NECMETTİN ERBAKAN
ÜNİVERSİTESİ

RTL-SDR Tabanlı Teknolojiler ile GSM Sinyal Analizi

[1] Fatih KARAGÖZ

Necmettin Erbakan Üniversitesi Bilgisayar Mühendisliği

fatihkkaragoz@gmail.com

Danışman Yrd. Doç Dr. Mehmet HACIBEYOĞLU

Özet

GSM mobil haberleşmede en çok kullanılan protokollerden biridir. Bu projede GSM protokol kullanan radyo frekanslarının belirlenmesi, analiz edilmesi ve son olarak şifrelenmiş sinyallerin açılması üzerinde duracağız. Bu işlemlerin yapılmasını sağlayan hem maaliyet hem performans açısından avantajları büyük olan SDR (Software Defined Radio) mimarisi üzerinde çalışma prensiplerinden bahsedilmek amaçlanmıştır.

SDR (Software Defined Radio) ağ katmanında çalışan ve özelleştirilmiş işler için üretilen donanımların hızlı frekans değiştirme özelliğinden yararlanarak çalışması mantığına denilenilir.

Anahtar kelimeler: SDR, Yazılım tabanlı radyo, GSM, GSM sinyal analizi, Mobil.

Abstract

GSM is one of the most used protocol in mobile communicatons. In this project , we intend determine the frequence of radio by using GSM protocol, and analyse it. Finally, we intend the decode the encrypted GSM signals. We used the SDR which SDR is both cheap technology and has performance.

SDR(Software Defined Radio) is working logic of developed hardware for specified work that works at the network layer.

Keywords : SDR, Software Defined Radio, GSM GSM signal analyse, Mobile.

1. Giriş

GSM 1980'li yılların başlarında Avrupa ülkeleri tarafından mobil iletişim standardını oraya koymak amacıyla geliştirilmiştir İlk yıllarında sadece Batı Avrupa ülkelerinin kullandığı bir standart olarak GSM ağına 1990'lı yıllarda Doğu Avrupa ve Avusturalya ardından ABD ve Güney Amerika eklendi. Yıllara göre dünyaya yayılma grafiği bir hayli hızlı seyreden GSM'in globalleşmesi evrensel bir mobil ağ kavramını doğurdu. Yola çıkış yıllarında Avrupa Telekomünikasyon Standartlar Komitesi'nin bir alt kuruşu olan Groupe Speciale Mobile'ın ismini taşısa da evrensel bir standart haline gelmesi öngörüldükten sonra "*Global System for Mobile Communicaitons*" ismi ile anılan mobil cihazlar için tasarlanan bir iletişim protokolüdür. GSM protokolünün 212 ülkede 2 milyardan fazla insan tarafından kullanılıyor olmasının sebebi

kullandığı hücresel ağ mantığıdır. GSM protokolünde bir iletişim hücreler arasında geçiş yapabildiğinden ötürü ülke, şehir gibi ayarlamalar yamaksızın hücreler arası geçiş özelliği sayesinde iletişim devam ettirebilir, bu da GSM protokolünü kullanan cihazların süreklilik ilkesine uygunluğunu gösterir.

1.1 Hücresel Yapı

Mobil ağları baz alacak olursak öncelikle alt ağlar (örn. İlçeler, semtler) kendi içlerin "hücre" denilen alanlara bölünür ve her hücrede bir baz istasyonu bulunur. Baz istasyonu istemci ve sunucu arasındaki iletişimi sağlayan sınırlı bir frekans aralığına sahip ekipmandır. Frekansların sınırlı olmasından dolayı aynı anda iletişim kurabilen cihaz sayısı da sınırlı olur. Hücresel yapıda çok sayıda istemcinin olduğu bir yere daha çok baz istasayonu konularak kapasite artırılmaktadır. Günümüzde baz istasyonlarında tevcih denilen bir sistem kullanılmaktadır ki bu da farklı yönlere doğru farklı güçlerde sinyaller yayarak çift yönlü iletişim sağlamaktadır.

Şekil 1.1.A : Bölünmüş hücresel yapı

1.2 Kullanılan frekans aralıkları

GSM standardında ihtiyaca göre frekans aralıklarına bölünmüş ve GSM protokolü için ayrılmış radyo frekansları vardır. GSM900 ve GSM1800 bunlardan en yaygın olanıdır.

GSM900: 900 Mhz bandında çalışan GSM900'da ayrılmış frekanslar 890-915 Uplink, 935-960 Downlink olarak rezerve edilmiştir. 50 Mhz'lik kullnabılabilir bir frekans aralığı söz konusudur bu da 125 çift frekansa denk gelmektedir.

GSM1800: 1800 Mhz bandında çalışan GSM protokolü versiyonudur ki; 1710-1785 arası uplink, 1805-1880 downlink olarak ayrılmıştır. 150Mhz toplam frekans sayısıdır ve frekans çifti 275 toplam fiziksel kanal 3000'e kadar çıkmaktadır.

Günümüzde yaygın olarak GSM900 kullanılmaktadır.

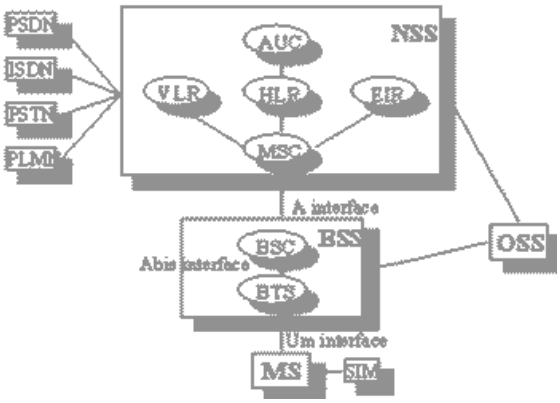
Uplink : GSM ağlarında baz istasyonuna doğru olan trafiğe denir.

Downlink : Baz istasyonundan mobil cihaza doğru olan trafiktir.

2. GSM ağ mimarisi

İki mobil cihazın iletişimi 4 parçadan oluşur.

i. Mobile Station
ii. Base Station Subsystem
iii. Network and Switching Subsystem
iv. Operating and Support Subsystem



Şekil 2.A : GSM Ağ Mimarisi

2.1 Mobile Station : Mobil istasyon mobil bir cihazdır. Teorik olarak tam çift yönlü iletişim mimarisine göre hem istemci hem snucudur. Kendi içinde ikiye ayrılır.

Bunlardan biri teminaldir monte edilmiş istemcilerdir denilenilir sabit telefonlar terminallere örnek verilebilir.

Bir diğeri SIM'dir. SIM'ler akıllı kartlar (Smart Card) olarak da adlandırılırlar. Tam manasıyla mobildir. PIN(Personel Identifier Number)'ler ile korunurlar.

2.2 Base Station Subsystem

NSS(Network and Switching Subsystem) ile ietişim kurmak için gereklilikleri içeren donanımları barındıran uzaydır. İçerisinde Baz İstasyonu ve Baz Kontrol İstasyonu'nu barındırır. Santral ile mobil istasyonun arasındaki bir geçiş kapısı görevi gören cihazlar topluluğu da denilebilir. BSC(Base Station Controller) yani Baz istasyonu denetleyicier ve BTS(Base Transceiver Station) yani Baz istasyonu alıcı-vericileri olmak üzere iki parçadan oluşur.

Baz istasyonu katmanında GSM protokolü dahilinde herbir konuşma kanalı TDMA (Time Division Multiple Access) tekonolojisi kullanılarak 8 parçaya ayrılarak veri taşıma yolları oluşturulur. Yani 8 kişi için görüşme sağlar.

2.2.1 BSC(Base Station Controller) Baz İstasyonu Denetleyiciler

Burda baz istasyonu ve santrallerle (MSSC – Mobile Service Switching Center) olan iletişimin doğruluğu teyid edilir ve onaylanan iletişim için güvenli çift yönlü bir kanal açılma işlemi gerçekleştirilir. Ayrıca "handover" denilen mobil istasyonun konuşma esnasında kullandığı kanalın herhangi bir nedenden değiştirilmesi işlemini kontrol eder.

Not: Burada bahsi geçen "handover" işlemi farklı aynı hücre içinde farklı frekans kanalları arasında yapılan geçiş işlemidir. Bir diğer "handover" işlemi ise farklı hücreler arasında yapılır, yani mobil istasyonun konum değiştirmesi gibi. Bu "handover" geçiş işlemini MSSC yapar.

2.2.2 BTS(Base Transceiver Station)

Mobil istasyonun santral ile iletişim kurabilmesi için gerekli donanımları içeren katmandır. BSB ile entegre çalışmak zorundadır. Frekansların paylaşımı isteklere cevap verebilme, gürültüleri en aza indirebilme gibi görevleri de vardır.

2.3 Network and Switching Subsystem

Bu bölümde öncelikle GSM yapısının kullandığı anahtarlama sisteminden söz edilecektir. Şebekede birbiriyle haberleşmekte olan iki cihazın birbirleri ile bağlantıya geçmesini sağlayan sistematik işlerdir. GSM'de devre anahtarlamalı sistem kullanılmaktadır.

Kısaca anahtarlama sisteminin çalışma prensibine değinecek olursak, aranacak bir numara ve aranan bir numara arasındaki

iletişim SS7 (Signalling System 7) Numara 7 İşaretleme Sistemi olarak Türkçe anılan sistemde santral ile mobil istasyon arasında bir “offhook” yapılır yani alışılagelmiş TCP bağlantılarında 3 Way Handshake aşamasında SYN paketi gönderimi gibi arkasından santral tarafından bir ses yollanır ki bu da yine üçlü el sıkışmada SYN+ACK paketi yani bir bağlantı kurulabilir cevabı ile benzerlik göstermektedir. Bağlantı kurulup paketler yollandıktan sonra yani telefon kapatıldıktan sonra üçlü el sıkışmada yapılan RST paketine benzer olarak SS7 sisteminde “onhook” gönderilir ki bu gönderim bağlantının düştüğünü belirtir. SS7 sisteminin başlıca avantajları,

I. Hatları daha verimlil kullanarak gürültüyü engellemek

II. Noktadan noktaya en doğru yolu seçmek ve iletişimi buu yol üzerinden açarak karmaşıklığı engellemek

olarak gösterilebilir.

Devre anahtarlamalı sistemde:

2.3.1 HLR (Home Location Register) Merkez Konum Kaydı

Mobil istasyonlar ile ilgili bilgilerin tutulduğu veritbanıdır. Bir kayıt sistemi kullanılarak aboneler girdikleri santral bölgesindeki HLR’nin VLR’den kullanıcıya ait bilgileri istemesi veya “roaming” (dolaşım) yapıyor olması halinde SIM kart bilgilerinin önce VLR’ye aktarılıp arkasından HLR’nin isteği üzerine HLR veritabanına kaydedilmesi ile yapılır.

2.3.2 VLR (Visitor Location Register) Ziyaretçi konum kaydı

Ziyarteçi aboneler için geçici bir veritabanı görevi görür. Bir abone bir baz istasyonuna ve baz istasyonunun bağlı olduğu santraln bölgesine girdiğinde VLR, HLR(Home Location Register) Merkez konum kaydından bu abone hakkında bilgi ister. Ve kendi veritabanına kaydederek ziyaretçiyi tanır. Santrale ait alandan çıkarsa o VLR’den mobil isatasyona ait kayıt silinir.

2.3.3 MSSC (Mobile Services Switching Center)

Ağ arayüzü ile bağlantıları kontrol eder. SS7 işaretleme işlemleri burada gerçekleşir.

2.3.4 AUC (Authentication Center) Doğrulama Merkezinin

GSM bağlantılarının olası saldırılardan korunması için gerekli şifreleme parametrelerini içerir.

2.3.5 EIR (Equipmant Identitiy Register) Cihaz Kimlik Kaydı

Ağa erişim yetkileri alınmış veya kısıtlanmış cihazların yönetimi gibi işlerin yapılabileceği bu alt katman cihaz bilgilerini tutan bir veritabanı olarak da adlandırılır. Ağ yönetim birimlerinde bulunan kara liste, beyaz liste “white list, black list” yani sadece bu cihazlar ağa erişim yetkisine sahiptir (white list) ya da sadece bu cihazlar ağa erişemesin (kara list) denilen mantıklarla benzerlik göstermektedir.

3.1 RTL-SDR Teknolojileri

Eskiden geniş radyo donanımlarına ekstra maaliyet ödenmekte iken RTL-SDR teknolojileri ile 5$ ile 20$ arasında değişiklik gösterebilen donanımların hızlı frekans değişitme özelliğinden yararlanarak radyo sinyallerini dinleme denilebilir. Uçakların yerlerini kendi radar ağlarını kullanarak tespit etme, meteoroloji balonlarını dinleme ve meteoroloji ile eşzamanlı olarak analiz edebilme, televizyon kanallarının frekans aralığında gezerek televizyon olmadan televizyon izleme bunlara verilebilecek basit örnekleri iken, dijital ortamlarda aktarılan ses sinyallerinin dinlenmesi, uçakların kule ile kurdukları iletişimi analiz edebilir, GSM sinyallerini analiz edebilme gibi şifrelenmiş olabilme ihtimali olan sinyal türleri üzerinde de uğraşılabilir.

Bahsi geçen cihazlara jargonda ‘dongle’ da denilebilmektedir. Bu cihazlar söylenildiği gibi piyasada 5$ ile 20$ arasında meblalara daha çok yurtdışından (çin, malezya) getirtilebilir. Farklı frekans aralıklarında bulunabilir ve ihtiyaca göre seçilmelidir.

Şekil 3.1.A : Çalışmada kullanılan Elonics E400 ya da altyapısında kullandığı teknoloji ile RTL2832U Elonics E400 55 MHz ile 2300 MHz arasında çalışabilme özelliğine sahip olup hemn hemn bütün RTL-SDR araçlarıyla çalışabilme özellliğine sahiptir.

4.1. Bir GSM sinyalini yakalama

GSM sinyali yakalamak için baz istasyonlarının yayın kanalları arasında gezmek gerekir ki bu dolu bir kanal bulma işlemidir. Bu işlem için Linux üzerindeki “grgsm” aracı gerek sistem kaynaklarının verimli kullanılması gerekse efektif çalışma açısından gayet “legihtweight” yani diğer araçlara göre bilgisayarı sistemi meşgul etmeyen bir araçtr. Bu yüzden bahsi geçen projede bu araç kullanılmaktadır.

4.1.1 GRGSM aracı ve özellikleri

GRGSM açık kaynaklı olmasından dolayı Github üzerinde kolaylıkla kaynak kodları bulunabilen kurulum aşamlarını kaynakçada belirteceğimiz bağlantı üzerinden indirilip elle kurulum yapılması gereken bir RTL-SDR aracıdır. Linux üzerinde bazı bağımlılıklar içerir. Bu bağımlıklar Linux kütüphanelerine bazı RTL-SDR kütüphaneleri eklemenizi ve kurmanızı ister.

Şekil 4.1.1.A : GR-GSM RTL-SDR Tool

4.1.1.1 RTL2832U aracımızı kalibre etmek

Kullandığımız cihaz/cihazlar default olarak geniş bir frekans aralığında geldiğinden bu frekans aralığını kullandığımız projeye göre ayarlamamız bize hız kazandıracaktır, aksi taktirde tüm frekanslar üzerine arama sinyali gönderileceği için zaman verimsiz bir proje olacaktır. Bahsi geçen projede "kal" adı verilen sdr cihazlarını kedisine parametre olarak verilen frekans aralığına göre kalibre etmek amacıyla tasarlanmış Linux komut satırında çalışan ve herhangi bir arayüzü bulunmayan aracı kullanacağız.

Kal aracında kullanacağımız parametreler -s (kullanılan GSM frekans aralığı sisteminin adı) ve -g (gain yani kaç dbi aralığında tarama yapılacağıdır.)

```
root@hmtteol:/home/hmtteol# kal -s GSM900 -g 40
Found 1 device(s):
  0:  Generic RTL2832U OEM

Using device 0: Generic RTL2832U OEM
usb_claim_interface error -6
Failed to open rtlsdr device #0.
root@hmtteol:/home/hmtteol# kal -s GSM900 -g 40
Found 1 device(s):
  0:  Generic RTL2832U OEM

Using device 0: Generic RTL2832U OEM
Found Fitipower FC0012 tuner
Exact sample rate is: 270833.002142 Hz
Setting gain: 40.0 dB
kal: Scanning for GSM-900 base stations.
[FC0012] no valid PLL combination found for 948600000 Hz!
Tuning to 948600000 Hz failed!
```

Şekil 4.1.1.1.A : Kal RTL-SDR kalibre aracı kullanımı

Kalibre edilme işi esnasında iki çeşir sonuç alınır. İlki kapalı veya herhangi bir açılmış bağlantı olmayan frekanslar bir diğeri ise bağlantı açılmış frekanslardır. Bağlantı açılmamış frekanslar "failed" olarak

```
Tuning to 948600000 Hz failed!
[FC0012] no valid PLL combination found for 948600000 Hz!
```

Şekil 4.1.1.1.B : Bağlantı açılmamış veya boş frekansların ekran çıktısı.

Bağlantı açılmış frekansların ise bir kanal numarası bulunur ve bu kanal numarası evrensel standartlar gereği frekans ile bulunur.

```
GSM-900:
        chan: 10 (937.0MHz + 15.592kHz) power: 1462977.30
        chan: 46 (944.2MHz - 20.230kHz) power: 1489517.14
        chan: 60 (947.0MHz + 35.040kHz) power: 3037278.75
        chan: 61 (947.2MHz - 20.249kHz) power: 5199913.08
```

Şekil 4.1.1.1.C : Bağlantı açılmış ve kanal numarasına sahip frekans çıktısı

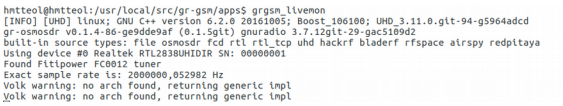
Analaşılacağı üzere belli başlı frekans aralıkları dolu ve bu aralıklarda herhangi bir GSM bağlantısı olmuş olma olasılığı ve bir konuşma yapılabiliyor olabilme olasılığı mümkün. Hedef frekans aralığı belirlendikten sonra paketlerin yakalanması için gerekli ortamı hazırlamamız gerekiyor.

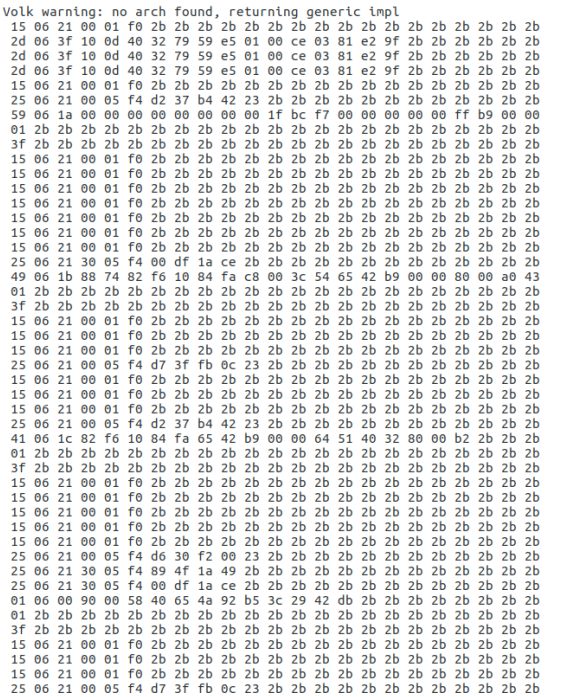
4.1.1.2 Paketlerin yakalanması ve monitörlenmesi

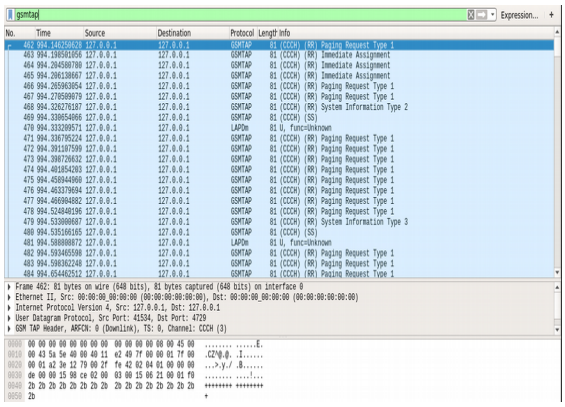
Paketleri yakalamak için gr-gsm aracını kullanacağımızı söylemiştik paket analizni yapmanın iki yolu vardır. İlki direkt canlı olarak izleemek ve bir araç ile analiz edip paketleri bırakmaktır. İkincisi kayıt altına alıp kaydedilmiş paketler üzerinden analiz yapmaktır. İlk olarak canlı paket analizi yapalm. Bu gr-gsm'in "*livemon*" adlı modulü ile yapıyoruz. Kaynakçada kullanımı için bağlantısı verilen grgsm_livemon adlı python programı paketleri yakalar fakat analiz için bir monitörleme aracına ihtiyaç duyar. Bahsi geçen projede monitörleme aracı olarak TCP/IP ağlarında sıkça kullanılan ve daha birçok protokole ait verilen analiz edilmesine olanak sağlayan araç olan "*Wireshark*" kullanacağız. Linux komut satırından root kullanıcısı olarak Wiresharkı açıyoruz.

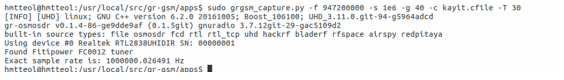
```
hmtteol@hmtteol:~$ sudo su
root@hmtteol:/home/hmtteol# wireshark
QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
```

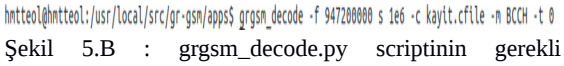
Şekil 4.1.1.2.A : Wiresharkın açılması











Arkasından local olarak bilgisayarımıza taktığımız “*dongle*” ile çalışacağımız için “*lo*” yani “*loopback*”i seçiyoruz.

Monitörleme ortamını hazırladığımıza göre artık paketleri yakalayabiliriz.

```
hmtteol@hmtteol:/usr/local/src/gr-gsm/apps$ grgsm_livemon
[INFO] [UHD] linux; GNU C++ version 6.2.0 20161005; Boost_106100; UHD_3.11.0.git-94-g5964adcd
gr-osmosdr v0.1.4-86-ge9dde9af (0.1.5git) gnuradio 3.7.12git-29-gac5109d2
built-in source types: file osmosdr fcd rtl rtl_tcp uhd hackrf bladerf rfspace airspy redpitaya
Using device #0 Realtek RTL2838UHIDIR SN: 00000001
Found Fitipower FC0012 tuner
Exact sample rate is: 2000000,052982 Hz
Volk warning: no arch found, returning generic impl
Volk warning: no arch found, returning generic impl
```

Şekil 4.1.1.2.B : grgsm_livemon.py scriptinin çalıştırılması

Gr-gsm Livemon programına bir frekans veriyoruz ki bu frekans “*kal*” programından aldığımız ve içersinde bir GSM bağlantısı olduğunu düşündüğümüz frekanstır.

Bu frekansı alıp gr-gsm livemon’un frequency alanına girdiğimizde paketlerimiz yakalanmaya başlıyor.

```
Volk warning: no arch found, returning generic impl
 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 2d 06 3f 10 0d 40 32 79 59 e5 01 00 ce 03 81 e2 9f 2b 2b 2b 2b 2b 2b
 2d 06 3f 10 0d 40 32 79 59 e5 01 00 ce 03 81 e2 9f 2b 2b 2b 2b 2b 2b
 2d 06 3f 10 0d 40 32 79 59 e5 01 00 ce 03 81 e2 9f 2b 2b 2b 2b 2b 2b
 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 25 06 21 00 05 f4 d2 37 b4 42 23 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 59 06 1a 00 00 00 00 00 00 00 00 1f bc f7 00 00 00 00 00 ff b9 00 00
 01 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 3f 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 25 06 21 30 05 f4 00 df 1a ce 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 49 06 1b 88 74 82 f6 10 84 fa c8 00 3c 54 65 42 b9 00 00 80 00 a0 43
 01 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 3f 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 25 06 21 00 05 f4 d7 3f fb 0c 23 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 25 06 21 00 05 f4 d2 37 b4 42 23 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 41 06 1c 82 f6 10 84 fa 65 42 b9 00 00 64 51 40 32 80 00 b2 2b 2b 2b
 01 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 3f 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 25 06 21 00 05 f4 d6 30 f2 00 23 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 25 06 21 30 05 f4 89 4f 1a 49 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 25 06 21 30 05 f4 00 df 1a ce 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 01 06 00 90 00 58 40 65 4a 92 b5 3c 29 42 db 2b 2b 2b 2b 2b 2b 2b 2b
 01 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 3f 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
 25 06 21 00 05 f4 d7 3f fb 0c 23 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
```

Şekil 4.1.1.2.C : Yakalanan paketlerin terminaldeki hexadecimal karşılıkları

Yakalanan paketleri Wireshark’ta görsel bir sıraya dökmek ve analizi kolaylaştırmak adına “*gsmtap*” filtresini verebiliriz.

```
No.   Time          Source      Destination  Protocol Length Info
  462 994.146250628 127.0.0.1   127.0.0.1    GSMTAP     81 (CCCH) (RR) Paging Request Type 1
  463 994.198501056 127.0.0.1   127.0.0.1    GSMTAP     81 (CCCH) (RR) Immediate Assignment
  464 994.204580780 127.0.0.1   127.0.0.1    GSMTAP     81 (CCCH) (RR) Immediate Assignment
  465 994.206138667 127.0.0.1   127.0.0.1    GSMTAP     81 (CCCH) (RR) Immediate Assignment
  466 994.265963054 127.0.0.1   127.0.0.1    GSMTAP     81 (CCCH) (RR) Paging Request Type 1
  467 994.270509079 127.0.0.1   127.0.0.1    GSMTAP     81 (CCCH) (RR) Paging Request Type 1
  468 994.326276187 127.0.0.1   127.0.0.1    GSMTAP     81 (CCCH) (RR) System Information Type 2
  469 994.330654066 127.0.0.1   127.0.0.1    GSMTAP     81 (CCCH) (SS)
  470 994.333209571 127.0.0.1   127.0.0.1    LAPDm      81 U, func=Unknown
  471 994.336795224 127.0.0.1   127.0.0.1    GSMTAP     81 (CCCH) (RR) Paging Request Type 1
  472 994.391107599 127.0.0.1   127.0.0.1    GSMTAP     81 (CCCH) (RR) Paging Request Type 1
  473 994.398726632 127.0.0.1   127.0.0.1    GSMTAP     81 (CCCH) (RR) Paging Request Type 1
  474 994.401854203 127.0.0.1   127.0.0.1    GSMTAP     81 (CCCH) (RR) Paging Request Type 1
  475 994.458944960 127.0.0.1   127.0.0.1    GSMTAP     81 (CCCH) (RR) Paging Request Type 1
  476 994.463379694 127.0.0.1   127.0.0.1    GSMTAP     81 (CCCH) (RR) Paging Request Type 1
  477 994.466904882 127.0.0.1   127.0.0.1    GSMTAP     81 (CCCH) (RR) Paging Request Type 1
  478 994.524840196 127.0.0.1   127.0.0.1    GSMTAP     81 (CCCH) (RR) Paging Request Type 1
  479 994.533000687 127.0.0.1   127.0.0.1    GSMTAP     81 (CCCH) (RR) System Information Type 3
  480 994.535166165 127.0.0.1   127.0.0.1    GSMTAP     81 (CCCH) (SS)
  481 994.588808872 127.0.0.1   127.0.0.1    LAPDm      81 U, func=Unknown
  482 994.593465598 127.0.0.1   127.0.0.1    GSMTAP     81 (CCCH) (RR) Paging Request Type 1
  483 994.598362248 127.0.0.1   127.0.0.1    GSMTAP     81 (CCCH) (RR) Paging Request Type 1
  484 994.654462512 127.0.0.1   127.0.0.1    GSMTAP     81 (CCCH) (RR) Paging Request Type 1

▸ Frame 462: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface 0
▸ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
▸ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
▸ User Datagram Protocol, Src Port: 41534, Dst Port: 4729
▸ GSM TAP Header, ARFCN: 0 (Downlink), TS: 0, Channel: CCCH (3)

0000  00 00 00 00 00 00 00 00  00 00 00 00 08 00 45 00   ........ ......E.
0010  00 43 5a 5e 40 00 40 11  e2 49 7f 00 00 01 7f 00   .CZ^@.@. .I......
0020  00 01 a2 3e 12 79 00 2f  fe 42 02 04 01 00 00 00   ...>.y./ .B......
0030  de 00 00 15 98 ce 02 00  03 00 15 06 21 00 01 f0   ........ ....!...
0040  2b 2b 2b 2b 2b 2b 2b 2b  2b 2b 2b 2b 2b 2b 2b 2b   ++++++++ ++++++++
0050  2b                                                 +
```

Şekil 4.1.1.2.D : Yakalanan paketlerin Wireshark monitörleme ortamı görüntüsü

5. Yakalanan sinyallerinin kod çözme işlemleri

Yakalanan paketlerin kod çözülebilme işlemi için ARFCN numarasını pakelerin içinden “*immediate assignment*” paketlerinden alıyoruz.

Burada artık alınan paketleri kayıt altın almamız gerekiyor bunun içinde “*grgsm_capture.py*” scriptini kullanıyoruz.

```
hmtteol@hmtteol:/usr/local/src/gr-gsm/apps$ sudo grgsm_capture.py -f 947200000 -s 1e6 -g 40 -c kayit.cfile -T 30
[INFO] [UHD] linux; GNU C++ version 6.2.0 20161005; Boost_106100; UHD_3.11.0.git-94-g5964adcd
gr-osmosdr v0.1.4-86-ge9dde9af (0.1.5git) gnuradio 3.7.12git-29-gac5109d2
built-in source types: file osmosdr fcd rtl rtl_tcp uhd hackrf bladerf rfspace airspy redpitaya
Using device #0 Realtek RTL2838UHIDIR SN: 00000001
Found Fitipower FC0012 tuner
Exact sample rate is: 1000000.026491 Hz
hmtteol@hmtteol:/usr/local/src/gr-gsm/apps$ █
```

Şekil 5.A : Yakalanan paketlerin kayıt altına alınması

Kayıt altına almak için çeşitli paremetreler kullnaılmıştır kısaca “-f” parametresi kayıt altına alınacak frekansı göstermektedir. “-s” parametresi frekans aralığının MHz veya Khz cinsinden kaç sıfır içerdiğini 1e6, 1e3 cinsinden belli eder. “-g” gain yani frekans taraması yapılacak alanı belirler.

Daha sonra Kc ve TMSI denilen mobil istasyonun baz istasyonu ile bağlantı kurarken doğrulama yaptığı değerler telefona indirilen bir uygulama sayesinde alınır ve “*grgsm_decode.py*” programı çalıştırılır.

```
hmtteol@hmtteol:/usr/local/src/gr-gsm/apps$ grgsm_decode -f 947200000 s 1e6 -c kayit.cfile -m BCCH -t 0
```

Şekil 5.B : grgsm_decode.py scriptinin gerekli parametreler ile paketleri decode etmesi

TMSI değeri ile paketler arasında arama yapıp çıkan *“immediate assignment”* paketlerinin birinden timeslot değeri alınır.

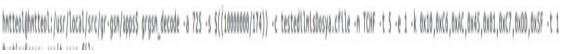
“*system information type 1”* paketlerinin birinden ARFCN numaraları listesi alınır.

Wireshark paketlerinde paketlerin hangi algoritma ile şifrelendiği bilgisi de yer alır. Genelde A5/3 şifreleme algortması ile şifrelenmiş olur ki *“grgsm_decode.py”* bu algoritmayı çözebilir.

Şekil 5.C : Decode aşamasında TMSI Kc key’inin kullanılması.

Decode edilmiş paketler içerisinde tekardan TMSI değeriyle arama yapıldıktan sonra *“assignment command”* paketlerinin birinden *“Training sequence” “Hopping channel” “MAIO” “HSN”* değerleri alınır.

grgsm_decode.py programına tekrar alınan bu değerler paremetre olarak verilip çıktı dosyası .au.gsm uzantısıyla kayıt edilir.



Şekil 5.D : Paketlerden çıkartılan belirleyici bilgilerin tekar grgsm_decode programına verilmesi

Kaydedilen dosyayı kaynakçada bağlantısı verilen dosyanın içinde gsm sinyallerine dair bir sinyal olup olmadığını bulan bu araç ile incelendikte sonra tekrar grgsm_decode programına sample rate ve test aracından alınan dosya eklenerek gerekli parametreler ile verilir.

Şekil 5.E : Gerekli parametrelerle decode edilmiş ses dosyasının çıkarılması

6.Sonuç

RTL-SDR teknolojileri kullanılarak ucuz donanımlar üzerinde büyük radyo frekansları yakalayarak herhangi bir ortamda aralarında bağlantı kurulan baz istasyonu ve mobil cihaz arasında bilinen TMSI ve Kc(Key) değeri ile bir mobil cihaza ait kayıt altına alınmış ve yerel hafızada depolanmış şifreli GSM paketlerinden ses dosyalarının çıkarılması için öncelikle gerekli kimlik doğrulama bilgilerinin çıkarılmasının ardından GSM protokolünden gelen kaydedilmiş paketler decrypt edilmiştir. Kod çözme aşaması TCK 163. maddesinince bazı kodlar gizli tutulmuştur.

5.Kaynakça

[1] Oğuzhan Taş, Fatih Alagöz , “*GSM Güvenliğinde Son Durumlar*”, Boğaziçi Üniversitesi 2017

[2] Azzet Gülşen , “*900 VE 1800 MHz Frekans Bandlarının Gelecekteki Kullanımı ve Türkiye Analizi”*, Bilgi Teknolojileri ve İletişim Kurumu, Temmuz 2013 .

[3] Govarthanam K S, Abirami M, Kaushik J, “*Economical Antenna Reception Design for Software Defined Radio using RTL-SDR*”, Karpagam College of Engineering, Coimbatore-641032, India

[4] Arjunsinh Parmar 1 , Kunal M. Pattani 2, “*Sniffing GSM Traffic Using RTL-SDR And Kali Linux OS*”, International Research Journal of Engineering and

Technology (IRJET), C U Shah College of Engg. & Tech. e-ISSN: 2395 -0056
[5] Fatih Karagöz, “RTL-SDR GR-GSM USAGE” 11 Mayıs 2017 www. fatihkaragoz.me

[6] GSM Alt yapısı ve bileşenleri ,6 Haziran 2011 wwwteknikpcdersleri.com

[7] RTL-SDR Official Website www.rtl-sdr.com