Rahva Teknik ve Sosyal Araştırmalar Dergisi
Cilt: 2, Sayı: 2, 2022, Sayfa: 179 - 188

Rahva Journal of Technical and Social Studies
Vol: 2, Issue: 2, 2022, Page: 179 - 188

Araştırma Makalesi

Radyo Frekans Parmak İzi Toplamak için Yazılım Tanımlı Radyoya Dayalı Düşük Maliyetli Bir Çözüm

Hüseyin PARMAKSIZ[1,✉], Cihan KARAKUZU[2,]

[1]Bilecik Şeyh Edebali Üniversitesi, Rektörlük, Bilgi İşlem Daire Başkanlığı, Bilecik, Türkiye
[2]Bilecik Şeyh Edebali Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği, Bilecik, Türkiye

✉Sorumlu Yazar: huseyin.parmaksiz@bilecik.edu.tr

Geliş tarihi / Received: 05/11/2022 Kabul tarihi / Accepted: 24/11/2022

Özet: Teknoloji ve sistemlerin gelişmesiyle nesnelerin internet (IoT) kullanımı her geçen gün artmaktadır. IoT cihazlarının yaygın kullanımı, bu sistemlerin nasıl güvence altına alınabileceği sorusunu gündeme getirmektedir. Kaynak kısıtlamaları nedeniyle IoT cihazlarında güvenlik önlemi almak mümkün değildir. Bu nedenle, IoT cihazlarında güvenlik giderek daha önemli hale gelmektedir. Literatür incelendiğinde kablosuz cihazlar için ek bir güvenlik katmanı olarak radyo frekansı parmak izi teknikleri kullanıldığı görülmektedir. Kimlik sahtekarlığı veya kimlik sahtekarlığı saldırılarını önlemek için güvenlik amacıyla kablosuz cihazları tanımlamada cihazların donanım bileşenlerindeki üretim kusurları nedeniyle benzersiz parmak izleri kullanılmaktadır. Bu çalışmada, IoT güvenliğini artırmak için etkili bir yöntem olarak kullanılan kablosuz sinyallerin toplama sistemi gerçeklenmiştir.

Anahtar Sözcükler: *DragonOS, Gnu radio, Hackrf one, IoT, radio frekans parmak-izi, yazılım tanımlı radyo.*

A Low Cost Solution Based on Software Defined Radio for Acquisition Radio Frequency Fingerprints

Abstract: The use of the Internet of Things (IoT) is increasing with the advancement of technology and systems. The widespread use of IoT devices begs the question of how to secure these systems. Due to resource constraints, it is not possible to implement security measures on IoT devices. As a result, security is becoming increasingly important in IoT devices. Radio frequency fingerprinting techniques are used as an additional security layer for wireless devices, according to the literature. Unique fingerprints are used to identify wireless devices for security purposes to prevent spoofing or spoofing attacks due to manufacturing defects in the hardware components of the devices. In this study, a wireless signal acquisition system is implemented as an effective method of increasing IoT security.

Keywords: *DragonOS, Gnu radio, Hackrf one, IoT, radio frequency fingerprint, software defined radio.*

1. Giriş

Radyo Frekans (RF) parmak izi, elektronik cihazların yaydıkları sinyallerde üretim kusurları ile oluşan eşsiz bir özelliktir. RF parmak izi çeşitli cihazları tanımlamak için kullanılan bir teknik olup askeri alanda radarların izlenmesinde yaygın olarak kullanılmaktadır (Parmaksız & Karakuzu, 2022). IoT cihazlarındaki donanım bileşenlerin üretim aşamasındaki kusurlardan kaynaklı oluşan RF parmak izleri güvenlik problemlerine çözüm olacak bir yaklaşımdır. Bunun nedeni diğer güvenlik çözümleri gibi yazılımsal veya farklı yöntemlerle müdahale edilemeyecek ve değiştirilemeyecek şekilde tekil olmasıdır. RF parmak izleri, Bluetooth, Wi-Fi, GSM v.d. haberleşme sistemlerine sahip cihazlardan elde edilmektedir. Bu cihazların iletişim kurduğu anda sinyalin belirli durumları (öncül/geçici/kararlı) vasıtasıyla elde edilmektedir (Köse v.d., 2019).

Yazılım tanımlı radyo (SDR), son zamanlarda analog ve dijital iletişim alanında, RF sinyal yakalama çözümlerinde popüler hale gelmiştir. Daha yüksek kapasiteli sistemler, RF tayfının büyük kısmını alabilen ve işleyebilen eksiksiz bağımsız radyo sistemlerine izin veren Evrensel Yazılım Radyo Çevre Birimi (USRP) platformunun ağ bağlantılı serisini içermektedir. Orta kapasiteli, hem alma hem de gönderme kabiliyetine ve 20 MS/s'ye kadar örnekleme hızlarına sahip, 6 GHz'e kadar çalışan HackRF One SDR'dir. RealTek RTL2832U, 2.4 MS/s'ye kadar örnekleme, 2 GHz'e kadar çalışmaktadır (VonEhr v.d., 2016). Yazılım tanımlı radyoların detaylı karşılaştırması Tablo 1'de verilmiştir.

Tablo 1. Yazılım tanımlı radyoların karşılaştırılması (Akhtyamov v.d., 2015).

	HackRF	**BladeRF**		**USRP**		
		x40	**x115**	**B100 starter**	**B200**	**B210**
Radyo spektrumu	30 MHz – 6 GHz	300 MHz – 3.8 GHz		30 MHz – 2.2GHz [a]	50 MHz – 6 GHz	
Bant genişliği	20 MHz	28 MHz		16MHz[b]	61.44 MHz[c]	
Dupleks	Yarım	Tam		Tam	2x2 MIMO	
Örnekleme boyutu	8 bit	12 bit		12/14 bit	12 bit	
Örnekleme oranı	20 Msps	40 Msps		64/128 Msps	61.44 Msps	
Arayüz (hız)	USB 2 (480 megabit)	USB 3 (5 gigabit)		USB 2 (480 megabit)	USB 3 (5 gigabit)	
Mikrodenetleyici	LPC43XX	Cypress FX3		Cypress FX2	Cypress FX3	
Açık kaynak	Evet	HDL + Code schematics		HDL + Code schematics	Host Code[d]	
Fiyat	~320$	~420$	~650$	~675$	~675$	~1100$

[a] Alma/gönderme için ayrı ek kartlar gereklidir. WBX alıcı-verici bu kite dahildir.
[b] 16 bitlik örnekler kullanılıyorsa bunun yarısıdır.
[c] Tek yarım dupleks kanal için 56 MHz, kanal tam dupleks başına 30.72 MHz'dir.
[d] Ettus, B210/B200 için HDL + Code + Schematics'in yayınlanacağını doğrulamaktadır.

Bu sistemler için yazılım desteği, C++ veya Python gibi çeşitli programlama dillerinde özel rutinler yazma yeteneği veya rutinleri donanıma bağlamak için ücretsiz açık kaynaklı GNU Radio sinyal işleme paketi kullanılmaktadır. Öğretim amaçları için, öğrencilerin iletişim sistemleri oluşturmak için iletişim bloklarını yapılandırmasına ve bağlamasına olanak sağlamak için GNU Radio veya Matlab Simulink gibi grafik geliştirme araçları da kullanılmaktadır. Ek olarak, bu iletişim sistemi akış grafiklerini birçok uyumlu donanım cihazına sorunsuz ve kolay bir şekilde bağlamak için açık kaynak modülleri mevcuttur; düşük maliyetli bir anten ile öğrenciler, standart laboratuvar test ekipmanı üzerinde özelliklerini incelerken iletişim sinyallerini iletmekte ve almaktadırlar. Ayrıca, URH, SigDigger, SDR# gibi güçlü ve kullanımı kolay analiz araçları deneyimi artırmaktadır. Literatürdeki RF sinyal yakalama çalışmalarına ait özet Tablo 2'de sunulmaktadır.

Tablo 2. Literatürdeki RF sinyal yakalama çalışmaları.

Yayın Referans	**Kullanılan SDR yada donanım**	**Cihaz/Haberleşme Protokolü**	**Uygulama**
(Barbeau v.d., 2006)	-	(3COM-4, Ericsson-4, Test Radios-2)/Bluetooth	Matlab
(Ureten & Serinken, 2007)	Watkins-Johnson model WJ-8633 alıcı, Tektronix TDS3054	IEEE 802.11b 2.4 GHz ISM bandındaki Wi-Fi sinyalleri	-
(Stewart v.d., 2015)	RTL-SDR	FM radio, UHF band sinyalleri, ISM sinyalleri, GSM, 3G ve LTE mobil radyo, GPS ve uydu sinyalleri	Matlab & Simulink
(Nouichi v.d., 2019)	HackRF One	Cep Telefonları/GSM	GNU Radio
(Yu v.d., 2019)	USRP N210	Ti CC2530 ZigBee	Matlab ve Tensorflow

(Ezuma v.d., 2019)	Keysight MSOS604A	DJI M100 UAV / -	Matlab
(Mohanti v.d., 2020)	Ettus B200mini	DJI Matrice M100 UAVs/Airid	Matlab WLAN toolbox
(Lin v.d., 2020)	USRP B210	ASUS, Panda, ve TOTO-Link AP/Wi-Fi	XGBoost
(Xu v.d., 2020)	USRP B210	Hubsan X12, Hubsan X15, Hubsan FPV1/Radiolink AT10	GNU Radio
(Al-Shawabka v.d., 2020)	USRP X310 USRP N210	IEEE 802.11a/g	GNU Radio
(Reus-Muns v.d., 2020)	USRP X310 USRP B210	IEEE 802.11a, LTE, 5G-NR	POWDER PAWR platformu (Matlab, GNU Radio)
(Uzundurukan v.d., 2020)	Tektronix TDS7404	Akıllı Telefonlar / Bluetooth	Matlab veya AWR
(Liu v.d., 2020)	USRP B210	ADS-B	Matlab
(Huang v.d., 2021)	ADALM-PLUTO	ADALM-PLUTO/waveform	Matlab
(Chen v.d., 2021)	USRP N210	E06-MLE124AP2/Wi-Fi 2.4 GHz	GNU Radio
(Liu v.d., 2021)	BladeRF	ADS-B	Matlab

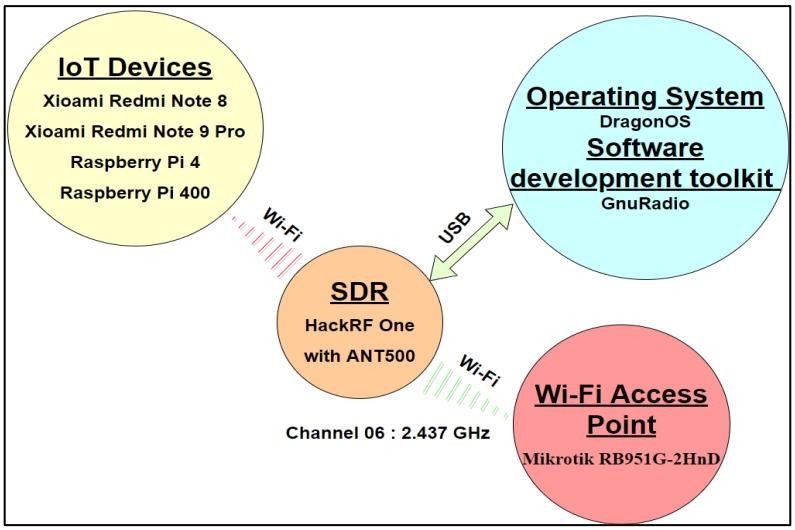
Mevcut RF parmak izlerinin çoğu yüksek maliyetli RF alıcılar ile geliştirilmiş ve bu şartlardaki başarım sonuçları literatürde yer almaktadır. Ancak, bu cihazlarda geliştirilen yöntemlerin pratikte yaygın olarak kullanılması için düşük sistem maliyeti ve sistem esnekliği açılarından değerlendirilmesi gerekmektedir. Bu çalışma kapsamında, düşük maliyetli alıcılarla RF parmak izi sinyalleri toplanmaktadır. Ayrıca mini bilgisayar olarak nitelendirilen düşük kaynaklı Raspberry Pi 4 (RPi-4) üzerinde koşan DragonOS'nin literatürde frekans tayfı ve sinyal analiz süreçlerine büyük kolaylıklar getireceği düşünülmektedir.

2. Materyal ve Metot

IoT cihazlarından sinyal toplamak için Şekil 1'de gösterildiği gibi bir sinyal toplama sistemi tasarlanmıştır. Sinyal yakalamak için ANT500 teleskopik antenli düşük maliyetli bir HackRF One SDR kullanılmaktadır. Açık kaynak GNU Radio uygulaması ile sinyal yakalama süreçleri modellenmektedir.

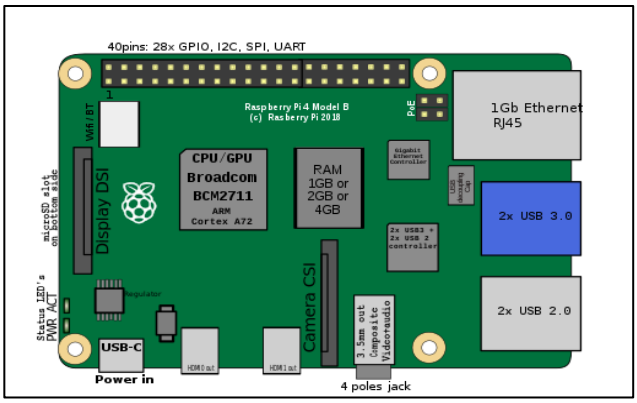
Wi-Fi sinyallerini yakalamak ve kaydetmek için kullanılan bileşenler:

- IoT cihazları: RPi-4, RPi-400, Xiaomi Redmi Note 8, Xiaomi Redmi Note 9 Pro
- Kablosuz SOHO Gigabit AP : Mikrotik RB951G-2HnD,
- Yazılım tanımlı radyo: HackRF One,
- Yazılım radyolarını uygulamak için sinyal işleme blokları sağlayan ücretsiz ve açık kaynaklı yazılım geliştirme araç seti: GNU Radio,
- İşletim sistemi: Ubuntu 20.04.4 LTS tabanlı DragonOS,
- Sistemde kullanılan diğer yazılımlar: Matlab, Wireshark, Python, shell-script, Universal Radio Hacker (URH), SigDigger, Raspberry Pi imager, SD Card Formatter, Win32 Disk imager v.d.
- Faydalı araçlar: xxd, od, inspectrum, setxkbmap, nmcli v.d.



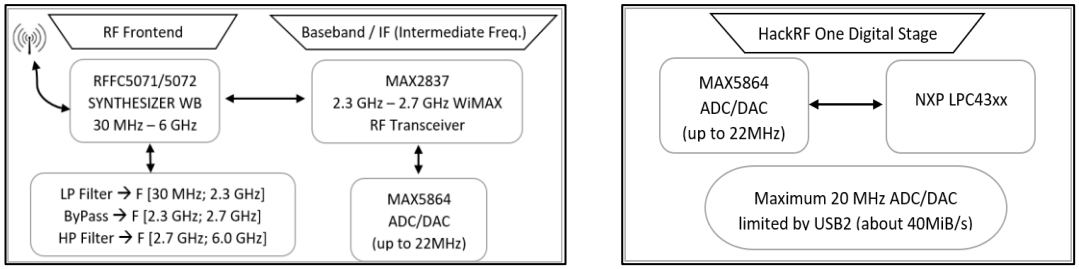
Şekil 1. Sinyal yakalama sisteminin genel yapısı.

Çalışmada, Mikrotik erişim noktası (Access Point) üzerinden belirli kanallarda ve frekanslarda Wi-Fi yayını sağlanmaktadır. Mobil cihaz ya da Wi-Fi erişimi olan cihazlardan bu kanal ile iletişim esnasında araya HackRF One SDR ile girilerek bu sinyallerin dinlenmesi ve yakalanması sağlanmaktadır. HackRF One ile yakalanan ya da izlenen sinyallerin mobil kenar hesaplama (MEC) süreçleri RPi-4 üzerinde koşan DragonOS ile sağlanmaktadır. RPi, mini bilgisayar olarak da ifade edilmektedir (Özbay v.d., 2016). Çalışmada kullanılan RPi-4'e ait bileşen diyagramı Şekil 2'de verilmiştir.



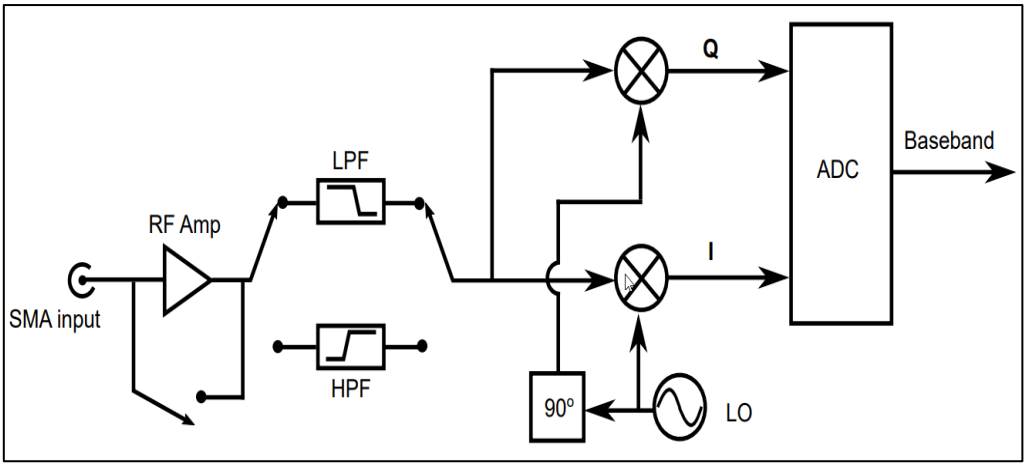
Şekil 2. RPi-4 bileşen diyagramı.

HackRF One, GNU Radio ile çalışan bir SDR aksesuarıdır (Abirami v.d., 2013). HackRF One, 1 MHz ila 6 GHz çalışma aralığı ve yazılım kontrollü anten bağlantı noktası gücü (3,3 V'ta 50 mA) ile radyo sinyallerinin saniyede 20 milyon örnekte yarı çift yönlü iletimini sağlamak için tasarlanmış bir donanım platformudur. Şekil 3, iki bölümlü ön uç/temel bant ve dijital aşamadaki HackRF One blok yapısını göstermektedir.



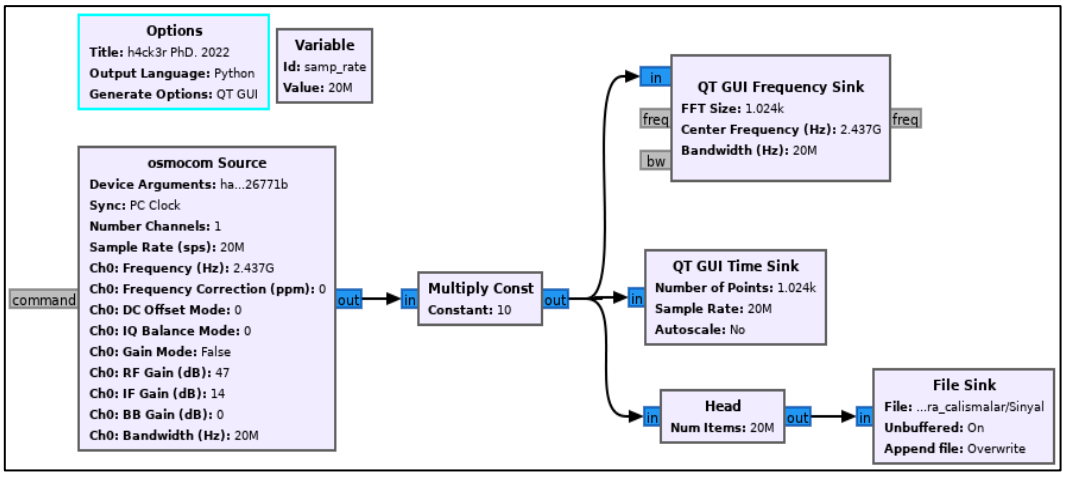
Şekil 3. HackRF One ön uç/temel bant (sol), dijital aşamaları (sağ) (Gummineni & Polipalli, 2020).

HackRF One SDR ile ilgili olarak, Şekil 4 alıcı tarafının bir blok diyagramını göstermektedir. Antenden (SMA konektörü) gelen RF giriş sinyali, sinyalin aktif cihaz aracılığıyla atlanabildiği, kullanıcı tarafından değiştirilebilen bir geniş bant Düşük Gürültülü Amplifier (Low Noise Amplifier), 14 dB kazanç, MGA-81563 ile yükseltilmektedir. Seçilen frekans aralığına bağlı olarak bir Yüksek Geçiren Filtre (HPF) veya Alçak Geçiren Filtre (LPF) ile filtrelenebilmektedir. Dörtlü karıştırıcısı, faz içi (I) ve kareleme (Q) olarak adlandırılan iki bileşen sunmaktadır. Lokal Osilatör sinyali, doğrusal olmayan bir bileşen üzerinde hareket ettiğinde, yüksek frekanslı giriş bandını IF aralığına getirmektedir. Voltaj kontrollü osilatör, RFFC5072 yonga seti ile faz kilitli döngü stabilize karıştırıcı, gelen frekans enerjisini 2.3 GHz ile 2.7 GHz arasında bir IF'ye çevirir, daha sonra 8 bitlik analogdan dijitale dönüştürücü (ADC) ile sayısallaştırılmaktadır. Özellikle HackRF One, bandı bir kerede 22 MHz'e kadar kapsayan bir ADC'ye, MAX 5864'e sahiptir. Maksimum SDR, 20 MHz'lik bir bant genişliğine ayarlanmıştır ve akışı daha sonra 32-bit ARM Cortex işlemcisine, LPC43XX'e gönderilir, daha sonra USB kanalına aktarılmaktadır. RTL birimlerinin IF'leri 3.57 MHz veya 4.57 MHz (R802 tuner durumunda) veya hatta sıfır IF (feshedilmiş E4000 tuner) aralığındadır. Düşük bir IF seçimi daha iyi seçicilik sağlarken, daha yüksek IF'ler daha düşük mikser görüntü yanıtları ile sonuçlanır, bu nedenle seçicilik ve görüntü yanıtı arasında bir değiş tokuş vardır (Valkanas v.d., 2019).



Şekil 4. HackRF One alıcı tarafı blok şeması(Perotoni & dos Santos, 2021).

GNU Radio, RF gerçek zamanlı uygulamalar için bir donanım aygıtının arka ucu olan sinyal işleme blokları sağlamaktadır. GNU Radio'daki programlar, grafiksel bir arayüz olarak, hem C++ hem de Python'da yazılır, derlenir ve işletim sistemlerine (örneğin DragonOS, Linux, Mac OSX ve Windows 10) sahip genel amaçlı işlemcilerin çoğunda çalıştırılmaktadır. Tipik olarak, GNU Radio'daki en yüksek programlama seviyesi Python'da yazılır (yani, sinyal işleme bileşeni başlatma ve kontrol) ve zamana duyarlı herhangi bir işlem C++'da yapılır. Şekil 5, bu çalışmada sinyal yakalama için GNU Radio yazılım paketinde kullanılan blokları ve bloklar aracılığıyla oluşturulan ilişkileri göstermektedir. Kaynak bloğu, örnekleme hızı tarafından tanımlanan sinyali yakalar veya alır ve belirtilen frekansla yükseltir. Osmocom kaynağı, çeşitli donanım türlerini işleme, karmaşık veriler üzerinde çalışma ve tip I ve Q çıktı örnekleri üretme yeteneğine sahiptir. İkili bir dosyaya akış yazmak için File Sink Block'u kullanılmaktadır. Bu dosya, ikili dosyaları (Matlab, C, Python, ...) okuyabilen herhangi bir programlama ortamı ile uyum sağlamaktadır. Örneğin, karmaşık seçilirse ikili dosya, IQIQIQ sırasına göre float32'lerle doldurulacaktır. İkili veriler hiçbir meta veri veya başka bilgi içermemektedir.

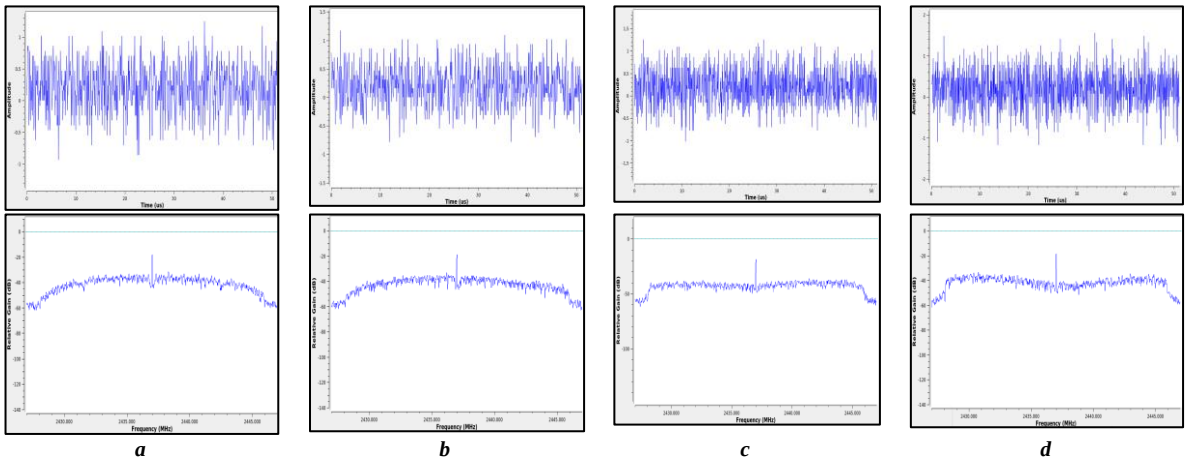


Şekil 5. GNU Radio sinyal yakalama model blok diyagramı.

Sinyaller yakalanırken Mikrotik erişim noktası ile aynı çalışma frekansında yayın yapan cihazların olmamasına dikkat edilmiştir. Ayrıca erişim noktasına bağlantı gerçekleştirilencek cihazların ortam erişim yönetimi *(MAC)* adresleri ile erişim noktası üzerinde erişim kontrol listesi *(ACL)* düzenlenmiştir. Bu sayede sistemin farklı *MAC* adresli cihazlar tarafından sabote edilmesinin önüne geçilmektedir. Aynı çalışma frekansında yayın yapan cihaz varsa Faraday kafesi değerlendirilebilir (Ohmura v.d., 2014). Sinyal toplama scripti erişim noktasına bağlantısını tamamlamış ve dinamik ana bilgisayar yapılandırma protokolü *(DHCP)* ile internet protokol versiyon 4 *(Ipv4)* adresini almış cihazların *iperf3* vasıtasıyla hız testlerine başladıktan sonra, ilgili *MAC ve/veya Ipv4* adresli cihazın yaptığı trafik kayıtları oluştuğunda (*tcpdump ile iperf3 portu, MAC ve ilgili ipv4 adresi dinlenerek*) sinyal kaydetme süreci tetiklenmektedir.

3. Bulgular

Xioami Redmi Note 8, Xioami Redmi Note 9 Pro cep telefonu, RPi-4 ve RPi-400 cihazlarından sinyaller toplandı. Şekil 6'da, bu cihazlardan alınan Wi-Fi radyo frekans sinyallerine ait zaman ve frekans etki alanları gösterilmektedir. Üst kısımdaki görsellerde X (apsis) ekseni zamana (sn) karşılık gelirken, Y (ordinat) ekseni sinyalin genlik değerlerini temsil etmektedir, alt kısımlardaki görsellerde ise X ekseni frekansı (MHz), Y ekseni ise göreceli kazancı (dB) temsil etmektedir. Bu veriler GNU Radio ile sinyal kayıt altına alınmadan önce Şekil 6'daki gibi görselleştirilmektedir.

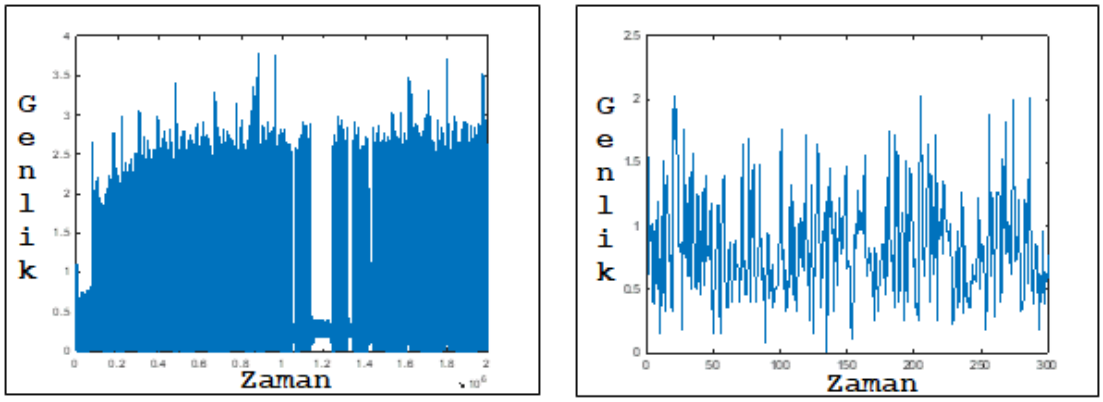


a ***b*** ***c*** ***d***

Şekil 6. Wi-Fi sinyalinin zaman (üst) ve frekans (alt) etki alanı gösterimleri (a: Redmi-Note 9, b: Redmi-Note 8, c: RPi-400, d: RPi-4).

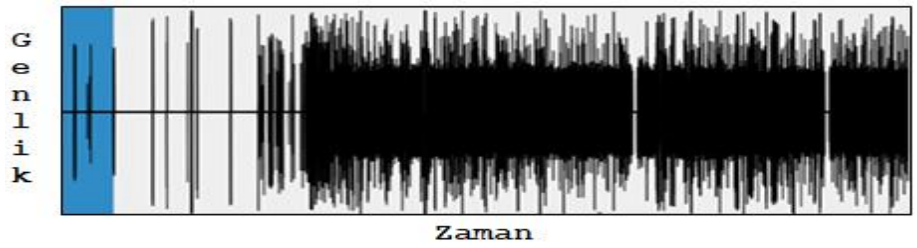
DragonOS'de yazdığımız *shell script* ile sinyal I/Q bileşenlerine ayrıştırılabilmektedir. Matlab hem I/Q bileşenleriyle hem de karmaşık olarak GNU Radio aracılığıyla kaydedilen değerleri işleyebilmektedir. Şekil 7'de veri toplama sistemi ile kayıt altına alınan bir verinin Matlab ortamında

görselleştirmesi sunulmaktadır. Buradaki verilerden özellikler çıkartılarak sınıflandırma işlemlerinde kullanılabilmektedir. Ayrıca yazılım tanımlı radyo alıcılarından alınan sinyalleri analiz etmek ve görselleştirmek için *inspectrum* kullanılmaktadır.



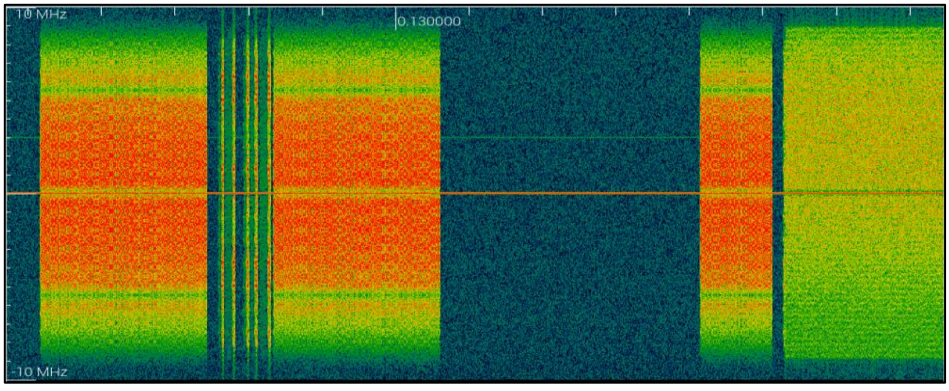
Şekil 7. RPi-4 RF sinyali (sol: tüm sinyal, sağ:ilk zirve noktasından önceki 300 değer – geçici sinyal)

DragonOS işletim sistemi üzerinde yazılan shell script ile Şekil 5'teki modelin tetiklenmesi başlatılarak yakalanan sinyallere zaman damgası eklenerek kayıt altına alınmaktadır. URH, havada uçuşan bitleri ve baytları tanımlamayı kolaylaştırır, modülasyon parametrelerini otomatik algılar ve sinyallerin kolayca demodülasyonuna olanak tanımaktadır. Ayrıca sinyal kaydetme, sniff protokol ve tayf analizi yapmaktadır. Hem Windows hem de Ubuntu işletim sistemlerinde URH ile kayıt altına alınan sinyallerin aksine GNU Radio ile kayıt altına alınan sinyallerinde analizi yapılabilmektedir. Şekil 8'de GNU Radio programı ile kayıt altına alınan örnek bir sinyal gösterilmektedir.



Şekil 8. URH ile analiz öncesi örnek sinyal gösterimi.

Kayıt altına alınan sinyale ait tayf, açık kaynaklı işletim sistemlerinde Inspectrum aracı ile görüntülenerek analiz edilebilmektedir. Inspectrum, RTL-SDR veya HackRF gibi SDR'lerden oluşturulan IQ dosyalarıyla uyumludur. Şekil 9'da X ekseni FFT boyutu ile zamana bağlı olarak pencerenin örnek sayısı belirlemektedir. Bant genişliği, örnekleme frekansıyla değil, örnekleme hızıyla ilgilidir. Gerçek örneklemede, ~20MS/s'lik örnekleme hızıyla, 10MHz'lik bir bant genişliği beklenmektedir ancak HackRF One karmaşık örnekleme yaptığından örnekleme oranı ile bant genişliği eşit olmaktadır. Şekil 9'da Y ekseni [-10MHz,+10MHz] örnekleme oranını ifade etmektedir.



Şekil 9. Inspectrum ile sinyalin tayfı.

Inspectrum'un desteklediği dosya türleri örnekleri:

- *.sigmf-meta, *.sigmf-data - SigMF kayıtları
- *.cf32, *.cfile - Karmaşık 32-bit kayan nokta örnekleri (GNU Radio, osmocom_fft)
- *.cs32 - Karmaşık 16 bit işaretli tamsayı örnekleri (SDRAngel)
- *.cs16 - Karmaşık 16 bit işaretli tamsayı örnekleri (BladeRF)
- *.cs8 - Karmaşık 8 bit işaretli tamsayı örnekleri (HackRF)
- *.cu8 - Karmaşık 8 bitlik işaretsiz tamsayı örnekleri (RTL-SDR)
- *.f64 - Gerçek 64-bit kayan nokta örnekleri (Matlab)

4. Tartışma ve Sonuç

Düşük maliyetli HackRF One SDR ve GNU Radio, sinyal yakalama süreçlerinde literatürde yaygın olarak kullanılmaktadır. Bu makalede, IoT cihazlarından RF parmakizi sinyallerini yaklamak için gerçeklenen Şekil 10'da bir görseli verilen sistem tanıtılmıştır. Sistemde kullanılan DragonOS işletim sistemi, kullanıcılar ile SDR arasındaki iletişimi yönetmektedir.Bu çalışmada,RPi-4 IoT cihazı, DragonOS işletim sistemi, HackRF One SDR ve GNU Radio programları RF parmak-izi yakalama sisteminde bütünleştirilmiştir. Gerçeklenen sistem ile çok sayıda RF parmak izi sinyali yakalanmış ve işlenmek üzere kaydedilmiştir. Bu sistemde kullanılan RPi-4 IoT cihazı ve yazılım tanımlı radyo işlevselliği için özel olarak paketlenmiş Debian tabanlı bir Linux dağıtımı olan DragonOS'nin literatürde tayf ve sinyal analiz kısmında büyük fayda sağlayacağı düşünülmektedir.

Şekil 10. Gerçeklenen sistemin bir görüntüsü.

Çıkar Çatışması

"Yazarlar çıkar çatışması olmadığını beyan etmişlerdir."

Yazarların Katkı Oranı

"Yazarlar makaleye eşit oranda katkı sağlamış olduklarını beyan etmişlerdir."

Etik Beyan

"Bu çalışmada sunulan veri, bilgi ve belgeler akademik ve etik kurallar çerçevesinde elde edilmiştir."

Finansal Destek

"Bu araştırma, Bilecik Şeyh Edebali Üniversitesi Bilimsel Araştırma Projeleri kapsamında 2021-01.BŞEÜ.01-01 numaralı proje ile desteklenmektedir."

Teşekkür

"Tüm akademik çalışmalarımda olduğu gibi bu yayında da önderliği, yardım ve desteklerini esirgemeyen doktora tez danışmanım Prof. Dr. Cihan KARAKUZU'ya teşekkür ederim."

Açıklama

Çalışma, birinci yazarın doktora tezinde kullandığı sinyal yakalama kısmını içermektedir.

Kaynakça

Abirami, M., Hariharan, V., Sruthi, M., Gandhiraj, R., & Soman, K. (2013). Exploiting GNU radio and USRP: An economical test bed for real time communication systems. 2013 fourth international conference on computing, communications and networking technologies (ICCCNT),

Akhtyamov, R., Golkar, A., & Hanson, M. (2015). Development and stratospheric flight demonstration of a SDR-enabled Federated System. Jun-2015.[Online]. Available: https://www. researchgate. net/profile/Rustam_Akhtyamov/publication/282279134_Development_and_stratospheric_flight_demonstration_o f_a_SDR-enabled_Federated_System/links/560a4bdb08ae1396914bb27c. pdf.[Accessed: 14-Jan-2020].

Al-Shawabka, A., Restuccia, F., D'Oro, S., & Melodia, T. (2020). Massive-Scale I/Q Datasets for WiFi Radio Fingerprinting. Computer Networks, 182, 107566.

Barbeau, M., Hall, J., & Kranakis, E. (2006). Detection of rogue devices in bluetooth networks using radio frequency fingerprinting. proceedings of the 3rd IASTED International Conference on Communications and Computer Networks, CCN,

Chen, L., Zhao, C., Zheng, Y., & Wang, Y. (2021). Radio Frequency Fingerprint Identification Based on Transfer Learning. 2021 IEEE/CIC International Conference on Communications in China (ICCC),

Ezuma, M., Erden, F., Anjinappa, C. K., Ozdemir, O., & Guvenc, I. (2019). Micro-UAV detection and classification from RF fingerprints using machine learning techniques. 2019 IEEE Aerospace Conference,

Gummineni, M., & Polipalli, T. R. (2020). Implementation of reconfigurable transceiver using GNU Radio and HackRF One. Wireless Personal Communications, 112(2), 889-905.

Huang, D., Al-Hourani, A., Sithamparanathan, K., Rowe, W. S., Bulot, L., & Thompson, A. (2021). Deep Learning Methods for Device Authentication Using RF Fingerprinting. 2021 15th International Conference on Signal Processing and Communication Systems (ICSPCS),

Köse, M., Taşcioğlu, S., & Telatar, Z. (2019). RF fingerprinting of IoT devices based on transient energy spectrum. IEEE Access, 7, 18715-18726.

Lin, T.-Y., Lai, C.-M., & Chen, C.-W. (2020). Using SDR Platform to Extract the RF Fingerprint of the Wireless Devices for Device Identification. CS & IT Conference Proceedings,

Liu, Y., Wang, J., Niu, S., & Song, H. (2021). ADS-B signals records for non-cryptographic identification and incremental learning. IEEE, Piscataway, NJ, USA, Data Set.

Liu, Y., Wang, J., Song, H., Niu, S., & Thomas, Y. (2020). A 24-hour signal recording dataset with labels for cybersecurity and IoT. IEEE, Piscataway, NJ, USA, Data Set.

Mohanti, S., Soltani, N., Sankhe, K., Jaisinghani, D., Di Felice, M., & Chowdhury, K. (2020). AirID: Injecting a custom RF fingerprint for enhanced UAV identification using deep learning. GLOBECOM 2020-2020 IEEE Global Communications Conference,

Nouichi, D., Abdelsalam, M., Nasir, Q., & Abbas, S. (2019). IoT devices security using RF fingerprinting. 2019 Advances in Science and Engineering Technology International Conferences (ASET),

Ohmura, N., Ogino, S., & Okano, Y. (2014). Optimized shielding pattern of RF faraday cage. 2014 International Symposium on Electromagnetic Compatibility, Tokyo,

Özbay, H., Parmaksız, H., Karafil, A., & Kesler, M. (2016). Farklı Eğim Açılarındaki Fotovoltaik Panellerin Elektriksel Ölçümlerinin Raspberry Pi ile İzlenmesi. Düzce Üniversitesi Bilim ve Teknoloji Dergisi, 4(2), 711-718.

Parmaksız, H., & Karakuzu, C. (2022). A Review of Recent Developments on Secure Authentication Using RF Fingerprints Techniques. Sakarya University Journal of Computer and Information Sciences, 5(3), - (basım aşamasında).

Perotoni, M. B., & dos Santos, K. M. (2021). SDR-based spectrum analyzer based in open-source GNU radio. Journal of Microwaves, Optoelectronics and Electromagnetic Applications, 20, 542-555.

Reus-Muns, G., Jaisinghani, D., Sankhe, K., & Chowdhury, K. R. (2020). Trust in 5G open RANs through machine learning: RF fingerprinting on the POWDER PAWR platform. GLOBECOM 2020-2020 IEEE Global Communications Conference,

Stewart, R. W., Barlee, K. W., Atkinson, D. S., & Crockett, L. H. (2015). Software defined radio using MATLAB & Simulink and the RTL-SDR.

Ureten, O., & Serinken, N. (2007). Wireless security through RF fingerprinting. Canadian Journal of Electrical and Computer Engineering, 32(1), 27-33.

Uzundurukan, E., Dalveren, Y., & Kara, A. (2020). A database for the radio frequency fingerprinting of Bluetooth devices. Data, 5(2), 55.

Valkanas, A., Pandey, D., & Leib, H. (2019). Surfing the radio spectrum using RTL-SDR. IETE Journal of Education, 60(2), 65-73.

VonEhr, K., Neuson, W., & Dunne, B. E. (2016). Software defined radio: choosing the right system for your communications course. 2016 ASEE annual conference & exposition,

Xu, C., Chen, B., Liu, Y., He, F., & Song, H. (2020). RF fingerprint measurement for detecting multiple amateur drones based on STFT and feature reduction. 2020 Integrated Communications Navigation and Surveillance Conference (ICNS),

Yu, J., Hu, A., Zhou, F., Xing, Y., Yu, Y., Li, G., & Peng, L. (2019). Radio frequency fingerprint identification based on denoising autoencoders. 2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob),