA SIC ve OMA Güç ve Verileri Karşılaştırması [18]

Tüm bu karmaşık modülasyon teknikleri içerisinde anlık ya da bölgesel konuma uygun olarak kullanılması gereken kullanıcı kimlik profili ne kadar hızlı belirlenirse, sistemin çalışma verimi de o kadar artacaktır. Tüm bu modülasyon işlemlerinde belirlenen ayrışma profil tanımlama

sırasında SM-DP tarafından sunulmaktadır. Ancak farklı içeriklerdeki SM-DP seçeneklerinin eUICCler için kullanılabilmesi için çok aktif SM-SR sunucuların kullanılması gerekecektir.

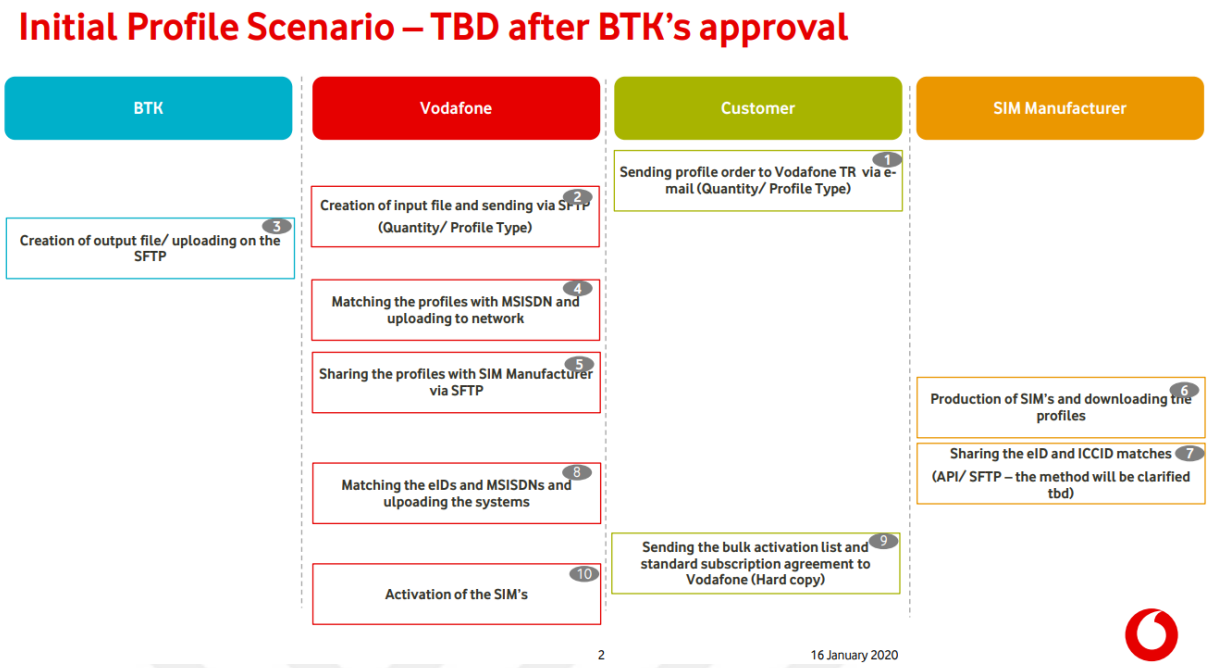
3. MALZEME VE YÖNTEM

Bu çalışmamda hücresel haberleşme içerisinde yerini yeni olarak almış olan elektronik gömülü üniversal tümleşik kullanıcı kimlik kartlarının (eUICC) yönetiminde kullanıcı profillerinin sahip olduğu operatör kriterlerinin yönetildiği sunucular arasında profil nakil işlemlerinin doğru şekilde nasıl yapılması gerektiğini tanımlayacağız. Bu tanımlamada özel bir kriter ele alınacaktır.

Endüstriyel olarak çok kapsamlı bir üretim sürecini içerdiğinden dolayı, yeni nesil SIM kartların otomotiv üretim sektörü yöntemin etkilediği alan olarak örnek olarak seçilmiştir. Bu yüzden otomotivin neden GSM bağlantısına ihtiyaç duymaktadır ve bu teknolojinin içerisindeki uygulama boşluğundan nasıl etkilendiğini göstermek için uygun bir örnek olacaktır. Aynı zamanda çalışmada söz konusu regülasyonların düzenleyici olan akredite kuruluş olan GSMA hakkında bilgilere yer verilecektir. eSIM ve eUICC hakkında bilgiler verilecek olup, kullanıcı rofilleri hakkında kapsamlı bir içerik sunulacaktır. [33]

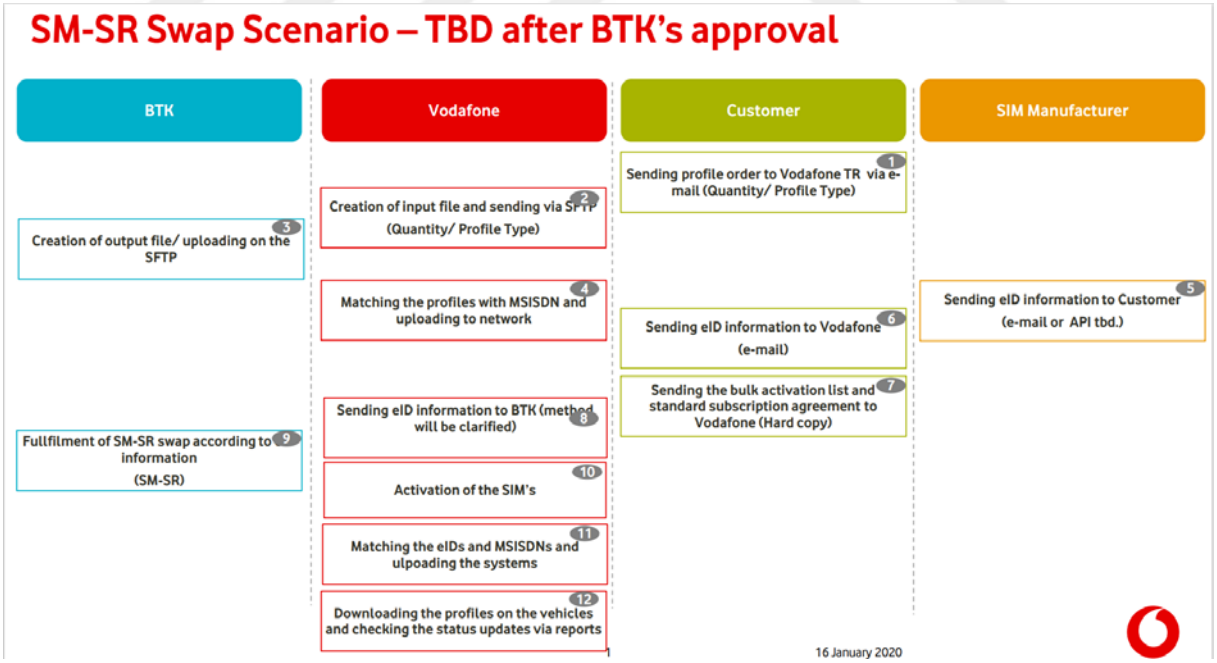
Yukarıda sayılan açıklamalardan sonra tezimin amacı olan SIM kart üreticisi olmayan SM-SR sunucularına SIM kart üreticisi bir SM-SR sunucusundan takas işleminin nasıl gerçekleştirileceğini açıklayacağım. Tezi oluştururken deneysel bir yöntem kullanılacak. 40 adet yeniden programlanabilir gömülü tümleşik kullanıcı kimlik kartı kullanılacaktır. Bu kartlar SM-SR sunucusu yurt dışında bulunan bir SIM kart üreticisi tarafından üretilecek, profil bilgileri yerli bir MNO tarafından tedarik edilip Türkiye Hücresel Haberleşme ağına ait profil bilgileri ile yerli ancak SIM kart üreticisi olmayan SM-SR sunucusuna taşınacaktır. Bu profillerin Türkiye'deki sunucu da uyandırılarak başlatılabilmesinin iki yolu olacaktır [6].

Birincisi bu eUICC'ler içerisinde bulunan ayağa kalkma profilleri yerli MNO'ya ait olarak üretilecek ve başlatılacak. Bu durumda herhangi bir transfer operasyonu gerçekleştirmeye gerek kalmayacaktır.



Şekil 3-1 Başlangıçta Yerli MNO ve SM-SR Profili İle Başlayan Senaryo

İkinci olarak yabancı operatör ve yabancı EUM SM-SR sunucusu üzerinde ayağa kaldırılan profillerinin taşınması işlemi.



Şekil 3-2 SM-SR Taşıma İşlemi

Tezinde konusu olan SM-SR transfer senaryosunu tüm adımları ile ilgili deney araç gereçleri ile gözlemleyeceğiz.

Deneylerimizde

1-QXDM: QXDM logları KVKK kapsamında gizli bilgiler içerdiğinden dolayı herhangi bir görüntü ya da bulgu paylaşılamayacaktır. Bu araç cihazın gömülü olduğu entegre kartına SSH bağlantısı yapılarak Linux Terminal Penceresinden “bash script” kullanılarak erişilmiştir.

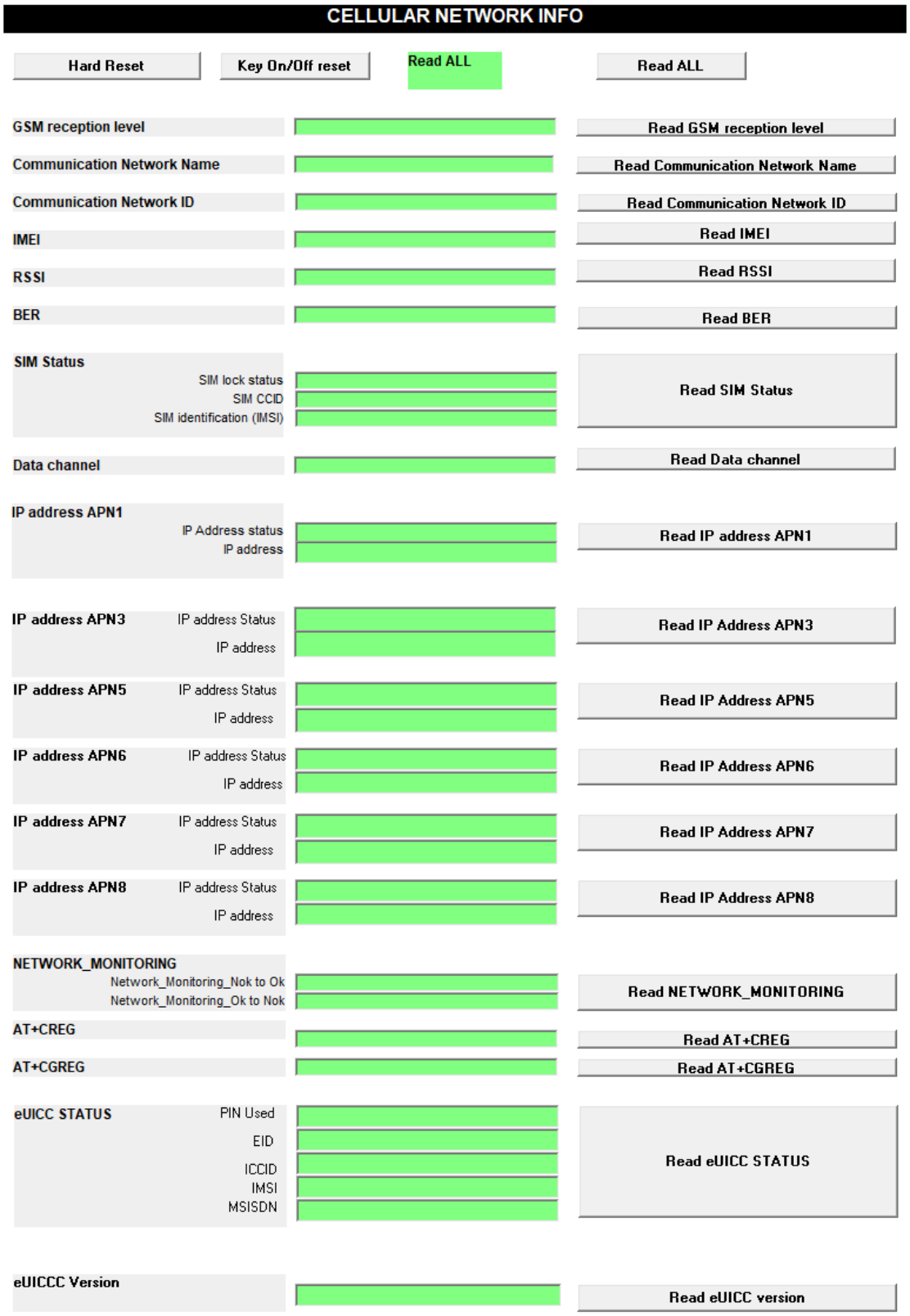
2-DDT2000 araçları kullanılacaktır. Şekil 3-3’te ilgili aracın ara yüzü görülebilir.

Yapılacak olan işlem Şekil 3-2’de görüldü üzere 12 adımdan oluşmaktadır. Bu adımlar müşteri siparişinden başlayıp transfer işleminin tamamlanmasına kadar geçen test deney senaryosunu bize anlatmaktadır. GSMA tarafından yayınlanan SGP.01-v4.0.pdf [33] Uzaktan eUICC SM-SR transfer yönergesinde belirtilen adımlardan ziyade öncelikle Şekil 3-2’de testlerimizde kullandığımız MNO olan Vodafone tarafından eUICC’ler için kullanılacak olan profiller tanımlanmalıdır. Bu yüzden standartta belirtilen yöntemden başka bir senaryonun uygulanması gerekmektedir ve standart dokümanına eklenmelidir. Adımları teker teker açıklamak gerekecek olursa;

1. Müşteri tarafından eUICC siparişlerinin MNO tarafına iletilmesi gerekmektedir. Böylece bir SIM kart üretim aşaması başlatılacaktır.
2. Yerel MNO tarafından profiller üretilecektir ve SFTP ile profillerin kaydolacağı SIM kart üreticisi olmayan SM-SR sunucu hizmeti veren kurumun Türkiye’deki karşılığı olan Bilgi Teknolojileri Kurumu’na iletilecektir.
3. SIM kart üreticisi olmayan SM-SR sunucusu tarafından gerekli profil çıktıları oluşturulacak ve SFTP ile yerli MNO’ya gönderilecek
4. MSISDN bilgileri profiller ile eşleştirilecek ve hücresel ağa yüklenecek.
5. Eski SM-SR sunucusu EID bilgilerini Müşteriye gönderilir.
6. Müşteri EID bilgilerini yerli operatöre gönderir.
7. Müşteri aktivasyon talebini MNO’ya gönderir.
8. EID bilgileri yeni yerli SM-SR sunucusu işletmecisine gönderilir.
9. SM-SR üzerinde ilgili profil bilgileri tamamlanmış olur ve cihaz yerli hücresel ağ üzerinde çalışmak için hazır hale gelir.
10. MNO talebi gelen eUICC’leri aktive eder.

11. Sağlama Adımı
12. MCKS ile ilgili adım

Sağlama ve MCKS adımları haricindeki sürecin metodu tanımladığı testler 25.03.2021 tarihinde ön hazırlıkları ile birlikte Vodafone, BTK, Groupe Renault, Protahub ve Thales firmalarının desteği ile 11:00 itibari ile başlayacak ve 17:00 dolaylarında tamamlanacaktır.



Şekil 3-3 DDT2000 Hücresel Ağ Ara Yüzü Boş

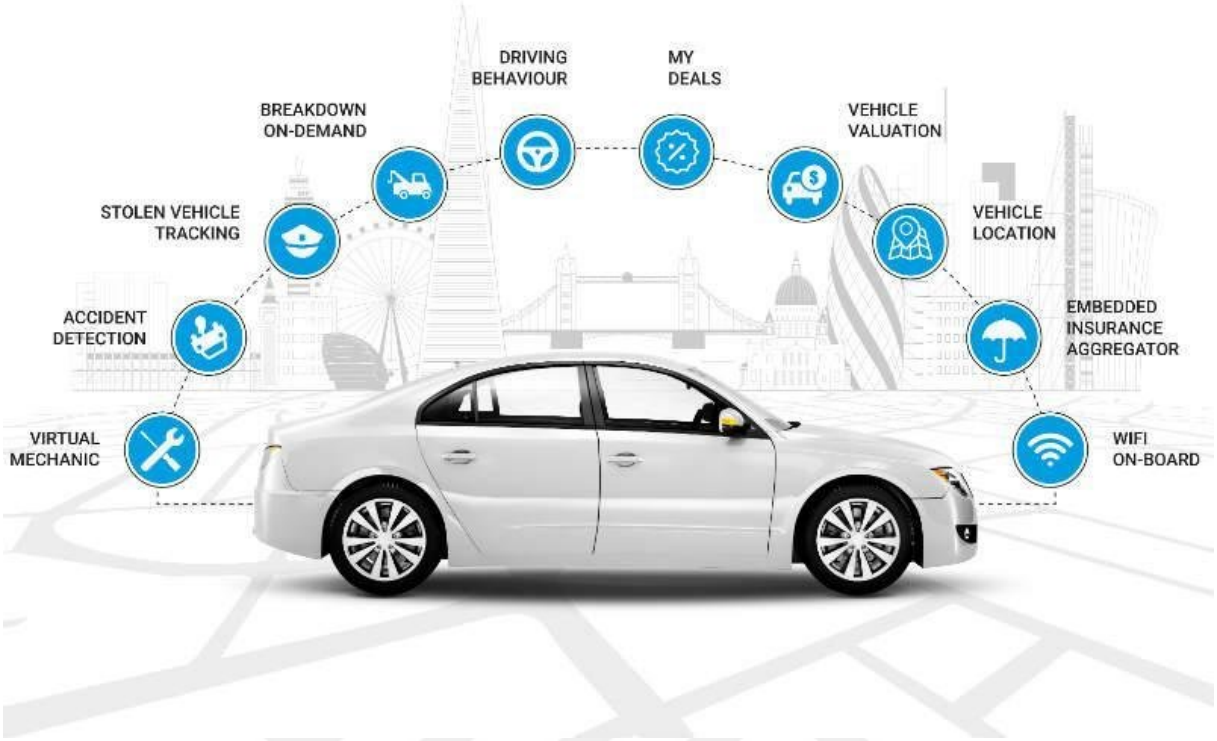
3.1. IOT, M2M VE BAĞLANTILI ARAÇLAR

GSM teknolojisinin hayatımıza veri iletimini daha hızlı bir şekilde sunmasıyla birlikte artık interneti sadece insanlar arasındaki bilgi paylaşımında değil, makinelerin de birbirleri arasında ihtiyaç duydukları iletişimi sağlamaları için kullanmaya başladık. Endüstride, evlerimizde, araçlarımızda, çiftliklerimizde, sayaçlarımızda, kişi ve hayvan takip cihazlarımızda, kısacası makinelerin birbirleriyle haberleşmesinin, aradan insan kontrolünün yazılım kontrolüne devredildiği tüm alanlarda M2M yani makineler arası haberleşme teknolojik ihtiyaçların belirlenmesinde önemli hale gelmiştir. Yapılan bu işlemlerin tamamının son kullanıcıların ve geliştiricilerin okuma, bilgilenme, yazma, değiştirme, açma, kapatma, güncelleme, tanımlama, susturma, bekletme vb. işlemleri, bu işlemlerin geçmiş bilgileriyle birlikte çoklu yetkili ve yetki seviyeleri farklı kullanıcılara internet üzerinden erişiminin sağlandığı ortama da Nesnelerin interneti, İngilizce kısaltması olarak IoT adlandırılması yapılmıştır. Tüm bu veriler bulut katmanı üzerinde saklanmakta, biriken bilgiler ihtiyaçlara göre filtrelenip bulut katmanı denilen sunucularda hizmete sunulmaktadır.

3.2. BAĞLANTILI ARAÇLAR

Bağlantılı araçlar yani dünya genelindeki adıyla “Connected Cars” araç üreticilerinin kullanıcılarına yeni yayınlanan regülasyonlar ile sağlamak zorunda oldukları ve kalite ve hizmeti arttırmak adına fazladan ekledikleri internet bağlantılı özelliklerin araçlara uygulandığı sistemlerin genel adıdır. Aşağıda tanıttığımız özellikler ikinci bölümde üzerinden geçtiğimiz bek çok iletişim sisteminin farklı kombinasyonlarla kullanılmasını gerektiren farklı veri iletim hızlarını ve sürelerini servis kalitelerini güvenlik seviyelerini gerektiren bir çalışma alanıdır. Bu yüzden bu alanda bantların çok daha etkin kullanılması gerekecektir. Yakın gelecekte hayatımızda çok daha fazla yer edecek “Autonomous Drive” (kendi kendini süren araçlar), elektrikli araçlar ile, yolculuklarımızda kullandığımız araçlarımızın veri ihtiyacı gün geçtikçe daha da fazla artacaktır. Bunları daha verimli bir şekilde planlamak adına 5G teknolojisinin altyapısında kullanılacak modülasyonun kullanım şeklinin tasarlanmasın tasarlanması gerekmektedir. Bunu anlamak için öncelikle yakın gelecekte sunulacak olan bağlantılı araç fonksiyonlarını inceleyeceğiz. Çünkü araçların içerinde ihtiyaç duyulacak bağlantı türü çok değişkenlik göstermektedir ve akıllı bir sisteme ihtiyaç duymaktadır. Trafiğin yoğunluğu, trafiğin içerisindeki kullanıcı profili kullanıcıların internet kullanım saatleri gibi değişkenlere

bağlı olarak verinin, veri trafiğinin, verinin üzerinden akacağı sistemin kullanacağı modülasyonun akıllı bir şekilde ayarlanması gerekmektedir. Bu yüzden bağlantılı araçların geçeceği konumlarda bağlantı modülasyonunun neden akıllı bir sisteme ihtiyaç duyacağını anlamak için bağlantılı araçların bize sunacağı bazı sitemleri inceleyelim.



Şekil 3-4 Bağlantılı Araç [34]

3.2.1. Uzaktan Kilitleme/Açma



Şekil 3-5 Uzaktan Kilitleme

Uzaktan kilitleme açma özelliği aracın yanında olmadan uzaktan kilitleyip açabilmemize olanak verecek bir özellik olarak bağlantılı araçlarda yer alacak bir özelliktir. Bu özellik sayesinde internete bağlantısı olan cihazımızdan aracımızın yanında olmasak da çok uzaklardan aracın kapılarını kilitleyip açabilmemizi sağlayacak bir özelliktir. Bunu yapabilmemiz için gerekli olacak bilgi kesin olarak çok yüksek güvenlikle ve doğru bir şekilde taşınmalıdır. Daha

önceden belirttiğimiz gibi QoS seviyesi 2 olarak belirlenmedir ve üçüncü kişilerin ataklarından korunmalıdır.

3.2.2. Uzaktan Çalıştırma



Şekil 3-6 Uzaktan Çalıştırma

Aracın uzaktan çalıştırılmasını sağlayacak bu servis aracın "key fob" olarak adlandırılan anahtar kodunun, CAN haberleşme ağı üzerinde aktif bir şekilde okutulmasını gerekmektedir ve yüksek güvenlikle iletilmelidir. Veri boyutları çok küçüktür ancak yüksek güvenlik ile taşınması gereken bir bilgi içermektedir. Kullanıcıların aracın çok uzağında olsalar bile araçlarını çalıştırabilmelerine olanak sağlar.

3.2.3. Uzaktan Araç Durumu Sorgulama



Şekil 3-7 Uzaktan Diagnostik Sorgulama [35]

Bu özellik filolarda, araç kiralama firmalarında ve markaların servis bilgilerinde çok önemli bir yere sahip olacaktır. Bu bilgiler aracın “Diagnostic” olarak adlandırılan kayıtlarının tutulduğu, hata kodlarının saklandığı elektronik hafıza alanlarıdır. Burada aracın yakıt durumundan kilometre bilgisine kadar pek çok bilgi elde edilebilir. Orta büyüklükte veriler içeren bu paketler orta seviyede güvenlik ile taşınılabilir. Bu bilgiler sayesinde araç sürücüsüne ya da filo sahibine değerli araç bilgileri sağlanabilecektir.

3.2.4. Uzaktan Güncelleme



Şekil 3-8 Uzaktan Güncelleme FOTA[36]

Araçların içerisinde kullanılmakta olan mekanik sitemler artık yerlerini elektronik ile kontrol edilen sistemlere bırakmaktadırlar. Bu elektronik sistemler gün geçtikçe daha modern ve geliştirilebilir sistemlere evirilmişlerdir. Hatta bazı sistemler mekanik sistemlerden tamamen bağımsız olarak çalışan, doğrudan elektronik sistemlerdir. Bu durumda pek çok elektronik cihaz gibi bu modüllerinde zamanla güncellemeye ihtiyaç duymaları gayret doğal bir durum olarak karşımıza çıkmaktadır. Bu bilgiler hem yüksek güvenlik önlemi istemektedir hem de çok büyük boyutlarda olabilmektedir. Araçlar gibi hızlı hareket eden mobil alanlarda yüksek bağlantı hızlarını sağlamak, baz istasyonlarının arasında seyreden araç içerisindeki modemin bağlantısının devamlılığını sağlamak gerekmektedir. İngilizce olarak “handover” adı verilen baz istasyonları arasındaki taşıyıcı değişikliğinin doğru ve kararlı bir şekilde yapılması gerekmektedir. Hatta paketlerin bağlantı kaybedildiği durumlarda, bağlantı tekrardan sağlandığında indirme ya da yükleme işlemine kaldığı yerden devam edebilmesi gerekmektedir.

3.2.5. Eğlence Sitemleri



Şekil 3-9 Renault Multimedya

Eğlence sistemleri yeni nesil araçlarda internet ve mobil telefon etkileşimleri ile çok ilintilidir. Burada ağırlıklı olarak video ve çeşitli tiplerde ses verilerinin paketlerinin akış yolu ile iletilmesini gerektiren bir altyapı ihtiyacı doğmaktadır. Bu tip iletimde verinin güvenliğinden çok hızı önemlidir. Sistem verinin tam olarak iletildiğinden emin olmak zorunda değildir. Ağırlıklı olarak UDP kullanılan bu verilerin iletimi sırasında yine baz istasyonu değişikliklerinin yapıldığı esnada hızların belirli bir seviyede tutulası ve kanalda kullanılan bant veri oranlarının yüksek olması istenmektedir.

3.2.6. Bölgesel Çit

Bu özellik özellikle filo yönetim sistemlerinde ve araç güvenliğine önem veren kullanıcıların tercih edeceği bir özelliktir. Bu özellikte aracın konum bilgisi coğrafi harita üzerinde işaretlenmektedir. Bu bililer GPS dediğimiz küresel pozisyonlama sistemi yardımıyla elde edilen konum verilerinin daha önceden sistem kontrolörü tarafından işaretlenen sınırların içerisinde mi yoksa dışarısında mı olduğunun kontrolünün yapılması ile elde edilir. Bu tip verilerin sıklığı kullanıcı ya da kontrolör tarafından belirlenir. Küçük pakette veriler olsa da güvenlik açısından önem taşımaktadır. Bu yüzden güvenlikli sistemler ile taşınması gereken

veri guruplarındandır. Ayrıca bu sistemler kullanıcı ya da kontrolörlere araçları belirtilen alanların dışarısına çıkarıldığında yarılar gönderebilmektedir.

3.2.7. Araç Konum Bilgileri

İstenildiği taktirde GPS verilerinden aracın konumunun saptanabilmesini sağlayan sistemdir. Ayrıca yön bulma; İngilizce adıyla "navigation" sistemleri içerisinde de bu GPS verileri kullanılmakta, akış verileri birleştirilerek trafik yoğunlukları otopark bilgileri olarak da kullanılabilmektedir. Bu bilgiler küçük boyutlu olsa da karmaşık bir veri trafiğinin yaşandığı bir sistemdir.

3.2.8. Sürücü Performans Bilgileri

Sürücünün aracı nasıl kullandığı ile ipuçları veren bilgilerin toplanmasını sağlayan özelliklerdir. Ticari anlamdan pek çok avantaj sağlamaktadır. Örneğin kasko ya da sigorta şirketlerinin verecekleri teklifler bu veriler kullanılarak verilebilmektedir. Ayrıca araç üreticileri araçları sağlık durumuyla ilgi verileri bu bilgiler ışığında daha ayrıntılı olarak bulabileceklerdir. Örneğin çok fazla dur kalk yapan bir sürücü profili bu dur-kalklar esnasında aracın debriyaj sistemini çok zorlamaktadır. Hem aracına arar vermektedir hem de kaza riski daha fazladır. Bu gibi veriler toparlandığında ticari değeri yüksek bir veri havuzu oluşturulacaktır. Toplu halde çekilmesi planlanan bu veriler yüksek boyutlarda da olabileceği gibi düşük boyutlarda filtrelenmiş verilerde olabilir.

3.2.9. Acil Durum Çağrıları

Avrupa ve Türkiye'de 2019 itibari ile mecburi olarak devreye girecek olan bu sistem araç herhangi bir acil durum içerinde bulunduğunda kendiliğinden acil durum merkezini aramakta, acil durum merkezine araçla ilgili verilerin aktarılabilmesini sağlamaktadır.

Özetle belirtecek olursak bu ve bunun gibi karmaşık ve çeşitli bilginin alınıp verileceği karmaşık bir ekosistemde çeşitli ölçeklerde hız ve bant ihtiyacı doğacaktır [39]. Elimizdeki altyapının çok daha verimli bir şekilde kullanılması için bu sistemlerin daha akıllı bir şekilde kontrol edilmesi gerekmektedir.

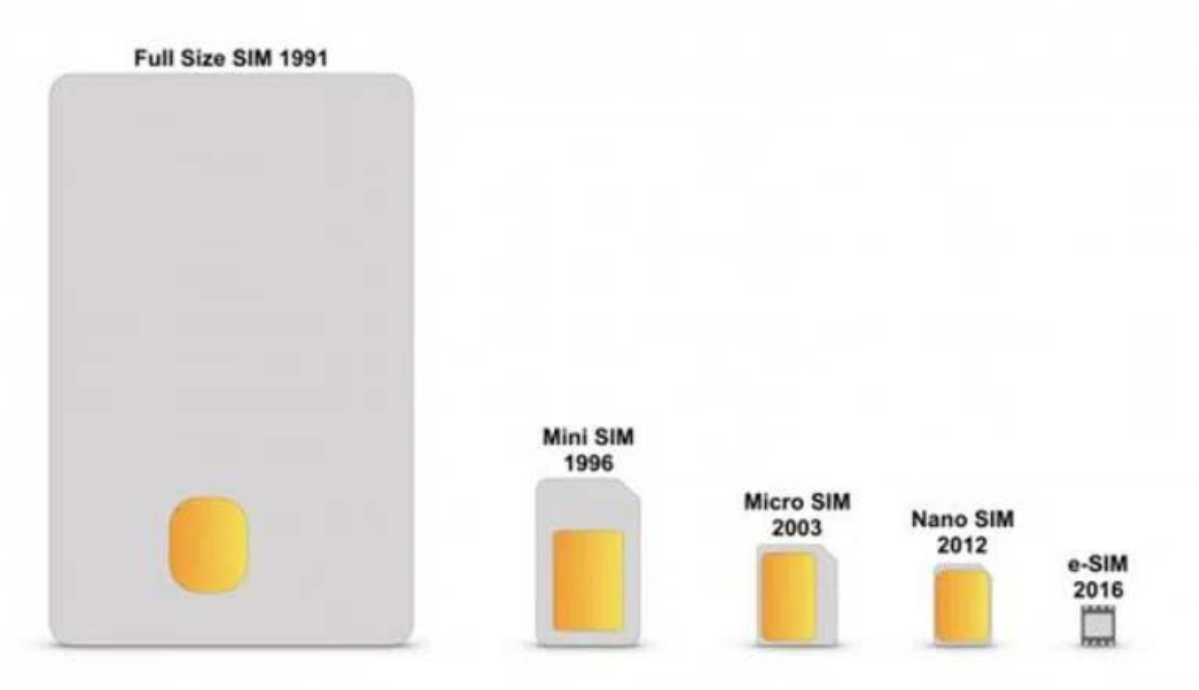
Ancak konunun bir diğer hassas noktasında siber güvenlik gereksinimleridir. 112 Acil Çağrı Servisi Tabanlı Araç İçi Acil Çağrı Sisteminin Yerleştirilmesi İle İlgili Tip Onayı Yönetmeliği [39] kanunlaştıktan sonra 2018 yılından sonra tip onay belgesi almış olan tüm araçlarda 112

acil durum sistemi bulunmak zorundadır. Yönetmelikte açıklandığı üzere bu sistem hücresel iletişim teknolojisi üzerinden haberleşecektir. Ancak hem üretim hatlarının durumu, gerekse de endüstrileştirme açısından eski tip plastik SIM kartların bu cihazların içerisinde kullanılması otomotiv elektroniği standartlarına göre de mümkün değildir. Bu yüzden bu tip sistemlerin içerisinde yine BTK tarafından yayınlanan BTK eSIM Kararnamesinde [38] yeni geliştirilen elektronik gömülü bütünleşmiş SIM kartların nasıl kullanılacağı tanımlanmıştır. Bu süreçten sonra SIM kart üreticisi olmayan Türkiye gibi ülkelerde bu sistemleri uygulamaya almak için bir yöntem gerekli oldu. Türkiye'de üretilen ya da yurtdışında üretilerek Türkiye'ye ithal edilen tüm araçlarda kullanılan acil durum arama sistemlerinin tamamı yabancı MNO SIM kartları taşımaktaydı. Ayrıca bu SIM kartların bağlı oldukları SM-SR sunucuları SIM kart üreticilerine ait ve yurt dışında konumlandırılmış sunuculardı. Bu durum ilgili kanunlara [38] aykırı olduğundan dolayı profil bilgilerinin ve yönetimlerinin Türkiye'ye aktarılması gerekti.

3.3. GSMA

GSMA dünya genelinde GSM uygulamalarının düzenlenmesi güncellenmesi, değişen ihtiyaçlar doğrultusunda yeni standartların belirlenmesinde rol oynamaktadır. [1] GSM Birliği (genel olarak 'GSMA' veya Mobil İletişim için Global Sistem, orijinal olarak Groupe Special Mobile olarak anılır), dünya çapında mobil ağ operatörlerinin çıkarlarını temsil eden bir endüstri kuruluşudur. 750'den fazla mobil operatör tam GSMA üyesidir ve daha geniş mobil ekosistemdeki 400 şirket daha ortak üyedir. GSMA, üyelerini endüstri programları, çalışma grupları ve endüstri savunuculuk girişimleri aracılığıyla temsil eder.

3.3.1. SIM Kartlar



Şekil 3-1 SIM Kartlar

SIM kartlar; abone kimlik modülü, bir entegre devre kartının işletim sistemi tarafından çalıştırılan, ilgili kullanıcı ve profil bilgilerini güvenli bir şekilde depolayan, uluslararası mobil abone kimliği(IMSI) numarası ve ilgili anahtarı, kullanıcı ve abone profil bilgilerini tanımlayan, mobil telefon cihazlarındaki aboneleri belirlemek ve kimliklerini doğrulamak için kullanılır. SIM devresi, genellikle gömülü kontakları ve yarı iletkenleri olan PVC'den yapılmış evrensel bir bütünleşmiş devre kartıdır (UICC). SIM kartlar farklı mobil cihazlar arasında aktarılabilir. İlk UICC akıllı kartları, kredi ve banka kartları büyüklüğündeydi; boyutları yıllar içinde birkaç kez küçültüldü, genellikle elektrik kontakları aynı tutuldu, böylece daha büyük bir kart daha küçük bir boyuta kesilebildi.

Bir SIM kart, benzersiz bir seri numarası (ICCID), uluslararası mobil abone kimlik (IMSI) numarası, güvenlik doğrulama ve şifreleme bilgileri, yerel ağla ilgili geçici bilgiler, kullanıcının erişebildiği hizmetlerin bir listesi ve iki şifre içerir. Normal kullanım için bir kişisel kimlik numarası (PIN) ve PIN kilidini açmak için bir kişisel blokaj açma anahtarı (PUK). Avrupa'da, seri SIM numarasına (SSN) bazen uluslararası bir makale numarası (IAN) veya bir ön ödemeli kart aboneliği için çevrimiçi kaydolurken gerekli olan bir Avrupa makale numarası (EAN)eşlik eder.

Tablo 2- SIM Kartlar

Tam boyutlu (1FF)	1991	ISO/IEC 7810 :2003, ID-1	85,6 mm (3,37 inç)	53,98 mm (2,125 inç)	0,76 mm (0,030 inç)
Mini SIM (2FF)	1996	ISO/IEC 7810:2003, ID-000	25 mm (0,98 inç)	15 mm (0,59 inç)	0,76 mm (0,030 inç)
Mikro SIM (3FF)	2003	ETSI TS 102 221 V9.0.0, Mini-UICC	15 mm (0,59 inç)	12 mm (0,47 inç)	0,76 mm (0,030 inç)
Nano SIM (4FF)	2012 başı	ETSI TS 102 221 V11.0.0	12,3 mm (0,48 inç)	8,8 mm (0,35 inç)	0,67 mm (0,026 inç)
Gömülü SIM (eSIM)	2016	ETSI TS 102.671 V9.0.0 JEDEC Design Guide 4.8, SON-8 GSMA SGP.22 V1.0	—	—	—

SIM, başlangıçta ETSI tarafından TS 11.11 sayılı şartnamede tanımlandı. Bu tanımlama, Sim'in fiziksel ve mantıksal davranışını açıklamaktaydı. SIM kart teknolojisinin gelişmesi ile birlikte UMTS, şartname çalışmaları evrimsel bir sürece girdi ve 3GPP altında çok sıkı regülasyonlara tabi tutuldu. Bu sıkı regülasyonlar sayesinde GSM tüm dünya üzerinde standartlaşabilmiş en kapsamlı ve global teknoloji uygulaması haline geldi.

İlk SIM kart 1991 yılında, akıllı kart üreticisi Giesecke & Devrient tarafından geliştirildi. Bugün, SIM kartlar her yerde bulunur ve 40 milyardan fazla cihazın dünya çapında hücresel ağlara bağlanmasına olanak sağlar. Uluslararası Kart Üreticileri Birliği'ne (ICMA) göre, 2016 yılında küresel olarak üretilen 5,4 milyar SIM kart vardı. Bugün ise hücresel IOT ve 5G ağların yükselişi 2020 yılında 20 milyar hücresel cihaza SIM kart ihtiyacı doğurdu. Bununla birlikte mobil veri hızlarının kalitesinin ve bant genişliğinin yükselmesi ile birlikte adetler 50 milyarın üzerinde 2021 yılı bitmeden getirilmesi gömülü-SIM (Esim) ve uzak SIM sağlama (RSP) GSMA'dan [40]"dijital" SIM kart sağlama ve mobil ağ operatörleri için diğer katma değerli

hizmetlerin devreye alınması ile SIM kart abone sayılarının yakın gelecekte 1 trilyonun üzerine çıkması beklenmektedir.

3.3.2. eSIM

Doğrudan bir tümleşik devreye lehimle sabitlenmiş küçük bir çiptir. Bu form faktörünün resmi adı MFF2'dir. Makine-2-Makine (M2M) Form Faktörü. Normal SIM kartımızla aynı şekilde çalışır. Orada UICC ve IMSI gibi programlanmış çeşitli benzersiz tanımlayıcılar vardır. Bu, cihazınızı yakındaki hücresel kulelerle iletişim kurarken tanımlamak için kullanılır. Bu tip SIM kartlarda çok faktörlü kimlik doğrulama vardır, bu doğrulama yapılırsa cihazını kartınıza etkin bir şekilde lehimlediğiniz anlamına gelir. Bariz fark, eSIM'i karttan sökmeden karttan çıkarmanın bir yolu olmamasıdır. Bu, başka bir hücresel sağlayıcıya geçiş yapamayacağınız anlamına gelir. eSIM teknolojisi M2M için çok garantili bir yöntem olsa da dezavantajı tümleşik entegre devre üzerinde lehim sökme işlemi yapılmadan başka bir mobil operatöre yani MNO'ya geçişin mümkün olmamasıdır. Bu nedenle sadece M2M için değil diğer cihazlarda da abonelere ve kullanıcılara operatör ülke ve profil değişikliği sağlayabilecek olan programlanabilir entegre tümleşik kullanıcı kimlik kartları tasarlanmıştır.

3.3.3. eUICC

Bir IoT ya da M2M MFF2 SIM kartı, SIM kart başına bağlantı seçeneği sunan, dosya sistemi, operatör anahtarları ve Uluslararası Mobil Abone Kimliği (IMSI) gibi bir SIM kartın çalışması için gerekli tüm bilgileri tutan ve genellikle bir operatöre atanan ve dolayısıyla bir tane veren bir SIM profiline sahiptir.

eUICC'nin geleceği gerçekten büyük bir şekilde değiştirdiği yer tam olarak burasıdır. Etkin bir şekilde birden çok SIM profilinin bir 'kapsayıcısı'(İngilizce adı ile container) olarak hareket eder, böylece bir MFF2 kartı aynı anda birkaç farklı bağlantı seçeneğini ve operatörü barındırabilir ve aralarında seçim yapabilir. Bu seçenekler önemlidir, çünkü hiçbir operatör tam çalışma süresini, sabit fiyat garantisini, kapsama alanı taahhüdünü veya teknolojilerinin güncel kalacağını garanti edemez.

Bu özelliği ile, bir ağda bir kesinti olursa veya bir ağ bandı kapatılırsa, kullanıcıların SIM profillerini değiştirmelerine ve Sim'i çıkarmak zorunda kalmadan eUICC 'konteynerine' eklenen bir SIM profili ile bağlantıyı sürdürmelerine olanak tanır.

Havadan Kontrol Edilebilme (OTA)

OTA eUICC'nin bir başka önemli faktörüdür, MFF2 kartı bir cihaza gömülüyken, OTA erişim ile SIM profillerini uzaktan ekleme veya "sağlama" yeteneği, onu özellikle yaklaşan endüstriyel IoT devrimi ile alakalı hale getirir. Bu, OEM'lere ve IoT uygulama geliştiricilerine çok daha fazla özgürlük ve kontrol sağlar. Üretim noktasında bir MFF2 kartı yerleştirebilir ve ardından cihazı tümleşik devreden sökmeye gerek kalmadan gerekli OTA olarak profiller tedariği yapabilirler.

SIM profillerini değiştirme özgürlüğü, kaynak sertifika yetkilisinin GSMA veya her operatörün ve profilin meşru olmasını ve bağımsız veri akışlarına ve rollere sahip olmasını sağlayan başka bir düzenleyici kurum olduğu bir sertifika zincirine dayalı güvenli bir mimari tarafından denetlenir. Bu güvenli mimari, SIM profillerini sağlama ve kaldırma ve tüm bunları MFF2 kartına dokunmadan yapabilme özelliği nedeniyle, eUICC standardı bir kez uygulandığında, yeni operatörleri yönetmek için süresiz ve sınırsız bir şekilde değiştirilebileceği yaklaşık 20 yıllık bir ömre sahiptir.

Anlayacağımız üzere SIM kartlar artık sadece cep telefonlarında ve sabit profiller ile uzun süre tanımlanarak hizmet verecek çipler olmayacaklardır. Geçmiş 30 yıl boyunca teknolojinin bize sağladığı imkanlar doğrultusunda plastik SIM kartlar hizmetlerini neredeyse tamamlamışlardır. Programlanabilir SIM kartlar anlık profil değişimi ihtiyaçlarını

3.3.4. SM-DP

SM-DP, bir M2M RSP ortamında kullanılır. İşlevi, bir MNO'dan ham profil bilgilerini almak, uygun IMSI/Ki çifti bilgileriyle kişiselleştirmek ve SM-SR tarafından eUICC'ye iletilmeye uygun bir forma dönüştürmektir.

M2M ortamında profil indirme işlemi aşağıdaki gibidir:

1-Bir oturumu tetiklemek için ön hazırlık profilinin sağlayıcısına ait SMSC aracılığıyla SM-SR tarafından eUICC'ye gönderilen SMS

2-eUICC, cihazın BIP ve SM-SR'nin (SMS'de bulunan) URL'sini (veya IP adresini) kullanarak bir veri oturumu kurmasını ister.

3-eUICC ve SM-SR (ES5) arasında kurulan CAT_TP veya HTTPS aktarım bağlantısı

4-SM-DP ve eUICC arasında güvenli bir kanal kurulur

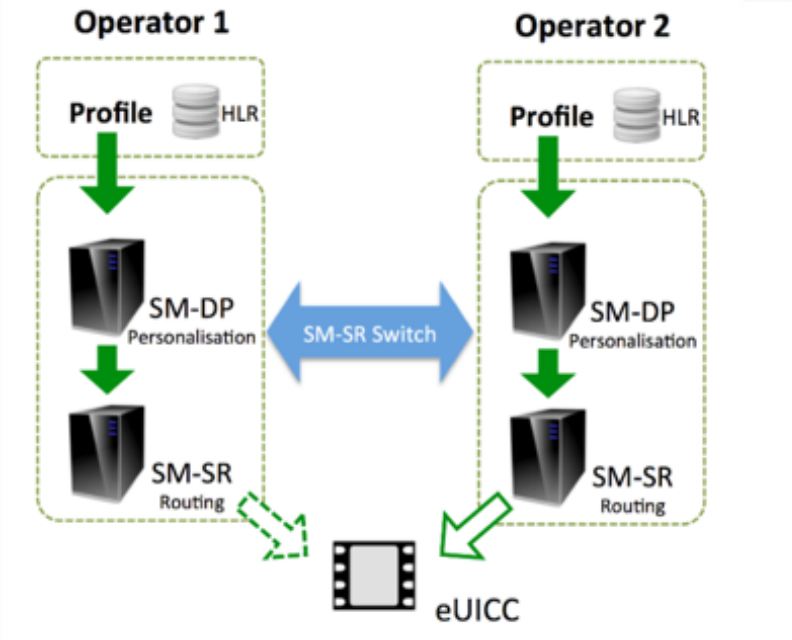
5-SM-DP tarafından bir profil indirme işlemi başlatılır

Uzaktan Uygulama Yönetimi (RAM) veya Uzaktan Dosya Yönetimi (RFM), SM ve eUICC arasında yukarıdaki gibi veri bağlantısı kullanılarak veya sadece SMS kullanılarak uygulanabilir.

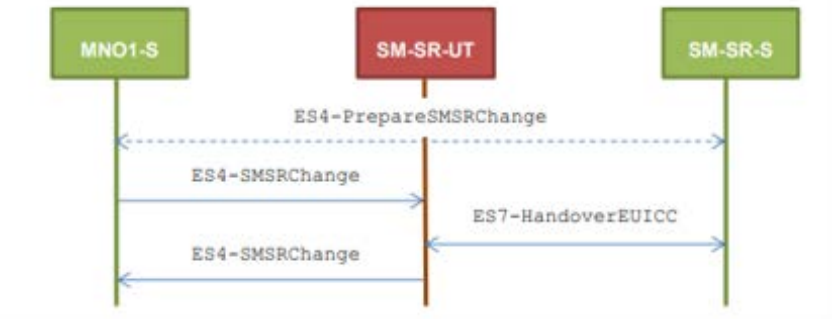
3.3.5. SM-SR

SM-SR, daha sonra eUICC'ye indirilmiş olan operatör profillerinin durumunu yönetmekten sorumludur (operatör profilleri, SM-SR işlevleri kullanılarak etkinleştirilebilir, devre dışı bırakılabilir, silinebilir). Ayrıca, operatör profillerinin teslimi için eUICC ve SM-DP arasındaki iletişim bağlantısını da güvence altına alır. SM-SR, kontrolü altındaki tüm eUICC'lerin bir veri tabanını ve bunları yönetmek için kullanılan anahtar setlerini tutar.

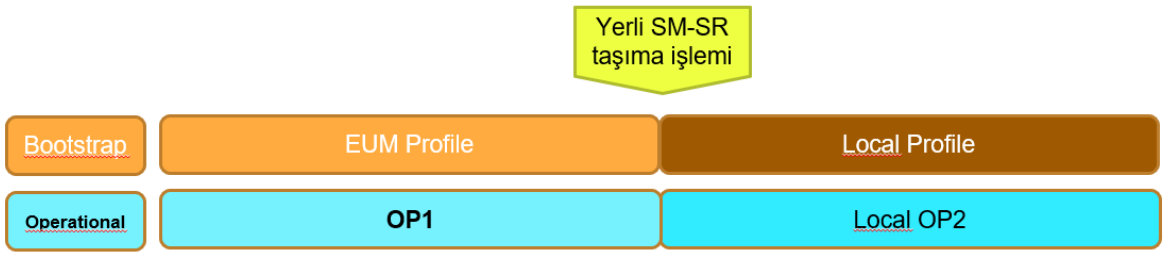
3.4. SIM KART ÜRETİCİSİ SM-SR SUNUCUSUNDAN SIM KART ÜRETİCİSİ OLMAYAN SM-SR SUNUCUSUNDA PROFİL TRANSFERİ



Şekil 3-2 SM-SR Transferi [33]



Şekil 3-3 Anahtar Seremonisi [33]



Şekil 3-4 Yerli Profil Aktarım işlemi

Şekil 3-2'de gösterilen transfer işleminde ilgili kanunlara uygunluğu sağlamak için herhangi bir yerli olmayan bootstrap profilinin dahi eUICC içerisinde bulunmaması gerekmektedir. Burada önerdiğimiz yöntem ile eUICC içerisinden bootstrap profilinin silinerek yeni bir yerli bootstrap profili yazılmasını sağlamaktadır. Bizim tezimize konu olan çalışmada "Operatör1" yerli olmayan bir MNO profilinin yöneticisidir. SM-DP ve SM-SR arasında bir el sıkışma operasyonu gerçekleşmektedir. Burada önemli olan bu geçiş esnasında "ES4" kodu ile Şekil 3-3'te tanımlanan akış içerisinde öncelikle yeni ve yerli bootstrap profili gönderilir. Yeni ve yerli bootstrap profilinin başarılı bir şekilde içeriye alınmasından sonra, önce aktif profil pasif hale getirilir, daha sonra eUICC içerisinden bu pasif hale getirilen (eski aktif) profil silinir. Yerli olmayan bootstrap profili silinir. Yeni bootstrap profili, silinen bootstrap profilinin yerine yazılır. SM-SR SM-DP'ye sorgu atar, EID sahibi MNO için rezerv olan profil indirilir ve aktif profil olarak kaydedilir bknz Şekil 3-4.

Önerdiğimiz yöntemin doğru olarak çalıştığı ICCID ve HPLMN bilgileri Bulgularda yazıldığı gibi test edilmiştir.

4. BULGULAR

Malzeme ve yöntem kısmında açıklanan 40 adet eUICC profilinin yerli ve SIM kart üreticisi olamayan SM-SR sunucusuna taşınması başarı ile tamamlanmıştır. Bu testlerde alınan sonuçlardan sadece 1 adedi imha edilmek koşulu ile KVKK kapsamında yayınlanabilmiştir. Yaşanabilecek güvenlik açığı ve kişisel verilerin korunumu kanunu dolayısıyla kullanıcılara teslim edilecek profil bilgilerinin kullanıcı rızası ile ya da kullanıcı rızası olmadan yayınlanması kanunen yasaklanmıştır.

Transfer operasyonunun başarılı bir şekilde gerçekleştirildiğini aşağıda yer alan 4 adet profil bilgisi gözlemlenerek bulunabilir. Bu bilgiler hem QXDM üzerinden AT COMMAND Set ile teyit edilmiştir hem de SM-SR transfer işlemi yapılan eUICC'nin bağlı olduğu araç içerisinden Diagnostik Erişim Cihazı kullanılarak OBD portuna bağlanılarak ve de DDT2000 aracından istifade edilerek teyit edilmiştir.

ICCID

AT+CCID → 8990022062030892242

IMSI

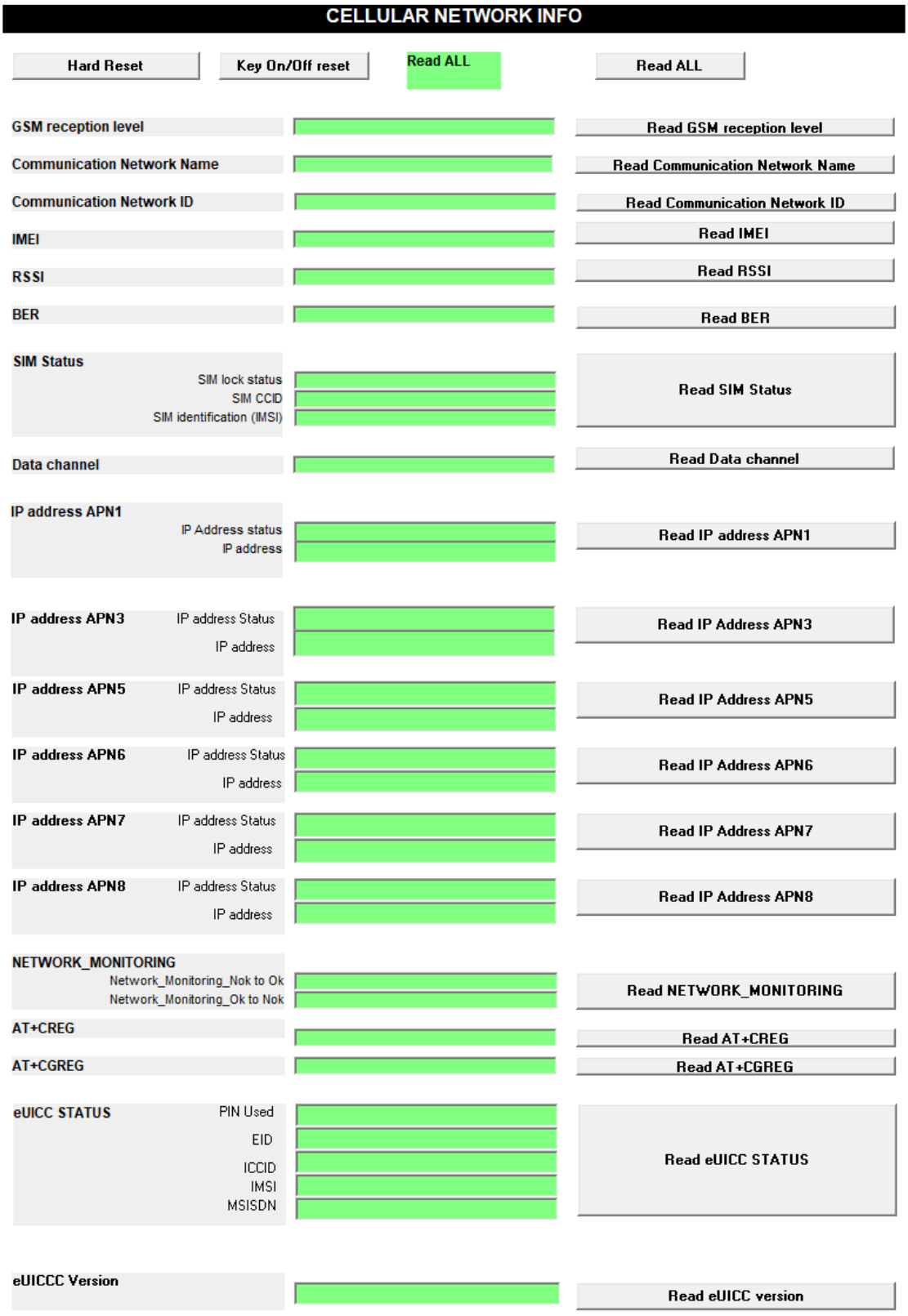
AT+CIMI →286022012328690

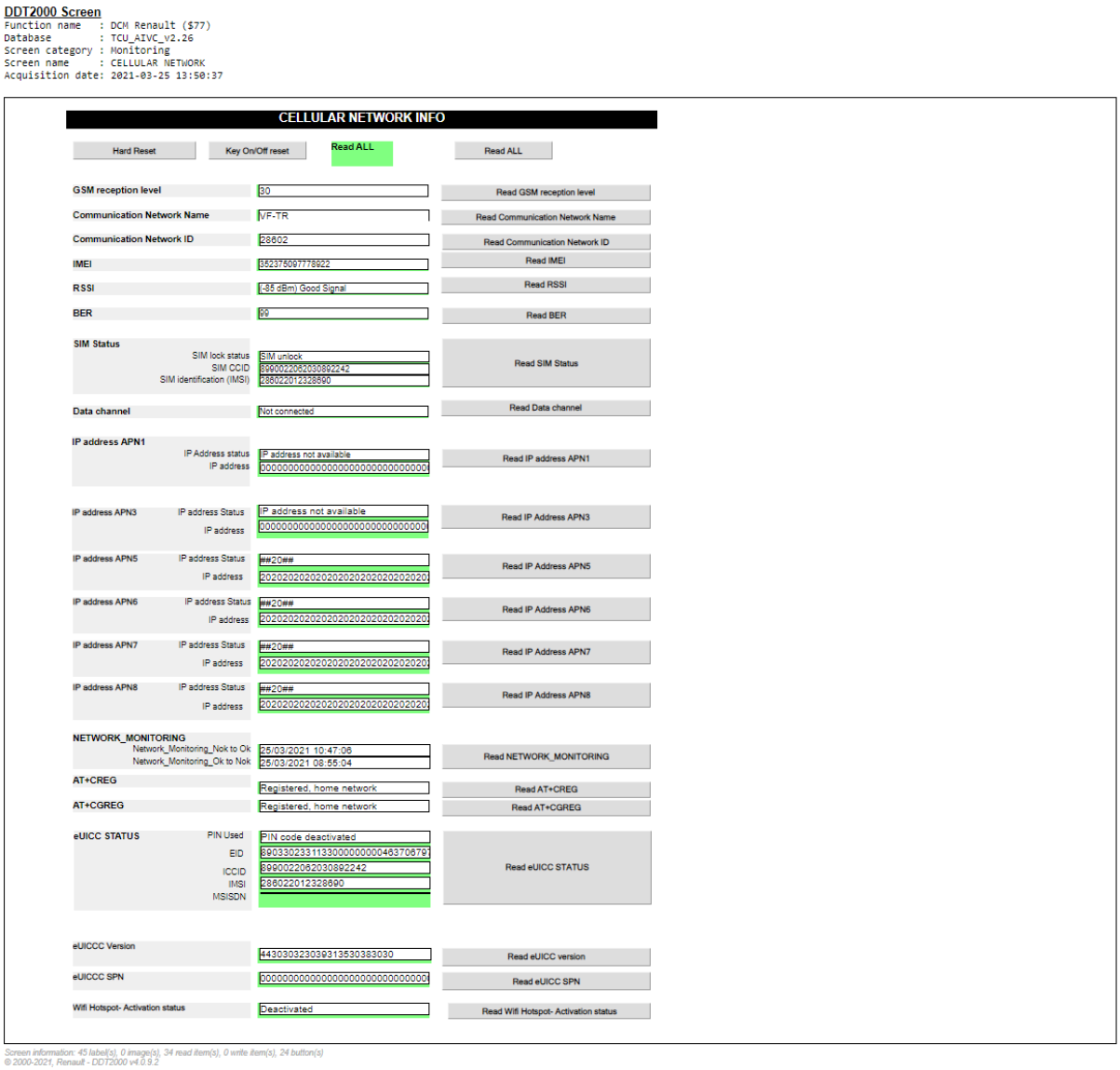
Communication Network Name

AT#SERVINFO→ VF-TR

Communication Network ID

AT#MONI? → 28602


CELLULAR NETWORK INFO
Hard Reset
Key On/Off reset
Read ALL
Read ALL
GSM reception level
Read GSM reception level
Communication Network Name
Read Communication Network Name
Communication Network ID
Read Communication Network ID
IMEI
Read IMEI
RSSI
Read RSSI
BER
Read BER
SIM Status
SIM lock status
SIM CCID
SIM identification (IMSI)
Read SIM Status
Data channel
Read Data channel
IP address APN1
IP Address status
IP address
Read IP address APN1
IP address APN3
IP address Status
IP address
Read IP Address APN3
IP address APN5
IP address Status
IP address
Read IP Address APN5
IP address APN6
IP address Status
IP address
Read IP Address APN6
IP address APN7
IP address Status
IP address
Read IP Address APN7
IP address APN8
IP address Status
IP address
Read IP Address APN8
NETWORK_MONITORING
Network_Monitoring_Nok to Ok
Network_Monitoring_Ok to Nok
Read NETWORK_MONITORING
AT+CREG
Read AT+CREG
AT+CGREG
Read AT+CGREG
eUICC STATUS
PIN Used
EID
ICCID
IMSI
MSISDN
Read eUICC STATUS
eUICCC Version
Read eUICC version



Şekil 4-1 Transfer İşlemi Başlangıcı

DDT2000 Screen

```
Function name   : DCM Renault ($77)
Database        : TCU_AIVC_v2.26
Screen category : Monitoring
Screen name     : CELLULAR NETWORK
Acquisition date: 2021-03-25 13:50:37
```



Şekil 4-2 Transfer İşlemi Sonucu

Sonuç olarak bulgular kısmında gösterilen QXDM çıktıları ve araç üzerinde okunan DDT2000 ekranları bize tezimizde anlatılan yöntemin başarılı olarak gerçekleştirildiğini göstermektedir.

Öneriler: Geriye kalan profil bilgilerinin de doğru şekilde aktarıldığı gözlemlenebilir. SIM üreticisi olmayan SM-SR sunucusundan SIM üreticisi olmayan SM-SR sunucusuna transfer süreci incelenebilir.

Sonuç: SIM üreticisi olmayan ülkelerde profil bilgilerinin güvenli bir şekilde saklanması sağlanmıştır.

5. TARTIŞMA VE SONUÇ

Bu transfer tipi Türkiye gibi kendi SIM kartını üretemeyen ancak kendi SIM kart kullanıcılarının ve SIM kart kullanarak çalışan cihazlarının milli değerini ve güvenliğini sağlamak amacı ile eUICC profillerini yerli sunucuda saklamak ve bu sunucudan yönetmek isteyen ülkelere bu işlemin nasıl yapılacağını gösteren yeni bir yöntem sunmaktadır. Burada GSMA standardında yer almayan, SIM Kart üreticisi olmayan bir sunucudan, kullanıcı profil bilgilerinin nakledilmesi işleminin garanti altına alınması büyük önem taşımaktadır. [33] dokümanında bu işlemin SIM kart üreticisi olan sunucu sağlayıcıları arasında sonradan nasıl gerçekleştirileceği anlatılmıştır. Fakat, Türkiye, Rusya, … vb. gibi SIM kart üreticisi olmayan ülkelerde sürecin nasıl uygulanacağı anlatılmamıştı. Mevcut profillerin sonradan yurtdışında kullanılma ihtiyacının doğması ya da ileride gelişecek olan farklı bir teknolojiye ayak uydurmak açısından bu tanımın yapılması gerekli olduğunu ihtiyacı fark edilerek bu alanın ihtiyacını karşılayan bir yöntem bu tezin kapsamında geliştirilmiştir. Önerdiğimiz bu yöntem GSMA standartlarına girmiştir [40].

Tüm bu eUICC teknolojisinin etkileyeceği farklı sektörler bulunmaktadır. Bireysel kullanımda olduğu gibi büyük endüstriyel ve lojistik firmalarının da etkileneceği ve faydalanacağı, çok yüksek kullanıcılı bir ekosistem oluşacaktır. [38]'da anlatılan otomotiv sektöründeki gelişmeler, bağlantılı araçların gelişmesi ve piyasadaki sayılarının artması ve buna bağlı olarak gelişen yeni yönetmelik ve kanunlar ile anlık olarak transferlerin, profil açma kapatma transfer etme gereksinimlerinin artmasına neden olacaktır. Onlarca SIM kart taşımak yerine, belirli rotalarda kullanılmak üzere belirli profiller OTA ile mobil cihazlara aktarılmasına büyük kolaylık sağlayacaktır. Örnek olarak, dünya üzerinde seyahat etmekte olan bir uçak ileride oto pilotlarının, data ihtiyaçlarını GSM üzerinden gerçekleştireceklerdir. Bunun verimli olarak kullanılabilmesi için uçaklara eUICC teknolojisi kullanılarak rota üzerinde ilgili kanunlarda [37, 39] anlatılan kısıtlar dahilinde kalacak şekilde profil geçişlerinin her ülke üzerinde hızlı ve kusursuz bir şekilde gerçekleştirilecektir. Bunun için uluslararası standarda [40] SIM üreticisi olamayan ülkelerde SM-SR sunucuları üzerinde kurallara ve kanunlara uygun bir transfer işlemi tanımlanması ile birlikte transfer işlemi SM-SR konusunda ek gereksinimleri olan alanlarda kesintisiz ve hızlı iletişim devam edebilecektir.

Bulguların gösterdiği üzere önerimiz yöntem başarı ile profil aktarımını başarılı bir şekilde yerli sunuculara aktarmış ve yönetimi yerli sunucuya taşımıştır.

QXDM loğlarının ve profil bilgilerinin doğruluğu tüm bilgiler için kontrol edilebilir. Tezi oluştururken yaptığım testler imkanlar dahilinde tam veri içeriğini kontrol edememiştir. Tüm bilgi alanları test edilerek işlem tam anlamıyla garanti altına alınabilir.

KAYNAKLAR

[1]. 6G Çalıştayı, 2021, https://sites.google.com/view/6gworkshop/, [Ziyaret tarihi: 21.04.2021]

[2]. OSI KATMANLARI, 2013, https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/osi-katmanlar%C4%B1, [Ziyaret tarihi: 15.04.2021]

[3]. Stusek, M., Zeman, K., Masek, P., Sedova, J., & Hosek, J. (2019, October). IoT protocols for low-power massive IoT: a communication perspective. In 2019 11th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT) (pp. 1-7). IEEE.

[4]. Hunkeler, U., Truong, H. L., ve Stanford-Clark, A., 2008, MQTT-S—A publish/subscribe protocol for Wireless Sensor Networks, *3rd International Conference on Communication Systems Software and Middleware and Workshops (COMSWARE'08)*, Ocak 2008, Bangalore, Hindistan, 791-798.

[5]. Al-Sarawi, S., Anbar, M., Alieyan, K., ve Alzubaidi, M., 2017, Internet of Things (IoT) communication protocols, *8th International Conference On Information Technology (ICIT)*, Mayıs 2017, Amman, Ürdün, 685-690.

[6]. Atmoko, R. A., Riantini, R., & Hasin, M. K., 2017, IoT real time data acquisition using MQTT protocol, *Journal of Physics: Conference Series*, Ekim 2016, Hotel Santika Premiere, Surabaya, Endonezya, IOP Publishing, Cilt 853 No. 1, p. 012003.

[7]. CoAP Architecture, https://raspberry-valley.azurewebsites.net/CoAP-Getting-Started/, [Ziyaret tarihi: 13.12.2021]

[8]. Danny H. Lee, D., 6.01.2021, XMPP: A Communication Protocol for the IoT,

https://medium.com/@danny_54172/xmpp-a-communication-protocol-for-the-iot-2e8fbb0fe327, [Ziyaret tarihi: 30.02.2022]

[9]. Introduction of SOAP and REST Web Services, https://www.javatpoint.com/soap-and-rest-web-services, [Ziyaret tarihi: 20.12.2021]

[10]. UPnP Device Architecture 2.0, 20.02.2015, https://docplayer.net/18111141-Upnp-device-architecture-2-0.html, [Ziyaret tarihi: 20.12.2021]

[11]. FDMA PNG Icon, https://www.iconspng.com/image/22835/fdma, [Ziyaret tarihi: 13.06.2022]

[12]. Sivakumar.D, S., Radio Interface Techniques, 20.04.2016, http://newtopics-world.blogspot.com/2016/04/radio-interface-techniques-fdmatdmacdma.html, [Ziyaret tarihi: 04.08.2022]

[13]. Avneesh Kumar, A., Difference Between GSM and CDMA Explained, 10.03.2014, https://careershapers.wordpress.com/2014/03/10/difference-between-gsm-and-cdma-explained/, [Ziyaret tarihi: 21.12.2021]

[14]. Radio Academy, https://www.taitradioacademy.com/topic/the-difference-between-fdma-and-tdma-1/, [Ziyaret tarihi: 21.12.2021]

[15]. Gopikrishnan K, G., 20.10.2020 https://technobyte.org/multiple-access-schemes-explained-compared/, [Ziyaret tarihi: 15.12.2021]

[16] R. Hoshyar, F. P. Wathan, and R. Tafazolli, "Novel low-density signaturefor synchronous CDMA systems over AWGN channel," IEEE Trans. Signal Process., vol. 56, no. 4, pp. 1616–1626, Apr. 2008.

[17]. Jasmin A. Mahal*and T. Charles Clancy, 13.06.2016, The BER analysis of OFDMA and SC-FDMA underpilot-assisted channel estimation and pilot jamming inrayleigh slow-fading channel, https://onlinelibrary.wiley.com/doi/epdf/10.1002/wcm.2685, [Ziyaret tarihi: 21.12.2021]

[18]. Mahmoud Aldababsa, Mesut Toka, , Selahattin Gökçeli, Güneş Karabulut Kurt, and Oğuz Kucur, 2018, A Tutorial on Nonorthogonal Multiple Access for 5G and Beyond, *Wireless communications and mobile computing 2018*, Hindawi, 1530-8669.

[19]. H. Nikopour, E. Yi, A. Bayesteh, K. Au, M. Hawryluck, H. Baligh, and J. Ma, 2014, SCMA for downlink multiple access of 5G wireless networks, in Proc. *IEEE Global Telecommun. Conf. (GLOBECOM)*, Aralık. 2014, Austin, TX, ABD, s 1–5.

[20]. R. Razavi, R. Hoshyar, M. A. Imran, and Y. Wang, 2011, Information theoretic analysis of LDS scheme," *IEEE Commun. Lett.*, cilt. 15, no. 8, s. 798–800.

[21]. M. Al-Imari, P. Xiao, M. A. Imran, and R. Tafazolli, 2014 , Uplink non-orthogonal multiple access for 5G wireless networks,. *Int. Symposium on Wireless Commun. Syst. (ISWCS)*, Ağustos. 2014, Barselona İspanya, s. 781– 785.

[22]. M. Al-Imari, M. A. Imran, and R. Tafazolli, 2012, Low density spreading for next generation multicarrier cellular systems, IEEE Int. Conf. Future Commun. Networks (ICFCN), Nisan 2012, Bağdat Irak, s. 52–57.

[23]. H. Nikopour and H. Baligh, 2013, Sparse code multiple access,.*Int. Symposium on Personal Indoor and Mobile Radio Commun. (PIMRC)*, Eylül. 2013, Londra İngiltere, pp. 329–336.

[24]. T. Cover, 1972, Broadcast channels, *Trans. Inf. Theory*, Ocak 1972, cilt. 18, no. 1, s. 2-14.

[25]. S. Kang, X. Dai, and B. Ren, 2015 "Pattern division multiple access for 5G," *Telecommunications Network Technology*, Mayıs 2015, cilt. 5, no. 5, s. 43–47.

[26]. L. Hanzo , M. Munster , B. J. Choi, and T. Keller, 2003, OFDM and MC-CDMA for Broadband Multi-User Communications, WLANs and Broadcasting, *John Wiley & Sons, Ltd* ISBN:9780470858790 , s 978.

[27]. T. Abe and T. Matsumoto, 2003, Space-time turbo equalization in frequency-selective MIMO channels, *IEEE Trans. Veh. Technol*, Mayıs 2003, cilt. 52, no. 3, s. 469-475.

[28]. M. Y. Alias, S. Chen, and L. Hanzo, 2005, Multiple-antenna-aided OFDM employing genetic-algorithm-assisted minimum bit error rate multiuser detection, *IEEE Trans. Veh. Technol*, Eylül 2005, cilt. 54, no. 5, s. 1713–1721.

[29]. L. Hanzo, S. Chen, J. Zhang, and X. Mu, 2014, Evolutionary algorithm assisted joint channel estimation and turbo multi-user detection/decoding for OFDM/SDMA, *IEEE Trans. Veh. Technol*, Mart. 2014., cilt. 63, no. 3, s. 1204–1222.

[30]. S. Vanka, S. Srinivasa, Z. Gong, P. Vizi, K. Stamatiou, and M. Haenggi, Superposition coding strategies: Design and experimental evaluation, *IEEE Trans. Wireless Commun*., cilt. 11, no. 7, s. 2628–2639.

[31]. N. I. Miridakis and D. D. Vergados, 2013, A survey on the successive interference cancellation performance for single-antenna and multiple-antenna OFDM systems, *IEEE Commun. Surveys Tutorials*, cilt. 15, no. 1, s. 312-335.

[32]. Abhay Mohan, Ocak 2017, Non Orthogonal Multıple Access, Teknik rapor, Doi: 10.13140/RG.2.2.35859.89126.

[33]. GSMA Embedded SIM Remote Provisioning Architecture, 07.07.2020, https://www.gsma.com/esim/wp-content/uploads/2020/07/SGP.01-v4.2.pdf, [Ziyaret tarihi: 11.10.2021]

[34]. Duraisamy, S., 2017. A Case Study Review: Future of Internet of Things (IoT) in Malaysia, *International Jornal of Information Systeeand Engineering*, Kasım 2017, cilt:5 no:2 s126-138. Doi: 10.24924/ijise/2017.11/v5.iss2/126.138.

[35]. Colin Pawsey, C., Advanced Automotive Diagnostics Systems 13.11.2018, https://www.automotive-iq.com/autonomous-drive/articles/advanced-automotive-diagnostics-systems-from-diagnostics-to-prognostics, [Ziyaret tarihi: 21.12.2021]

[36] Updates Over The Air, https://www.bosch-mobility-solutions.com/en/mobility-topics/updates-over-the-air/, [Ziyaret tarihi: 21.12.2021]

[37]. BTK eSIM kararnamesi, 12.02.2019, Uzaktan Programlanabilir SIM Teknolojileri (eSIM), https://www.btk.gov.tr/uploads/boarddecisions/uzaktan-programlanabilir-sim-teknolojileri-esim/053-2019-web.pdf, [Ziyaret tarihi: 10.09.2021]

[38] Fethiye ÇUHADAROĞLU Otomotiv Sektöründe Bağlantılı Araçların Gelişiminde Mobil Şebekeler: Bilgi Teknolojileri ve İletişim Kurumu İçin Öneriler https://www.btk.gov.tr/uploads/thesis/fethiye-cuhadaroglu-tez.pdf, Mayıs 2021

[39] 112 Acil Çağrı Servisi Tabanlı Araç İçi Acil Çağrı Sisteminin Yerleştirilmesi İle İlgili Tip Onayı Yönetmeliği, 2015/758/AB, 16.08.2016, https://www.resmigazete.gov.tr/eskiler/2016/08/20160819-3.htm, [Ziyaret tarihi: 12.08.2021]

[40]. Embedded SIM Remote Provisioning Architecture Version 4.0 25 February 2019, https://www.gsma.com/newsroom/wp-content/uploads//SGP.01-v4.0.pdf, [Ziyaret tarihi: 20.12.2021]

EKLER

5.1. TURNİTİN TARAMASI

Nazif_Guray_Gungor

ORİJİNALLİK RAPORU

%11	%10	%1	%6
BENZERLİK ENDEKSİ	İNTERNET KAYNAKLARI	YAYINLAR	ÖĞRENCİ ÖDEVLERİ

BİRİNCİL KAYNAKLAR

1	tr.wikithe.ru İnternet Kaynağı	%3
2	Submitted to The Scientific & Technological Research Council of Turkey (TUBITAK) Öğrenci Ödevi	%2
3	www.theseus.fi İnternet Kaynağı	%1
4	trokul.com İnternet Kaynağı	%1
5	acikbilim.yok.gov.tr İnternet Kaynağı	%1
6	nek.istanbul.edu.tr:4444 İnternet Kaynağı	<%1
7	www.slideserve.com İnternet Kaynağı	<%1
8	9lib.net İnternet Kaynağı	<%1
9	dspace.akdeniz.edu.tr İnternet Kaynağı	<%1